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

FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk

Report Number A190067/Q/T/P21003
September 24, 2021

Executive Summary

FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk

Report Number A190067/Q/T/P21003
September 24, 2021

Why We Performed This Audit

We performed this audit in response to a March 2019 referral from our Office of Investigations regarding possible management deficiencies with the GSA Federal Acquisition Service's (FAS's) USAccess Program, which manages federal and contractor employee credentials. In June 2019, we issued an Alert Memorandum that identified specific USAccess information technology (IT) security vulnerabilities and administrative control weaknesses. After issuing the Alert Memorandum, we continued this audit to address additional control weaknesses related to FAS's oversight of the security and contractual requirements of the USAccess contract. Accordingly, the objective of our audit was to determine whether FAS has effective oversight and safeguards in place to ensure the contractor fulfills federal and Agency security and contractual requirements as part of the USAccess identity and credential management services contract.

What We Found

We found that FAS's oversight of the security and contractual requirements for the USAccess identity and credential management services contract is inadequate. 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. Additionally, the MSO has not effectively held the USAccess contractor accountable for key IT-security-related performance requirements. The MSO has also displayed insufficient oversight, management, and rigor in developing contract terms. Finally, 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.

What We Recommend

We recommend the FAS Commissioner improve USAccess contract oversight to ensure rigorous and accurate contract development and administration. Specifically, 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;
    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. His response is included in its entirety in ***Appendix B***.

Table of Contents

Introduction

We performed an audit of the GSA Federal Acquisition Service's (FAS's) oversight and control of the USAccess identity and credential management services contract. Through its USAccess Managed Services Office (MSO), FAS offers USAccess to federal agencies. USAccess currently serves more than 100 federal customer agencies.

Purpose

We performed this audit in response to a March 2019 referral from our Office of Investigations regarding possible management deficiencies with GSA's USAccess Program, which manages federal and contractor employee credentials. In June 2019, we issued an Alert Memorandum that identified specific USAccess information technology (IT) security vulnerabilities and administrative control weaknesses.[1] After issuing the Alert Memorandum, we continued this audit to address additional control weaknesses related to FAS's oversight of the security and contractual requirements of the USAccess contract.

Objective

Our objective was to determine whether GSA 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.

See ***Appendix A*** – Scope and Methodology for additional details.

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 MSO 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 (PIV) 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

[1] Restricted *Alert Memorandum: Significant Security Weaknesses in the USAccess System Placed National Security at Risk* (Memorandum Number A190067-2, June 20, 2019).

July 2020, the USAccess system maintained personally identifiable information (PII) and access rights for approximately 600,000 active PIV 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 9 option years. Of over 100 GSA IT systems, USAccess is 1 of only 5 that is designated as "high impact" under Federal Information Processing Standards Publication 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems.*[2] 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."

We initiated our audit in March 2019 in response to a referral from our Office of Investigations regarding possible management deficiencies with the USAccess Program. In June 2019, we issued an Alert Memorandum that identified specific control weaknesses in the contractor's implementation of USAccess and recommended that FAS take immediate action to secure the system. In August 2019, FAS notified the contractor that the USAccess system was not compliant with federal security standards. The letter detailed the weaknesses identified in our Alert Memorandum and stated that the contractor must develop and submit a response plan. In its October 2019 response, the contractor described policies, oversight efforts, and other actions underway to address the identified weaknesses.

In developing the Alert Memorandum, we saw evidence that weak contractual oversight may have contributed to the security vulnerabilities we identified. We also found possible violations of federal and Agency security policies and contractual requirements. While this report does not restate the deficiencies we communicated in the Alert Memorandum, we continued this audit to address additional control weaknesses. Accordingly, we modified our audit objective and focused our work on both security and contractual oversight and compliance.

[2] FIPS 199 defines the levels of potential impact on organizations and individuals in the event of a security breach, classifying impact levels as either low, moderate, or high.

Results

Finding – 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.

The FAS MSO's oversight of the security and contractual requirements for the USAccess identity and credential management services contract is inadequate. The MSO, in concert with GSA's Office of the Chief Information Security Officer (OCISO), 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 Information Technology Security Policy* (CIO 2100.1M) (GSA IT Security Policy) for more than a year. Additionally, the MSO has not effectively held the USAccess contractor accountable for key IT-security-related performance requirements. The MSO has also displayed insufficient oversight, management, and rigor in developing contract terms. Finally, 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.

Failure to Ensure Timely Remediation of IT Security Vulnerabilities

The MSO, in concert with GSA's OCISO, failed to ensure USAccess system IT security vulnerabilities were remediated within the required time frame and, as a result, the USAccess system operated in violation of GSA IT Security Policy for more than a year. Although GSA requires moderate vulnerabilities to be remediated within 90 days, nearly half of the IT security vulnerabilities cited in the April 2019 USAccess security assessment were not remediated within this time frame. These delayed remediations of USAccess, a high-impact, mission-critical system, resulted in ongoing risk for not just GSA, but also its more than 100 federal customer agencies.

In accordance with GSA IT Security Policy and GSA's IT Security Procedural Guide, *Managing Enterprise Risk* (CIO IT Security 06-30), USAccess must undergo an independent security assessment every 3 years to receive an authorization to operate as part of GSA's Assessment and Authorization process. This process ensures that the system has the proper security controls implemented. Following the assessment, the independent assessor delivers a security assessment report to GSA documenting vulnerabilities, findings, and recommendations. The USAccess contractor then develops an action plan specifying remediations or enhancements that must be implemented. Finally, OCISO personnel review the action plan, make a risk-level determination, and issue either a full or conditional authorization.

The April 2019 USAccess security assessment identified 89 moderate-risk security vulnerabilities. The MSO worked with the OCISO and the contractor to prioritize the needed remediations, oversee resolution efforts, and manage system risk. Nonetheless, nearly half of

the 89 vulnerabilities were not remediated within GSA's prescribed 90-day time frame. Our analysis revealed that:

- Overall, the elapsed time for the overdue remediations averaged 173 days, or 83 days past the 90-day deadline, with three requiring more than 300 days to successfully remediate.

- As of November 2020, one vulnerability remained unremediated, approximately 15 months after the original 90-day deadline.

Figure 1 below provides three examples of USAccess IT security vulnerabilities that were not remediated within the required time frame. It also identifies the risks and implications of those security vulnerabilities, further demonstrating the importance and significance of timely remediation.

Figure 1 – Examples of Substantially Overdue Vulnerability Remediations

Security Control Name and Description	Assessment Report Finding	Implication of Vulnerability	Days Overdue *(beyond 90-day requirement)*
[redacted]	[redacted]	[redacted]	154
[redacted]	[redacted]	[redacted]	156
[redacted]	[redacted]	[redacted]	180

Conditional authorizations. In total, more than 18 months elapsed from the issuance of the security assessment until the completion of our analysis. During that time, the USAccess system operated under two successive conditional authorizations to operate (conditional

authorizations) issued by GSA's OCISO. Conditional authorizations are the OCISO's attestation that the risk of continued operations to "organizational operations, organizational assets, individuals, [and] other organizations" is acceptable despite any unremediated security vulnerabilities identified by the most recent security assessment.

The two conditional authorizations, as shown below, continually extended the remediation time frame and allowed the USAccess system to operate well beyond GSA IT Security Policy requirements:

- April 23, 2019, Conditional Authorization:
  - Authorized USAccess system operation through October 11, 2019; and
  - Required remediation of identified vulnerabilities by July 31, 2019, which was 20 days beyond the 90 days prescribed by GSA IT Security Policy.

- October 11, 2019, Conditional Authorization:
  - Authorized USAccess system operation through October 11, 2020; and
  - Required remediation of remaining 15 vulnerabilities by October 11, 2020, which was 458 days beyond the 90 days prescribed by GSA IT Security Policy.

While OCISO personnel told us that they sometimes use conditional authorizations as a management tool to effect positive change, these conditional authorizations enabled USAccess, a high-impact, mission-critical system, to operate in violation of the Agency's own vulnerability remediation policies for more than a year. Further, the extended remediation time frame granted by the conditional authorizations weakened the MSO's ability to enforce USAccess contract terms.

In failing to ensure timely remediation of known IT security vulnerabilities, GSA exposed USAccess to ongoing risk. Such risk exposure affects not only GSA, but also the more than 100 federal customer agencies that rely on GSA's authorization to operate rather than conduct their own security assessments for USAccess. In addition, 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.

To protect GSA and its USAccess customer agencies from unnecessary risk, FAS must exercise proper contractor oversight and ensure timely remediation of USAccess IT security vulnerabilities.

Ineffective Accountability for Contractor Performance

The MSO has not effectively held the contractor accountable for key IT security performance requirements. In accordance with Federal Acquisition Regulation 46.4, *Government Contract Quality Assurance*, the USAccess contract contains a performance-based quality assurance surveillance plan (QASP), a mechanism by which the MSO is expected to hold the contractor

accountable if it is not meeting contractual requirements. Further, Federal Acquisition Regulation 46.202-4, *Higher-level contract quality requirements*, emphasizes the added importance of quality assurance in relation to criticality, "Requiring compliance with higher-level quality standards is necessary in solicitations and contracts for complex or critical items…."

Although the USAccess QASP contains performance objectives and financial penalties for performance failures, it lacks provisions that would hold the contractor responsible for unsatisfactory performance in several security-related areas. The MSO's tolerance for substandard performance has exposed the USAccess system to possible security risks and contributed to an environment lacking in accountability. Taken together, these issues have the potential to foster reputational damage to GSA and the USAccess Program.

Contractor performance assessments. Annually, the MSO completes an assessment evaluating the contractor's performance in areas such as quality, schedule, cost control, and management. In two recent assessments (discussed below), MSO officials documented that the USAccess contractor was having ongoing challenges managing its duties and responsibilities under the contract and cited release management and substandard configuration management, both security-related matters, as particular concerns.[3] These matters are discussed below.

2018-2019 contractor performance assessment. The MSO's 2018-2019 contractor performance assessment stated that the contractor's poor performance in areas of "vital importance to the continued operation and reputation of the program leave the program at risk of failure." Specifically, MSO officials reported that:

- Inadequate configuration management brought USAccess "within days" of losing its authorization to operate; and
- The contractor had not, during the reporting period, adhered to the agreed-upon testing time frame for new releases. Although user testing was supposed to take place 45 days prior to release, it was occurring 2 to 3 days prior to release, which did not "afford sufficient time to remediate any issues that may be found."
    - The contractor performance assessment details one case where a release proceeded without mitigating a known problem, resulting in functionality issues, more than 400 calls to the USAccess help desk in 1 day, and numerous customer complaints.
    - In another example of poor release management, the MSO reported that an issue that could have "easily been mitigated prior to release" resulted in damage to the program's reputation and "hampered the ability of the program to carry out its mission."

[3] Release management is the process of designing, developing, testing, and implementing hardware or software changes to the USAccess infrastructure in the least disruptive manner. Configuration management is a collection of activities aimed at establishing and maintaining the integrity of an IT system throughout its lifecycle.

2019-2020 contractor performance assessment. The MSO's 2019-2020 contractor performance assessment reported that, although the contractor's performance had improved, overall management, configuration management, and release management remained particular areas of concern. In the area of release management, MSO officials stated that the contractor was conducting pre-release testing 7 to 10 days prior to release, which still did not "afford sufficient time to remediate any issues that may be found." Regarding configuration management, the MSO reported that the contractor was working with GSA to develop and implement improved processes and that progress was "promising," but also that improvement was needed.

Configuration management and release management are contractually required performance elements, yet both contractor performance assessments state that the contractor's performance in these areas was deficient. While FAS worked with the contractor to improve configuration and release management, it did not penalize the contractor for its deficient performance. In addition, the contractor was not held accountable for its delays in remediating the 89 security vulnerabilities identified in the April 2019 security assessment. Neither configuration management nor vulnerability remediation are included in the contract's QASP and, in spite of ongoing performance deficiencies, MSO officials have not modified the plan to include these performance elements.

The QASP, however, does include a release-management-related performance element: "Planning Accuracy," which is described as "system change requests developed and deployed according to the mutually agreed upon schedule." While the MSO's contractor assessments do not cite deployment timing as a problem, they do report that release development prior to deployment is not in accordance with the agreed-upon schedule (i.e., the contractor is not adhering to appropriate user testing time frames). Nonetheless, MSO officials have not invoked the contract's Planning Accuracy provision, which would hold the contractor accountable for its performance and result in financial consequences.

QASP sufficiency. During our audit work, we interviewed current and former MSO officials about the USAccess QASP. A former USAccess contracting officer acknowledged that the QASP, as currently configured, is lacking in metrics and was poorly planned. Current MSO officials have also stated that the contract is "short on measures for performance" and lacks sufficient consequences for noncompliance with security control remediation deadlines.

The current contracting officer reported that the MSO is currently negotiating possible QASP revisions with the contractor in an effort to increase contractor accountability. However, our review of the draft revisions revealed that the proposed plan is virtually identical to the existing plan. The proposed changes address neither the configuration management nor the vulnerability remediation deficiencies noted above. In tolerating substandard contractor performance, the MSO continues to expose the USAccess system and, by extension, GSA and its customer agencies, to possible security risks.

To protect the integrity of the high-impact, mission-critical USAccess Program, FAS should increase contractor accountability and ensure quality performance by strengthening the contract's QASP. Further, FAS should invoke the plan's financial consequences as warranted. These recommendations are aligned with GSA's current efforts to improve contract administration Agency-wide as part of its Management and Internal Control Program. Specifically, GSA's *2019 Agency Financial Report* states that, with performance-based contracts constituting approximately 80 percent of GSA-obligated dollars, the Agency "needs to ensure these contracts contain the applicable performance standards and surveillance plans to allow proper assessment of the contractor's performance…."

Insufficient Oversight, Management, and Rigor in Developing Contract Terms

The MSO has not ensured that contract terms clearly and adequately reflect GSA policy and IT security guidance. We found that the MSO displayed insufficient oversight, management, and rigor in developing contract terms. The MSO has shown a similar lack of rigor, as well as a lack of urgency, in executing contract modifications that would correct deficiencies and strengthen contractual requirements. As described below, such insufficient control has the potential to increase security risk; compromise program effectiveness and efficiency; and lead to the unnecessary expenditure of time, effort, and taxpayer dollars on after-the-fact contract modifications.

Personnel security risk-level determinations. During contract development, FAS did not adequately consider personnel security risk-level determinations for contractor employees with significant security responsibilities and system access, such as system administrators.

According to the National Institute of Standards and Technology, personnel security involves assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals. Further, GSA's *HSPD-12 Personal Identity Verification and Credentialing Handbook* (CIO P 2181.1) (HSPD-12 Handbook) addresses risk-level determinations and requires that contractor employees have background investigations appropriate to their responsibilities, mirroring those of GSA employees performing the same duties. GSA managers are empowered to determine risk levels for positions under their purview, even ranging as high as a national security designation.

During testing, our sample of USAccess contractor employees included a system administrator with significant security responsibilities and system access who did not have a higher-level background investigation. The employee's Tier 2 background investigation was at a level identical to that of the other employees, including lower-level help desk personnel.[4] However,

[4] Background investigation levels are determined by a multitude of factors, including job responsibilities, access to classified or sensitive information, and access to IT systems. The lowest-level investigation, PIV-card-level clearance, requires favorable adjudication of a Federal Bureau of Investigation fingerprint check and a National Agency Check with Written Inquiries security investigation. Employee positions deemed moderate-risk or high-risk require more strenuous background investigations: moderate-risk positions require Tier 2 investigations and high-risk positions require Tier 4 investigations.

the HSPD-12 Handbook states that individuals "significantly involved [with] … mission-critical systems" are considered high-risk public trust positions, which require more-detailed Tier 4 background investigations.

The MSO has reconsidered the contract's personnel security standards and has been negotiating increased standards and their associated costs with the contractor. We recognize that such contract modifications require agreement by both parties, but also note that negotiations have been ongoing since at least August 2019 and a modification has not yet been implemented.

USAccess QASP. As reported above, MSO personnel have acknowledged that the USAccess QASP received insufficient attention during contract development. Yet, even in the face of ongoing contractor performance issues, the MSO has not made modifications to the contract's QASP. While the MSO is now considering modifications, the changes do not address the security-related performance concerns discussed above.

Control implementation. Subsequent to our June 2019 Alert Memorandum, GSA directed the USAccess contractor to address our concerns regarding IT security control weaknesses. In addressing one of the control deficiencies, the contractor merely stated that it would no longer occur. However, the MSO has not exercised due diligence to ensure a control has been implemented. Specifically, we asked MSO personnel if the contractor's attestation had been incorporated into the contract or otherwise memorialized, and they told us that the contractor's statement that the deficiency would no longer occur sufficed, and no further action was needed. As a result, FAS lacks ongoing assurance that the issue will not reoccur, thereby increasing risk to the USAccess system and its customers.

Inadequate oversight and management has the potential to increase security risk and compromise program effectiveness and efficiency—not just for GSA, but also for more than 100 federal customer agencies who rely on the integrity of USAccess. Further, lack of oversight and rigor in developing and revising contract terms puts GSA in a reactive posture that can lead to the unnecessary expenditure of time, effort, and taxpayer dollars. GSA should ensure that the MSO develops and manages the USAccess contract to properly reflect applicable federal and GSA security-related policy and guidance.

MSO Personnel Lack Clarity Regarding Security Requirements

MSO personnel lack clarity regarding security-related roles, responsibilities, and requirements. They 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.

Federal and GSA policy and guidance place responsibility for contractor personnel security and other security requirements directly with the MSO. Specifically, GSA IT Security Policy states that contracting officers and contracting officer's representatives are responsible for ensuring a contractor's compliance with the policy. Additionally, the GSA Acquisition Manual 504.1370, *GSA Credentials and Access Management Procedures*, holds contracting officers or their representatives accountable for contractor employee credentialing. Further, GSA's *Heads of Services and Staff Offices' and Requesting Officials' Roles and Responsibilities to Implement HSPD-12* (ADM 5400.2) similarly states that contracting officials are responsible for implementing contractor personnel security requirements.

In general, we found that personnel security for USAccess contractor employees is properly implemented. However, it appears that this is largely the result of contractor execution rather than MSO personnel actions or oversight. During our audit:

- Multiple MSO officials, on separate occasions, incorrectly claimed that USAccess contractor employees require only PIV-card-level clearances, which is the federal standard for contractor employees in low-risk positions.[5] Because the USAccess system maintains PII, *GSA Rules of Behavior for Handling Personally Identifiable Information (PII)* (CIO 2180.2) requires that contractor employees have at least a Tier 2 (formerly called Tier 2S) background investigation.

- An MSO contracting official incorrectly claimed that, beyond the basic PIV-card-level clearance, it is the USAccess contractor's responsibility to determine background investigation levels for its employees. In a subsequent meeting, the official again stated that the contractor assigns security levels for its own employees. However, GSA policy and guidance, including GSA IT Security Policy and the HSPD-12 Handbook, clearly place responsibility for risk-level determinations on GSA, not the contractor.

- MSO personnel, on separate occasions, appeared unaware of factors used in determining personnel security requirements. In one instance, an MSO contracting official stated they were unsure whether USAccess's "high impact" FIPS 199 categorization factored into contractor employees' risk-level determinations. Separately, another MSO official told us that USAccess's FIPS 199 categorization does not affect personnel security requirements. However, the HSPD-12 Handbook states that risk-level determination is partly based on the system's FIPS 199 categorization. The same MSO official also stated that PIV-card-level clearances were sufficient for contractor employees because they were not working with PII. However, as noted above, the USAccess system does contain PII; therefore, Tier 2 investigations are required at a minimum.

[5] PIV-card-level clearance requires favorable adjudication of a Federal Bureau of Investigation fingerprint check and a National Agency Check with Written Inquiries security investigation.

- MSO personnel, on multiple occasions, provided contradictory information about personnel-security-related contractual requirements. As noted above, an MSO contracting official erroneously told us during an interview that the contractor makes its own risk-level determinations. Another MSO official told us later that the contractor does not make risk-level determinations. A similar contradiction occurred when, in reviewing a roster of contractor employees, we observed that all of the employees had Tier 2 clearances. Because this contradicted MSO officials' repeated prior claims that contractor employees needed only PIV-card-level clearances, we asked MSO personnel for clarification. They told us that the Tier 2 clearances were contractually required.

- MSO personnel made multiple contradictory and incorrect statements about non-disclosure agreement (NDA) requirements. Initially, a contracting official informed us that contractor employees were required to complete NDAs, and that the NDAs were in the MSO's possession. Approximately 2 months later, the same contracting official informed us that the MSO was still in the process of getting the NDAs signed. Then, 14 months later, the contracting official told us that contractor employee NDAs were not required. Finally, 2 months later, the MSO provided us with NDAs that had been signed earlier that same month.

GSA has previously recognized the need for clearly defined roles and responsibilities in contract administration. Both the 2019 and 2020 *Agency Financial Report* cite the importance of ensuring that members of contracting teams strengthen coordination, gain a clear understanding of roles and responsibilities, and improve communication practices. Yet, MSO personnel have consistently demonstrated a lack of clarity and a corresponding lack of ownership regarding security-related contractual requirements despite the fact that federal and GSA policies and guidance clearly place responsibility for security-related contract oversight with the MSO. These deficiencies create an environment susceptible to errors that lead to improper implementation and oversight of security-related matters, including personnel security risk-level determinations and background investigations. FAS must ensure USAccess contracting and security officials are cognizant of the contract's security-related requirements and understand their roles and responsibilities for implementing and enforcing those requirements.

Conclusion

We found that FAS's oversight of the security and contractual requirements for the USAccess identity and credential management services contract is inadequate. The MSO, in concert with GSA's OCISO, 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. Additionally, the MSO has not effectively held the contractor accountable for key IT-security-related performance requirements. The MSO has also displayed insufficient oversight, management, and rigor in developing contract terms. Finally, 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.

Taken together, federal and GSA policy and guidance place responsibility for contractor performance, contractor compliance, and system security on MSO personnel. These individuals are collectively charged with ensuring that the USAccess system has the necessary security controls, the contract reflects security and privacy requirements, and the contractor is fully conforming to contract terms. To ensure proper contract development and administration, and to fulfill the goals of GSA's own Management and Internal Control Program, GSA must improve oversight of the USAccess contract.

Recommendations

We recommend the FAS Commissioner improve USAccess contract oversight to ensure rigorous and accurate contract development and administration. Specifically, the FAS Commissioner should:

1. 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.

2. Increase contractor accountability and ensure quality performance by:
    a. Revising the USAccess 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.

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;

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.

GSA Comments

The FAS Commissioner agreed with our recommendations. His response is included in its entirety in ***Appendix B***.

Audit Team

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

Sonya D. Panzo	Associate Deputy Assistant Inspector General for Auditing
Kyle D. Plum	Audit Manager
Suzanne B. Weiss	Auditor-In-Charge

Appendix A – Scope and Methodology

Our audit, initiated in response to a March 2019 referral from our Office of Investigations, examined GSA's contractual oversight of the USAccess Program. Our audit encompassed actions and activities under the current USAccess contract from February 2017 through April 2021. Specifically, we assessed whether: (1) security control remediations are handled within the required time frames, (2) adequate controls are in place to ensure effective and quality contractor performance, and (3) personnel security is properly and sufficiently implemented.

To accomplish our objective, we:

- Coordinated with our Office of Investigations to obtain background information regarding possible USAccess Program management deficiencies;
- Reviewed GSA policies, guidance, and procedures for contractor personnel security, with a particular focus on risk-level determinations and background investigations;
- Reviewed federal regulations and policies regarding personnel security;
- Reviewed federal regulations and policies governing IT security controls, including National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and the FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*;
- Reviewed the Federal Acquisition Regulation and GSA Acquisition Manual regarding contracting officer responsibilities, contract development and modification, and performance-based contracts;
- Reviewed GSA IT security policies and procedural guides related to IT acquisitions, IT risk management, external IT systems, and IT security vulnerability remediation;
- Gained an understanding of GSA's assessment and authorization process for IT systems, including security assessment reports, authorizations to operate, conditional authorizations to operate, vulnerability remediation policies and standards, and plans of action and milestones;
- Reviewed USAccess contract documentation including the QASP, the contractor's system security plan, and GSA-authored contractor assessment reports;
- Interviewed personnel from the USAccess MSO, the OCISO, and the Office of Mission Assurance;
- Requested and reviewed system logs, NDAs, plans of action and milestones, proposed contract modifications, and documentation related to existing contract modifications;
- Evaluated modifications and fund reallocations made to the USAccess contract;
- Tested the contractor's timeliness in providing system logs to GSA;
- Tested whether personnel security requirements for a judgmental sample of 20 contractor employees (from a total population of 194) had been implemented correctly and completely;
- Tested the remediation timeliness of 89 moderate-risk security control vulnerabilities identified in the April 2019 *USAccess Security Assessment Report* and tracked those remediations through November 2020; and

- Compared performance measures in the USAccess QASP to the contract's performance work statement.

We conducted the audit between March 2019 and April 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of the audit.

Appendix B – GSA Comments

DocuSign Envelope ID: BC8FDC07-F2E2-485D-9A54-E40D9641028A

GSA Federal Acquisition Service

9/7/2021

MEMORANDUM FOR: Sonya D. Panzo
Associate Deputy Assistant Inspector General for Auditing
Acquisition & Information Technology Audit Office (JA-T)

FROM: Sonny Hashmi
Commissioner
Federal Acquisition Service (Q)

Sonny Hashmi

SUBJECT: Response to the U.S. General Services Administration Office of Inspector General (OIG) Draft Report titled *FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk; Report Number (*A190067)

Thank you for the opportunity to comment on the referenced draft report FAS's Inadequate Oversight of Contractual and Security Requirements Places the USAccess Program at Risk, Report Number A190067, dated August 26, 2021. The Federal Acquisition Service (FAS) provides its response to the recommendations below:

OIG Recommendation 001

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

FAS agrees with this recommendation and has proactively implemented several measures to strengthen contractual requirements and improve communication with GSA's OCISO. In June 2020, a contract modification was awarded implementing a solution to strengthen security management. The team established monthly meetings to track and manage security vulnerabilities and determine levels of acceptable risk. Additionally, the USAccess program has now obtained a 3-year system Authorization to Operate (ATO). GSA will continue to build on these activities in the Corrective Action Plan.

OIG Recommendation 002

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

- 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.

FAS agrees with the recommendation and has implemented several measures to address and improve quality assurance procedures. GSA is developing an enhanced Quality Assurance Surveillance Plan (QASP) which establishes a regular cadence of several operational and status meetings with the vendor, program managers and contracting officer to track and address potential technical and/or security vulnerabilities. We will continue to build on these activities in the Corrective Action Plan.

OIG Recommendation 003

- 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, comprehensive, 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.

FAS agrees with the recommendation and has implemented several measures to address and improve implementation of security requirements. FAS modified the contract to clearly define personnel security clearance requirements and increased the level of security clearances for employees with elevated privileges. We will continue to build on these activities in the Corrective Action Plan.

Upon issuance of the final audit report, FAS will establish a Corrective Action Plan which will outline the specific actions to be taken in support of the implementation as well as the estimated dates for completion of those actions.

Thank you for the opportunity to review this draft report. If you have any questions, please contact Darlene Gore from the Identity Credentialing and Access Management Division at darlene.gore@gsa.gov or (703) 517-0805.
.

Appendix C – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

FAS Commissioner (Q)

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 & Access Management Division (QT3B)

Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

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