Office of Audits
Office of Inspector General
U.S. General Services Administration

IMPLEMENTATION REVIEW OF CORRECTIVE ACTION PLAN

FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk Report Number A190067/Q/T/P21003 September 24, 2021

Assignment Number A240055
August 23, 2024

Table of Contents

Introduction

We have completed an implementation review of the management actions taken in response to the recommendations contained in our September 2021 audit report, *FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk*, Report Number A190067/Q/T/P21003.

Objective

The objective of our review was to determine whether the Federal Acquisition Service (FAS) has taken the actions as outlined in the corrective action plan for *FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk* (see ***Appendix A***).

To accomplish our objective, we:

- Reviewed our audit report, *FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk*, which was issued on September 24, 2021;
- Met and corresponded with FAS personnel;
- Examined documentation submitted by FAS personnel for addressing the corrective action plan steps; and reviewed FAS's implementation of the guidance and procedures contained in these supporting documents.

Background

Homeland Security Presidential Directive 12 (HSPD-12), enacted in 2004, mandates the implementation of a government-wide standard for secure and reliable forms of identification for federal and contractor employees. In response to HSPD-12, FAS's Managed Services Office established the USAccess Program, which provides end-to-end identity and credential management services.

USAccess is a shared service that creates efficiencies across the federal government by centralizing the costs and administration of HSPD-12 mission support. More than 100 federal customer agencies use USAccess to enroll and adjudicate applicants, issue and maintain personal identity verification cards, and operate their identity and credential infrastructure. Customer agencies, including GSA, rely on the USAccess system to initiate background investigations for federal and contractor employees and manage access to federal buildings and information systems. The USAccess system houses biometric information necessary to verify the identities of federal and contractor employees, including name, date of birth, social security number, organizational and employee affiliation, and fingerprints. As of July 2020, the USAccess system maintained personally identifiable information and access rights for approximately 600,000 active personal identity verification cards and credentials.

The USAccess system is fully owned and operated by a contractor under a $154 million, 1-year contract awarded in February 2017, with nine 1-year options. Of more than 100 GSA information technology (IT) systems, USAccess is 1 of only 5 that is designated as "high impact" under Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.[1] Potential impact is deemed high when "the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Further, GSA describes USAccess as "mission critical."

On September 24, 2021, we issued an audit report, *FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk*, to FAS management. The objective of the audit was to determine whether FAS has effective oversight and safeguards in place to ensure that the contractor fulfills federal and Agency security and contractual requirements as part of the USAccess identity and credential management services contract.

Our audit found that FAS's oversight of the USAccess identity and credential management services contract is inadequate, resulting in violations of GSA IT Security Policy, ongoing security-related performance issues, and increased risk to personnel security.[2]

To address the report finding, we recommended that the FAS Commissioner improve USAccess contract oversight to ensure rigorous and accurate contract development and administration. Specifically, we recommended that the FAS Commissioner should:

1. Strengthen the USAccess contractual requirements to ensure timely remediation of USAccess IT security vulnerabilities by consulting with GSA's Office of the Chief Information Security Officer to:
    a. Identify and address possible disincentives for untimely contractor performance; and
    b. Develop performance standards that comply with IT security requirements.

2. Increase contractor accountability and ensure quality performance by:
    a. Revising the USAccess quality assurance surveillance plan to better reflect key aspects of contractor performance, including but not limited to timely security vulnerability remediation; and
    b. Exercising existing quality assurance surveillance plan provisions as appropriate to ensure quality contractor performance.

3. Ensure USAccess security requirements are appropriately and properly implemented by:
    a. Making risk-level determinations for USAccess contractor employees on a position-by-position basis;

[1] Federal Information Processing Standards Publication 199 defines the level of potential impact on organizations and individuals in the event of a security breach, classifying impact levels as either low, moderate, or high.

[2] GSA Order CIO 2100.1M, *GSA Information Technology (IT) Security Policy,* dated March 26, 2021.

b. Clearly, comprehensively, and accurately delineating all personnel security and other security-related contractual requirements, as well as the roles and responsibilities for implementing those requirements; and
c. Establishing controls that ensure GSA personnel are cognizant of security-related roles, responsibilities, and requirements as prescribed by GSA policy and guidance.

The FAS Commissioner agreed with our recommendations.

Results

Our implementation review determined that FAS management has taken appropriate corrective actions to address the recommendations. We determined that no further action is necessary.

Audit Team

This review was managed out of the Information Technology Audit Office and conducted by the individuals listed below:

Sonya Panzo	Associate Deputy Assistant Inspector General for Auditing
Cairo Carr	Audit Manager
Jinnan Chen	Auditor-In-Charge

Appendix A – Corrective Action Plan for Report Number A190067/Q/T/P21003

Federal Acquisition Service/Information Technology Category Corrective Action Plan

Designated Responding Official: Laura Stanton

Signature DocuSigned by: Laura Stanton 99B66D3F19DB4B4... **Date** 1/20/2022

Contact Person: Allen Hill

Telephone Number: (202) 701-7891

Date: December 15, 2021

Report Number A190067, FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk.	**OIG Recommendation 001**	**Date:** April, 2022

Finding(s): The USAccess Managed Services Office (MSO), which resides within FAS, in concert with GSA's Office of the Chief Information Security Officer, failed to ensure USAccess IT security vulnerabilities were remediated within the required time frame and permitted the USAccess system to operate in violation of GSA IT Security Policy for more than a year.

Root Cause of Finding (GSA internal use only): GSA's demonstrated lack of urgency, and the prolonged remediation timelines enabled by the conditional authorizations, may have signaled to the USAccess contractor that the Agency would accept untimely performance.

Recommendation: Strengthen the USAccess contractual requirements to ensure timely remediation of USAccess IT security vulnerabilities by consulting with GSA's OCISO to:

a. Identify and address possible disincentives for untimely contractor performance; and
b. Develop performance standards that comply with IT security requirements.

Action to be Taken Step by Step	Supporting Documentation	Documentation will be sent Last Duty Day of the month
Recommendation 001 - a; Action Step 001: Information Systems Security Manager (ISSM) will hold biweekly meetings with the system owner and information system security officer (ISSO).	1a. **Biweekly Agenda:** This document will provide high-level topics to be discussed during the meeting:	November 11, 2021
	1b. **Meeting Minutes:** This document will provide a high-level recap, outcomes, and action items captured during the meeting	November 11, 2021
	1c. **Plan of Action and Milestones (POAM) for moderate-risk vulnerabilities:** A web form that captures remediation milestones, target date, Acceptance of Risk (AOR) Memos on file, change tracking for moderate risk Vulnerabilities.	April 12, 2022
Recommendation 001 - a; Action Step 002: The vendor will report metrics on open vulnerabilities and status on a monthly basis in the monthly program review (MPR) meeting.	1. **USAccess Monthly Program Review Security Vulnerabilities Metrics Slide(s):** These slides will provide a vendor-supplied metrics report on open security vulnerabilities.	September 13, 2021
Recommendation 001 - a; Action Step 003: The vendor will be required to provide a plan to address risks/ vulnerabilities that cannot be remediated in 90-days within 14-days of identification of said risks/ vulnerabilities, submitting an "acceptance of risk" request: 003a: If a plan is not submitted in accordance with the requirements of Action Step 003 the contracting office will send a non-compliance letter as appropriate. 003b: Non-conformance will be addressed and documented in the annual Contractor Performance Assessment Reporting System (CPARS). 003c: Explore additional financial and performance quality disincentives, specifically as it relates to vulnerability remediation. Identified disincentives will be reviewed by the Office of General Counsel as part of revisions to the contract.	1. **Acceptance of Risk Request Memo Template:** This document will be supplied to the contracting officer and Information Systems Security Officer. 2. **Non-Compliance Letter Template:** Copies of the letter will be filed in Contracting Officer Files. 3. **Documented Communication:** Office of General Counsel's written response concerning legal sufficiency.	April 12, 2022 April 12, 2022 March 31, 2022

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent
Recommendation 001 - b; Action Step 001: The MSO will Incorporate the applicable remediation timeline as stated in the GSA IT security policy into service level agreements (SLAs); developing and adding metrics and price reduction or adequate consideration to the Quality Assurance Surveillance Plan (QASP) if the contractor does not comply with the policy or contract requirements.	1. **Planned Modified contract to include a revised QASP:** The Quality Assurance Surveillance Plan (QASP) will be revised to include the following two performance metrics: (1) Assessment and Authorization (A&A) / PWS Task C.5.5 and (2) Meet or Exceed applicable remediation timelines as stated in GSA IT Security Policy (PWS Task C.5.2.1.15). All critical/high vulnerabilities will be remediated in 30 days or fewer. All medium/moderate vulnerabilities will be remediated in 90 days or fewer. Please note: the contract modification number for this revision will be available after the modification is complete.	April 15, 2022

Report Number A190067, FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk.	OIG Recommendation 002	**Date:** May, 2022

Finding(s):
The MSO has also displayed insufficient oversight, management, and rigor in developing contract terms.

Root Cause of Finding (GSA internal use only): Although the USAccess Quality Assurance Surveillance Plan (QASP) contains performance objectives and financial disincentives for performance failures, it lacks provisions that would hold the contractor responsible for unsatisfactory performance in several security-related areas.

Recommendation: Increase contractor accountability and ensure quality performance by:

a. Revising the USAccess Quality Assurance Surveillance Plan (QASP) to better reflect key aspects of contractor performance, including but not limited to timely security vulnerability remediation; and
b. Exercising existing QASP provisions as appropriate to ensure quality contractor performance.

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent Last Duty Day of the month
Recommendation 002 - a; Action Step 001: We will review, update, and strengthen the QASP to better reflect key aspects of contractor performance, including but not limited to, timely security vulnerability remediation: a. The updated QASP will include the following two performance metrics; (1) Assessment and Accreditation (A&A) / PWS Task C.5.5 and (2) Meet or Exceed applicable remediation timelines as stated in GSA IT Security Policy (PWS Task C.5.2.1.15). All critical/high vulnerabilities will be remediated in 30 days or fewer. All medium/ moderate vulnerabilities will be remediated in 90 days or fewer. b. A comprehensive assessment will be performed to identify other aspects of contractor performance. If other areas are identified they will be included in the updated QASP.	1. **Contract Modification with Revised and Executed QASP:** The contract modification will be bilaterally signed. See Recommendation 001 - b; Action Step 001 for a description of planned revisions to the QASP. Please note: the contract modification number for this revision will be available after the modification is complete. 2. **Contract Areas of Performance Assessment**: Documented results of the assessment.	May 25, 2022 April 30, 2022

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent Last Duty Day of the month
Recommendation 002 - b; Action Step 001: MSO and Contracting Office will continue to monitor contractor performance, and exercise existing QASP provisions as appropriate to ensure quality contractor performance: 1. Monthly, the COR will review the QASP requirements and document results for the contract file. 2. The COR will identify areas of non-performance in accordance with the ITC COR Standard Operating Procedures and will request official action as appropriate from the contracting office in a formal letter or email. 3. Contracting office will notify the vendor of non-performance in a contractual letter in accordance with "FAR 52.246-4 Inspection of Services - Fixed Price" as appropriate. 4. Upon receipt of the revised draft QASP, the Contract Office will request legal sufficiency review of the proposed modification that includes the revised QASP. Specifically, the Contract Office will consult with the Office of General Counsel to explore how the QASP can be modified to enforce additional equitable price reductions or adequate consideration for acceptance of nonconforming supplies or services.	1. **QASP Monitoring Template:** This document will be utilized to capture results from monthly surveillance of vendor performance. 2. **Non-Performance Letter Template:** Non-performance letters will be issued as required. 3. **Documented Communication:** Office of General Counsel's written response.	March 31, 2022 March 31, 2022 March 31, 2022

Report Number A190067, FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk.	OIG Recommendation 003	**Date:** April, 2022

Finding(s): MSO personnel lack clarity regarding personnel security and other security-related roles, responsibilities, and requirements. As a result, MSO personnel have displayed ongoing confusion and misperceptions about contractual requirements.

Root Cause of Finding (GSA internal use only): MSO personnel have consistently exhibited misperceptions, a lack of ownership, and conflicting interpretations of security-related contractual requirements, particularly those related to personnel security, including risk-level determinations and background investigations. This lack of clarity and ownership creates an environment susceptible to errors, including those that could lead to improper implementation of personnel security.

Recommendation: Ensure USAccess security requirements are appropriately and properly implemented by:

a. Making risk-level determinations for USAccess contractor employees on a position-by-position basis;
b. Clearly, comprehensively, and accurately delineating all personnel security and other security-related contractual requirements, as well as the roles and responsibilities for implementing those requirements
c. Establishing controls that ensure GSA personnel are cognizant of security-related roles, responsibilities, and requirements as prescribed by GSA policy and guidance.

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent Last Duty Day of the month
Recommendation 003 - a; Action Step 001: Modify the contract to clearly define the clearance requirements for each end user, privilege roles and management; and develop a security risk-based matrix based on positions, and need for elevated privileges: 1. Define the type of background investigation and clearance level needed for each labor category included in CLIN 5 2. Update the contract language to clearly define clearance requirements for the end user, privileged user, and management roles.	1. **Planned Contract Modification - Modify Section B, CLIN 5 Labor Descriptions:** The contract modification will include the security risk-based matrix. Please note: the contract modification number for this revision will be available after the modification is complete.	April 15, 2022

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent
Recommendation 003 - b; Action Step 001: Restructure system roles within the system to better align with relevant GSA IT policies and standards. The program will more clearly identify and separate what is considered privileged users within USAccess, such that risk levels associated with the standards for privileged users are clearly defined and better understood.	1. **Planned Contract Modification:** The updated contract will remove any ambiguity regarding personnel security and other security-related contractual requirements. Please note: the contract modification number for this revision will be available after the modification is complete. 2. **USAccess Role Assignment Procedures Document:** This document will detail the processes and procedures for role assignment, and personnel responsible for each process.	April 15, 2022 April 15, 2022
Recommendation 003 - b; Action Step 002: A requirement for system administrators to have a higher level of clearance (Top Secret) will be added to the contract.	1. **Awarded Contract Modification:** The contract was modified and awarded on September 28: 1a. The contract modification GS00Q17AHC1003 P00040 clarified the security clearance requirements for contractors working on the contract and increased the security clearance requirements for contractor and subcontractor personnel performing privileged user functions on the USAccess Program. 1b. Section C.5.8 of the Performance Work Statement (PWS) was modified to include: *"C.5.8.1. Top Secret Clearance for Administrator or Technical Personnel Performing Privileged User Functions:* Contractor personnel performing privileged user functions on the USAccess program must be a U.S. Citizen with a Top-Secret clearance. Contractor personnel not performing privileged user functions but support the USAccess program, whether directly or indirectly, must be U.S. Citizens with a Public Trust clearance."	September 28, 2021

Action to be Taken Step by Step	Supporting Documentation to be sent to the OCFO BA or BG office	Documentation will be sent
Recommendation 003 - c; Action Step 001: Ensure that MSO personnel have completed annual security awareness training and have read and understood GSA security guidelines as they relate to security roles and responsibilities. Certificates of completion will be cataloged.	1. **HSPD-12 Requesting Roles and Contractor Background Processes & Procedures Document:** This document is to be developed by the MSO and will outline the MSO's part in complying with GSA's IT Security policies and procedures in relation to contractor background investigation. 2. **HSPD-12 Requesting Roles and Responsibilities Training** with Issued Certificate: This online, self-assigned training course is for HSPD-12 requesting officials. The purpose of this training course is to prepare the learner to assist and support the HSPD-12 background investigation and credentialing process for the contracts they administer. A certificate of completion is provided on successful completion of the course. According to GSA security policies and procedures training, CIO-IT Security-05-29, Revision 6 Security and Privacy Awareness and Role Based Training Program, training is required on an annual basis.	April 12, 2022 April 12, 2022
Recommendation 003 - c; Action Step 002: The MSO will consult with the Office of Mission Assurance (OMA) to determine the scope of the relevant policy and guidance with regards to personnel security to ensure MSO team members are aware of their roles and responsibilities.	1. **Contractor Background Investigation Process and Procedures**. This document outlines the process and procedures for submitting contractors for background investigation. 2. **Agenda:** This document will provide high-level topics to be discussed during the meeting. 3. **Meeting Minutes:** This document will provide a high-level recap, outcomes, and action items captured during the meeting.	September 22, 2021 April 12, 2022 April 12, 2022

Appendix B – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Acting FAS Commissioner (Q)

Acting FAS Deputy Commissioner (Q1)

FAS Deputy Commissioner (TTS)

FAS Chief of Staff (Q0A)

Assistant Commissioner for Information Technology Category (QT)

Deputy Assistant Commissioner for Category Management (QT3)

Director, Identity Credential and Access Management Division (QT3B)

Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

Deputy Assistant Inspector General for Acquisition Audits (JA)

Deputy Assistant Inspector General for Real Property Audits (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)