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

GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk

Report Number A190085/A/6/F21001
November 4, 2020

Executive Summary

GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk

Report Number A190085/A/6/F21001
November 4, 2020

Why We Performed This Audit

Personal Identity Verification (PIV) cards are used to access GSA buildings and information technology systems. Annually, GSA issues an average of 14,500 PIV cards to contract employees who support GSA's programs and operations. In 2016, the GSA Office of Inspector General's Office of Inspections performed an evaluation of GSA's management of contract employee PIV cards and found several issues related to GSA's recovery and destruction of PIV cards.[1] The issues identified in the Office of Inspections' 2016 evaluation remained a concern for our office, so this audit was included in our *Fiscal Year 2019 Audit Plan*. Our objective was to determine if GSA properly accounts for PIV cards issued to contract employees in accordance with federal regulation, policy, and guidance.

What We Found

GSA is mismanaging PIV cards issued to contract employees. As a result, GSA was unable to account for approximately 15,000 PIV cards issued to contract employees.[2] In addition, GSA failed to collect over half of the 445 PIV cards from contract employees who failed their background checks. GSA's poor management and oversight of these cards raises significant security concerns because the cards can be used to gain unauthorized access to GSA buildings and information systems, placing GSA personnel, federal property, and data at risk.

We identified three factors that are affecting GSA's management of PIV cards for contract employees. First, GSA uses unreliable data to track and monitor PIV cards, which limits its ability to properly account for the cards. Second, GSA does not have formal procedures for recovering PIV cards from contract employees, forcing GSA personnel to use a patchwork of inconsistent and largely ineffective methods for recovering the cards. Lastly, GSA has not implemented the oversight needed to ensure all PIV cards are recovered from contract employees.

[1] *GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Management of Contractor HSPD-12 PIV Cards* (Report Number JE16-002, March 30, 2016).

[2] We previously notified management of the unaccounted-for PIV cards in *Alert Memorandum: GSA Cannot Account for Thousands of Personal Identity Verification Cards Issued to GSA Contract Employees* (Memorandum Number A190085-2, November 22, 2019).

What We Recommend

We recommend that the GSA Deputy Administrator:

1. Continue to take action to account for and collect the PIV cards identified in our audit that remain outstanding by:
   a. Updating the GSA Credential and Identity Management System records for contract employees to ensure that they are accurate;
   b. Terminating and recovering all PIV cards no longer needed by former contract employees; and
   c. Reporting unauthorized cardholders for any PIV cards that cannot be recovered to the U.S. Department of Homeland Security for unauthorized possession of a United States identification card, in compliance with 18 U.S.C., Section 701.

2. Ensure collaboration between Heads of Services and Staff Offices to require enforcement of current policy and implement new policy to account for all PIV cards issued to contract employees by:
   a. Establishing PIV card recovery procedures that include specific steps to take for lost, stolen, and non-returned PIV cards, including withholding final payment if PIV cards are not returned, as outlined in Federal Acquisition Regulation 52.204-9, *Personal Identity Verification of Contractor Personnel*;
   b. Implementing procedures, using the GSA Credential and Identity Management System, that track and monitor GSA's recovery of PIV cards and include communicating the results to the requesting officials and regional leadership;
   c. Requiring training on PIV card issuance and recovery for personnel with responsibilities in the PIV card process;
   d. Coordinating with the U.S. Department of Homeland Security to establish emergency procedures (including when unfit determinations are made) for recovery of contract employee PIV cards, in accordance with Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; and
   e. Implementing the oversight of requesting officials and Office of Mission Assurance personnel to ensure GSA maintains accurate contract employee data in the GSA Credential and Identity Management System and retrieves PIV cards.

GSA agreed with our report finding and recommendations. GSA's comments are included in their entirety in ***Appendix B***.

Table of Contents

Introduction

We performed an audit of GSA's controls over the maintenance of Personal Identity Verification (PIV) cards for contract employees.

Purpose

In 2016, the GSA Office of Inspector General's Office of Inspections performed an evaluation of GSA's management of contract employee PIV cards and found several issues related to GSA's recovery and destruction of PIV cards. The issues identified in the Office of Inspections' 2016 evaluation remained a concern for our office, so this audit was included in our *Fiscal Year 2019 Audit Plan*. This audit focused on GSA's controls over the issuance and recovery of contract employee PIV cards issued after February 1, 2017, when GSA completed the corrective actions taken since the Office of Inspections' 2016 report.

Objective

The objective of our audit was to determine if GSA properly accounts for PIV cards issued to contract employees in accordance with federal regulation, policy, and guidance.

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

Background

The 2004 Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12), mandated the development and implementation of a government-wide standard for secure and reliable forms of identification for federal and contract employees. President George W. Bush issued this directive to increase efficiency, reduce identity fraud, and protect personal privacy. The directive created a federal standard for identification based on specific criteria for verifying an employee's identity that is resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.

On February 25, 2005, the U.S. Department of Commerce's National Institute of Standards and Technology published the Federal Information Processing Standards Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201). FIPS 201-2 (second version of FIPS 201, issued in August 2013) sets standards for implementing identity credentials stored on PIV cards for federal and contract employees.

FIPS 201-2 defines agency requirements for the issuance, maintenance, and termination of PIV cards. It also requires agencies to complete a background investigation prior to issuing a PIV card. In addition, these standards establish when a cardholder is no longer eligible to possess a PIV card, including upon:

- Completion of contractual obligations;
- Cancellation of contract;
- Termination of employment; or
- A failed background check.

When a cardholder is no longer eligible for a PIV card, FIPS 201-2 requires agencies to collect and disable the PIV card. This standard also requires that agencies disable unrecovered cards within 18 hours of notification that the card is unrecovered, unless 18 hours is an unacceptable delay. Agencies must also have procedures in place to issue emergency notifications in cases when 18 hours is unacceptable.

Federal Acquisition Regulation (FAR) 4.13, *Personal Identity Verification*, requires agencies to collect PIV cards as soon as a cardholder is no longer eligible to possess one. Additionally, FAR 4.13 requires the contracting officer to insert FAR 52.204-9, *Personal Identity Verification of Contractor Personnel*, in contracts when contract performance requires contract employees to have routine physical access to a federally controlled facility. FAR 52.204-9 states that the contract vendor shall account for all forms of government-provided identification and return this identification to the issuing agency. It also indicates that the contract vendor's failure to do so may result in the contracting officer delaying final payment.

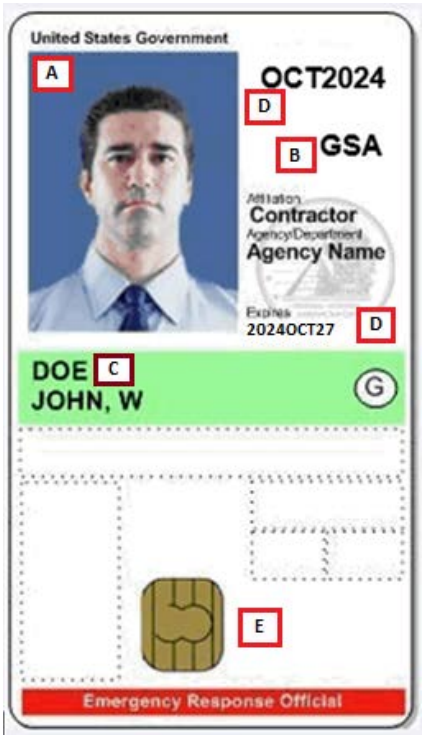
On August 5, 2005, the Office of Management and Budget issued *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*. This guidance provides specific instructions for implementing HSPD-12 and FIPS 201-2. Additionally, it emphasizes the use of an appropriate card authentication mechanism, with minimal reliance on visual authentication to the maximum extent practicable.

Finally, 18 U.S.C., Section 701, *Official badges, identification cards, other insignia*, outlines criminal penalties for anyone who unlawfully possesses a badge or identification card issued by the United States government. This emphasizes the importance of recovering PIV cards when they are no longer valid.

GSA PIV Card Process Overview

Issued in 2008, GSA Order CIO P 2181.1, *Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing*, establishes GSA's PIV card handbook, providing procedures for the PIV card process. This handbook identifies the PIV card as GSA's primary form of identification and mandates its use to authenticate access to physical and information technology (IT) resources in accordance with HSPD-12. *Figure 1* on the following page shows an example of a GSA PIV card.

Figure 1 – Example of a GSA PIV Card



A GSA PIV card primarily includes the following components:

A. Photograph of cardholder;

B. Issuing agency;

C. Cardholder's name;

D. Expiration date — 5 years from the date of issuance; and

E. Embedded chip that can be scanned to verify the authenticity of the card. This acts as an electronic credential.

GSA PIV cards are primarily used to access physically secured federal areas and IT systems through visual authentication or a card reader. Visual authentication relies on a person reviewing the cardholder's photo and expiration date, while a card reader is an electronic means to grant access based on whether a card's electronic credential is active.

GSA's Office of Mission Assurance (OMA) maintains the GSA Credential and Identity Management System (GCIMS) database to manage PIV cards for federal and contract employees. OMA uses this database to track PIV card issuance, electronic credential status, and card recovery.

Roles and responsibilities are assigned to many different participants. GSA Order ADM 5400.2, *General Services Administration Heads of Services and Staff Offices' and Requesting Officials' Roles and Responsibilities to Implement Homeland Security Presidential Directive-12*, defines the roles and responsibilities related to the contract employee PIV card process. The roles and responsibilities in GSA Orders CIO P 2181.1 and ADM 5400.2 are included in *Figure 2* on the following page.

Figure 2 – GSA PIV Card Process Roles and Responsibilities

Role	Responsibilities
GSA Contract Employee	• Provides information for their background investigation • Returns PIV card when no longer required
GSA Contract Vendor	• Initiates the PIV card request for its employees • Provides the GSA requesting official (RO) with any changes to employees working on a contract • Collects PIV cards from its employees when the cards are no longer required • Returns PIV cards to the GSA RO
GSA Contracting Officer	• Authorized to delegate the responsibilities related to PIV card recovery to the contracting officer's representative • Has the ability to withhold payment from the contract vendor for unrecovered PIV cards
GSA RO	• Requests PIV card issuance • Monitors PIV card process from issuance to destruction • Retrieves PIV cards from the contract vendor or contract employee
GSA OMA	• Oversees PIV card process for GSA • Maintains GCIMS • Provides PIV card training manuals • Hosts online training seminars
U.S. Department of Defense	• Conducts background investigations and sends the results to the U.S. Office of Personnel Management (OPM)
OPM	• Conducts adjudication of background investigations • Notifies GSA daily of adjudication results
U.S. Department of Homeland Security's (DHS's) Federal Protective Service	• Works with OMA to ensure the safety and security of GSA buildings
GSA HSPD-12 Managed Service Office (MSO)	• Manages the USAccess Program, which provides the key components necessary to manage the full lifecycle of a PIV credential

The RO is often the contracting officer's representative, project manager, GSA's Public Buildings Service (PBS) building manager, or local HSPD-12 point of contact.

GSA's PIV card approval process. In order to receive a PIV card, a contract employee must be assigned to work on a contract and follow the approval process outlined in *Figure 3.*

Figure 3 – GSA PIV Card Approval Process

PIV Card Approval Process
1. Contract vendor provides a list of its employees to the RO, who then submits it to OMA for review.
2. OMA sends personal information requests to the contract employees listed by the contract vendor.
3. Contract employees provide information to the RO.
4. RO forwards the contract employee's information to OMA.
5. OMA requests the initiation of a background investigation from the U.S. Department of Defense and notifies OPM of initiation.
6. OMA notifies the contract employee, contract vendor, and RO of initial fitness determination, which is based on a preliminary background investigation.
7. MSO prints and ships the PIV card to the desired MSO credentialing office.
8. Contract employee collects and activates their PIV card at the MSO credentialing office.
9. OPM notifies OMA of final fitness determination, which is based on the full background investigation.
10. OMA notifies the contract employee, contract vendor, and RO of the final fitness determination after receiving it from OPM.

GSA Order CIO P 2181.1 requires GSA to initiate background investigations, evaluate fitness determinations from the results, and issue appropriate identity credentials for all of its federal and contract employees who require access to IT systems or routine physical access to its controlled facilities for more than 6 months. A background investigation may consist of a criminal history and fingerprint check, record search, and written inquiries regarding a person's background. Once the background investigation is complete, OPM makes a determination on whether the contract employee is fit to receive a PIV card.

If the contract employee is determined to be unfit, the contract employee cannot work on GSA contracts under any circumstances. OMA would then notify the RO, who is responsible for ensuring that the contract vendor removes the contract employee from the GSA contract and recovering the contract employee's PIV card. The RO would then revoke that employee's GSA credentials and access to GSA IT systems and facilities. Examples of unfit determinations include criminal conduct, employment misconduct, and dishonesty issues.

Previous Office of Inspector General PIV Card Reports

Since 2016, the GSA Office of Inspector General has issued a series of reports identifying concerns with GSA's management of access cards. As previously mentioned, the Office of Inspections issued an evaluation report in March 2016, which found the following:

- GSA does not consistently collect and destroy inactive GSA contract employee PIV cards;
- Contract employees used expired PIV cards to access GSA-managed facilities;
- GSA does not comply with PIV card issuance requirements; and
- GCIMS data is inaccurate and incomplete.

Since the release of the Office of Inspections' evaluation report, our office has highlighted concerns over access card management in our annual assessments of GSA's management and performance challenges.[3] Our assessments reiterated that GSA-managed facilities are at an increased risk of unauthorized access due to mismanagement of access cards and included the following concerns:

- Unauthorized access to federal facilities increases the risk of a security event such as an active shooter, terrorist attack, theft of government property, or exposure of sensitive information;
- Significant deficiencies exist in GSA's process for managing GSA-issued PIV cards to contract employees and for completing contract employee background investigations;
- Deficiencies exist in GSA's tracking and maintenance of contract employee background investigation data stored within GCIMS; and
- GSA does not have adequate controls over access cards and cannot determine the extent of their associated security risks because it does not centrally monitor the management of these cards.

In response to these assessments, GSA agreed to address vulnerabilities associated with building-specific facility access cards and PIV cards.

During the course of this audit, we discovered that GSA could not account for nearly 15,000 contract employee PIV cards. Due to the serious security risks raised by these unaccounted-for PIV cards, our office issued an alert memorandum to the GSA Deputy Administrator on November 22, 2019. We issued this memorandum to inform GSA of this matter and to enable management to take immediate action to account for these PIV cards.

On January 21, 2020, the GSA Deputy Administrator responded to our memorandum, stating that GSA's OMA is actively working with all GSA's Services and Staff Offices to review and accurately update the status of all active contract employees.

[3] Assessment of GSA's Major Management Challenges for Fiscal Years 2017, 2018, 2019, and 2020.

Results

GSA is mismanaging PIV cards issued to contract employees. As a result, GSA was unable to account for approximately 15,000 PIV cards issued to contract employees. In addition, GSA failed to collect over half of the 445 PIV cards from contract employees who failed their background checks. GSA's poor management and oversight of these cards raises significant security concerns because the cards can be used to gain unauthorized access to GSA buildings and information systems, placing GSA personnel, federal property, and data at risk.

We identified three factors that are affecting GSA's management of PIV cards for contract employees. First, GSA uses unreliable data to track and monitor PIV cards, which limits its ability to properly account for the cards. Second, GSA does not have formal procedures for recovering PIV cards from contract employees, forcing GSA personnel to use a patchwork of inconsistent and largely ineffective methods for recovering the cards. Lastly, GSA has not implemented the oversight needed to ensure all PIV cards are recovered from contract employees.

Finding – GSA's mismanagement of contract employee PIV cards places GSA personnel, federal property, and data at risk.

GSA is mismanaging PIV cards issued to contract employees due to incomplete GCIMS data, lack of procedures for recovering cards, and a lack of oversight. As a result, GSA cannot account for thousands of PIV cards issued to contract employees and failed to collect hundreds of PIV cards from contract employees who failed background checks. This raises serious concerns because these cards could be used to gain unauthorized access to GSA buildings or IT systems, placing GSA personnel, federal property, and data at risk.

FAR 4.13 requires that agencies collect PIV cards if the contract vendor has removed the contract employee from the contract, the contract is terminated, or the contract is completed. GSA activated 39,090 contract employee PIV cards during our audit period (February 1, 2017, through August 31, 2019). Based on our review of GCIMS data, GSA cannot account for 14,928 (38 percent) of these cards. These cards are unaccounted for despite the fact that 2,122 of the cards are for contract employees who were removed from the contracts they were working on. The remaining 12,806 cards are related to contracts that are now expired. GSA should have collected these cards when the contract ended unless the contract employee was assigned to a new contract and the data in GCIMS was updated with the new contract number.

Moreover, as shown in *Figure 4* on the following page, the GCIMS data showed that 10,820 of the 14,928 (72 percent) PIV cards that GSA cannot account for still have an active electronic credential. This means that a contract employee who is no longer authorized to gain access to GSA buildings and IT systems could still gain access, even if those buildings and systems are secured by electronic card readers.

Figure 4 – Unaccounted-For Contract Employee PIV Cards

Contract Employee Status	Total Unaccounted-For	Credential Remains Active	Credential Terminated
Contract Expired	12,806	10,370	2,436
Removed from Contract	2,122	450	1,672
Totals:	**14,928**	**10,820**	**4,108**

An OMA official told us that the electronic credentials were deactivated for the 450 PIV cards associated with contract employees who were removed from their contracts, but that the GCIMS data OMA originally provided us did not reflect the correct information. While we confirmed that the credentials for all 450 PIV cards were terminated, these cards remain unaccounted for. If uncollected, these cards could be used to gain unauthorized physical access to buildings that are not secured with a card reader.

As previously noted, we alerted the GSA Deputy Administrator of these unaccounted-for PIV cards in a November 2019 audit memorandum. In her January 2020 response, the GSA Deputy Administrator stated that the Agency is taking action to address the unaccounted-for cards, which included:

- Working with Services and Staff Offices to review and update the status for all contract employees listed as active in the GCIMS database;
- Recovering and destroying PIV cards for contract employees no longer working on an active GSA contract; and
- Deactivating the electronic credential on all expired PIV cards.

However, as of July 16, 2020, the total number of unaccounted-for PIV cards remained significant, with 12,814 PIV cards still unaccounted for.

During the audit period, we also found that 445 active contract employees received unfit final determinations on their background checks. However, GSA did not collect 264 (59 percent) of the PIV cards issued to these unfit contract employees. We requested additional information regarding the unfit determinations for a random sample of 25 of the 264 unrecovered PIV cards. From that sample, the majority of unfit determinations were due to "dishonesty issues"; one unfit determination was due to "criminal conduct."

FIPS 201-2 requires that agencies terminate PIV cards if a background investigation determines that the cardholder should not have a PIV card. In these cases, FIPS 201-2 further requires that agencies collect and destroy the card; update any databases maintained by the card issuer to reflect the change; and, if the card cannot be recovered and destroyed, disable the card's

electronic credential. According to the data in GCIMS, of the 264 unrecovered PIV cards, 29 (11 percent) still had an active electronic credential; this means that 29 cardholders deemed unfit to access GSA areas and IT systems may have unauthorized access to these areas and systems even if they are secured by a card reader. An OMA official told us that the electronic credentials for these 29 PIV cards were terminated, but asserted that the GCIMS data originally provided to us did not reflect the correct information. We verified that the credentials for all 29 PIV cards were terminated. Nonetheless, all 264 unrecovered PIV cards may still allow for unauthorized physical access to buildings that are not secured with a card reader.

This raises serious security concerns because [redacted][4]

We found that the following factors contributed to GSA's inability to account for the approximately 15,000 contract employee PIV cards:

- GSA's ability to track PIV cards is limited by unreliable GCIMS data;
- GSA does not have adequate procedures for recovering PIV cards; and
- GSA has not implemented the necessary oversight to ensure PIV cards are recovered from contract employees.

These deficiencies are discussed in detail below.

Unreliable GCIMS Data Continues to Limit GSA's Ability to Track PIV Cards

As noted in the *Background* section of this report, our office identified concerns about the accuracy and reliability of PIV card data in GCIMS in 2016. We found that GCIMS continues to contain inaccurate and incomplete data. In addition to the unaccounted-for PIV cards, RO contact information in GCIMS was outdated or input incorrectly. In some instances, the ROs listed in GCIMS no longer worked on the subject contracts; in one instance, the RO no longer worked for GSA.

GSA employees confirmed the data inaccuracies. For example, one RO stated that while she attempted to verify the status of the PIV cards she was responsible for, she found the GCIMS data highly erroneous. An OMA official told us that GCIMS needs to be completely overhauled because it contains information that has been incorrect for years. Additionally, in the GSA Deputy Administrator's January 2020 response to our alert memorandum, she stated that GSA also found inaccuracies in the GCIMS data.

[4] Redactions in this report represent sensitive information related to federal security.

GCIMS data is primarily manually entered by OMA, with input from several different stakeholders in GSA's PIV card process. GSA contract employees and contract vendors are responsible for providing updated information to ROs. ROs are then responsible for relaying that information to OMA, which is responsible for entering, updating, and maintaining the information in GCIMS.

At the start of our audit, an OMA official told us that OMA had done a lot of work since the Office of Inspections' 2016 evaluation, and that we would not have much to report on. OMA also told us that they sent periodic reports to PBS indicating active contract employees on expired or soon-to-expire contracts. Nonetheless, GCIMS continues to contain invalid or missing data for a number of data fields.

For example, OMA acknowledged that the contract number data field often contains inaccurate data. This data field is critical because contract employee PIV cards are tied to a specific contract number when issued for tracking purposes. When this field contains inaccurate data, it is difficult to determine whether the PIV card holder is associated with an active GSA contract.

We also found examples of unreliable data critical for ensuring proper oversight of PIV cards issued to contract employees. Specifically, as of July 16, 2020, we found that 89,926 of the 277,588 (32 percent) of contract employee records in GCIMS contained incomplete or inaccurate data in at least one of the key data fields described below.

- *Job Title* – This field is integral for contract management and tracking purposes. It typically contains the general job a contract employee will perform. However, we found that contract employee records contained incomplete and inaccurate data for this field, including 49,927 blank data fields, as well as phone numbers instead of appropriate job titles.

- *GSA Point of Contact* – This field typically includes the name and email address of the GSA employee who is responsible for overseeing a contract employee's PIV card. Accordingly, it is vital for identifying who to contact if a PIV card should be collected, GCIMS data updated, or other administrative actions taken. However, this field included outdated information, including GSA Points of Contact who no longer worked for GSA or served in the role of an RO. Additionally, we found that a GSA Point of Contact was not listed for 54,892 contract employee records.

- *Vendor Point of Contact* – This field typically includes a contract vendor's name and email address. It is a key field used to determine who to contact if a contract employee's PIV card should be collected or to verify if a cardholder is still working on a contract. Similar to the GSA Point of Contact entries, we often found the data in this field was inaccurate and incomplete. For example, we found that a Vendor Point of Contact was not listed for 53,290 contract employee records.

When we brought these data issues to OMA's attention, they acknowledged the data inaccuracies and told us that they want a better way of managing the data. During the audit, OMA launched a Contract Dashboard to allow ROs to track the status of PIV cards assigned to them. The dashboard is fed with GCIMS information. While many ROs told us they believed this tool would help them manage their PIV cards, the effectiveness of the dashboard will likely be limited until the information in GCIMS is complete, accurate, and reliable.

GSA should establish procedures to review and update the contract employee records in GCIMS to ensure that they are accurate. In addition, GSA should implement procedures using GCIMS that track and monitor the recovery of PIV cards.

GSA Does Not Have Adequate PIV Card Recovery Procedures

PIV cards are used to access federal buildings and data systems. To protect federal personnel, property, and data, it is imperative that agencies establish clear and comprehensive procedures to recover cards after they are no longer needed. However, we found that GSA does not have adequate procedures in place for recovering cards from contract employees.

Federal regulations and GSA policy reflect the importance of recovering PIV cards in a timely manner. For example, FAR 4.13 requires that agencies collect PIV cards as soon as they are no longer needed. FIPS 201-2 requires agencies to establish procedures for emergency situations so PIV cards can be rapidly terminated and recovered. Additionally, GSA Order CIO P 2181.1 requires the contract employee to return PIV cards to the RO at the end of the project or immediately when a contract employee separates before contract completion. The RO is then responsible for returning the cards to OMA for destruction.

However, we found minimal guidance and no specific instructions on how ROs and contract vendors should recover and account for PIV cards, including in emergency situations. While OMA periodically sends out lists of some unaccounted-for PIV cards to PBS regional offices, we were told that the listings do not include clear instructions or guidance. Interviews with ROs and contract vendors, coupled with analysis of existing GCIMS data, showed that GSA's lack of procedures has left ROs and contract vendors uncertain of the steps they should take to recover and account for PIV cards.

In the absence of a formal PIV card recovery process, we found that ROs resorted to a variety of methods to track and retrieve issued PIV cards. Some examples include:

- *Developing a spreadsheet to track contract employee PIV cards* – One RO advised us she uses a spreadsheet to keep track of the PIV cards she manages and mails any recovered PIV cards to OMA. Of the 237 PIV cards assigned to this RO, 40 (17 percent) were unaccounted for.

- *Relying on card issuance forms sent to OMA to track contract employee PIV cards* – Another RO kept track of PIV cards by using the forms submitted to OMA to request a

PIV card. This RO told us she waits until she recovers many PIV cards before returning them in bulk to OMA. Of the 136 PIV cards assigned to this RO, 51 (38 percent) were unaccounted for.

- *Relying on the contract vendor to turn in a PIV card* – An additional RO told us he does not track contract employee PIV cards. Instead, he waits for the contract vendors or OMA to tell him to collect a PIV card. He estimated that contract vendors only return around 30 percent of PIV cards after a project is completed. Of the 719 PIV cards assigned to this RO, 485 (67 percent) were unaccounted for.

All three of these ROs told us they would benefit from some sort of formalized PIV card recovery procedures. The issue of PIV card recovery is often complicated and involves too many different parties for ROs to manage alone.

Most ROs we spoke with were unaware of the procedures to follow when a contract employee receives an unfit determination. OMA officials told us that when contract employees receive unfit determinations, ROs receive automated email notifications that include instructions to return all credentials and access cards to OMA.

Nonetheless, OMA officials acknowledged that PIV cards are often not returned after unfit determinations. One OMA official told us that OMA does not collaborate with ROs to track PIV cards with unfit determinations because that is the ROs' responsibility. She added that OMA would be willing to participate in the recovery of these cards if invited to do so; however, she also told us that OMA may not be adequately staffed to handle additional responsibilities.

In addition to the lack of a formal PIV card recovery process, none of the ROs we asked knew of any procedures in place for the recovery of contract employee PIV cards in emergency situations. For example, in the event that GSA has to remove a potentially dangerous contract employee from the building and recover their PIV card, it is required to have emergency procedures in place. ROs we interviewed responded inconsistently on how they should react to emergency situations. Some ROs stated that they would take it upon themselves to make DHS's Federal Protective Service aware of PIV-card-related emergencies; others told us that they would rely on building management for these emergencies.

In developing and implementing clear PIV card recovery procedures, GSA should include specific procedures for recovering PIV cards from construction contract employees. During our testing, ROs and contract officials voiced particular frustration with the difficulty of recovering cards for construction contracts. Based on our interviews, we learned that construction contracts experience high turnover, regular loss of contact with contract employees, and contract employees working on multiple contracts.

GSA Has Not Implemented Necessary Oversight to Ensure PIV Cards Are Recovered from Contract Employees

Oversight is integral to ensuring that an organization is operating effectively and meeting its objectives. However, we found that GSA has not implemented the oversight needed to ensure PIV cards are recovered from contract employees.

GSA's ability to recover PIV cards is significantly impaired because GSA does not have the oversight in place to ensure it effectively recovers PIV cards from contract employees. Under the current process, OMA periodically compiles and sends lists of unaccounted-for PIV cards to regional PBS officials for review. Due to the GCIMS data inaccuracies discussed previously in this *Finding*, OMA is unable to pull complete and reliable lists of unaccounted-for cards, forcing it to send incomplete and erroneous lists for review. While OMA sends these lists on a regular basis to regional PBS officials, we were told that the lists do not get distributed to the ROs consistently. Finally, OMA does not include clear instructions detailing requirements for review of the lists and timeframes for reporting results back to OMA. Many of the ROs we interviewed told us that they did not get the lists. We were informed by an OMA official that after OMA distributes the lists, there is no follow-up to ensure ROs take steps to recover the PIV cards.

In addition, GSA is not providing the necessary oversight to ensure that ROs and OMA personnel fulfill their responsibilities to recover PIV cards from contract employees. While OMA has overall responsibility for GSA's PIV card program, GSA places the responsibility on ROs to recover PIV cards from contract employees. However, we found that GSA does not have effective oversight measures in place to ensure these personnel are actively working to recover PIV cards. For example, GSA's existing performance standards for ROs and OMA personnel do not specifically focus on recovering PIV cards from contract employees and maintaining accurate contract employee data in GCIMS. Without oversight to ensure employees are fulfilling their duties, employees may be less likely to know what is required of them or understand the importance of their responsibility.

Lastly, GSA does not have effective oversight of training procedures for personnel involved in the PIV card process. While GSA does offer some PIV card training classes, they are not required of personnel who issue and recover PIV cards. An OMA official told us that GSA does not document when personnel have attended these PIV card trainings. Increased oversight of the training process should ensure that GSA personnel are receiving the knowledge they need to properly issue and recover PIV cards.

Oversight is needed to ensure that ROs and OMA personnel obtain complete PIV card data, have clear performance expectations, and are appropriately supervised to ensure that GSA tracks and recovers contract employee PIV cards. Therefore, GSA should implement the oversight necessary to ensure that ROs and OMA personnel fulfill their responsibilities and GSA effectively recovers PIV cards from contract employees.

In sum, GSA's poor management and oversight of PIV cards for contract employees pose significant security risks that may result in unauthorized access to GSA buildings or IT systems. We found that GSA is not maintaining reliable data to track and monitor PIV cards in GCIMS, has not established adequate PIV card recovery procedures, and is not providing the necessary oversight to ensure the recovery of PIV cards. Taken together, these weaknesses place GSA personnel, federal property, and data at risk.

Conclusion

GSA is mismanaging PIV cards issued to contract employees. As a result, GSA was unable to account for approximately 15,000 PIV cards issued to contract employees. In addition, GSA failed to collect over half of the 445 PIV cards from contract employees who failed their background checks. GSA's poor management and oversight of these cards raises significant security concerns because the cards can be used to gain unauthorized access to GSA buildings and information systems, placing GSA personnel, federal property, and data at risk.

We identified three factors that are affecting GSA's management of PIV cards for contract employees. First, GSA uses unreliable data to track and monitor PIV cards, which limits its ability to properly account for the cards. Second, GSA does not have formal procedures for recovering PIV cards from contract employees, forcing GSA personnel to use a patchwork of inconsistent and largely ineffective methods for recovering the cards. Lastly, GSA has not implemented the oversight needed to ensure all PIV cards are recovered from contract employees.

In response to our November 2019 alert memorandum, the GSA Deputy Administrator stated that the Agency has initiated steps to address the unaccounted-for contract employee PIV cards. As part of this effort, OMA is contacting ROs to update the status of contract employees who are still working on active GSA contracts. In addition, ROs will initiate the PIV card recovery for contract employees no longer working on active GSA contracts.

While these are positive steps, GSA needs to address the issues identified in our report that have allowed for so many unaccounted-for PIV cards and unrecovered cards from ineligible cardholders. In addition to accounting for the remaining PIV cards, GSA should establish PIV card recovery procedures, require training, establish emergency card recovery procedures, and implement necessary oversight related to PIV card recovery.

Recommendations

We recommend that the GSA Deputy Administrator:

1. Continue to take action to account for and collect the PIV cards identified in our audit that remain outstanding by:
    a. Updating the GCIMS records for contract employees to ensure that they are accurate;
    b. Terminating and recovering all PIV cards no longer needed by former contract employees; and
    c. Reporting unauthorized cardholders for any PIV cards that cannot be recovered to DHS for unauthorized possession of a United States identification card, in compliance with 18 U.S.C., Section 701.

2. Ensure collaboration between Heads of Services and Staff Offices to require enforcement of current policy and implement new policy to account for all PIV cards issued to contract employees by:
    a. Establishing PIV card recovery procedures that include specific steps to take for lost, stolen, and non-returned PIV cards, including withholding final payment if PIV cards are not returned, as outlined in FAR 52.204-9, *Personal Identity Verification of Contractor Personnel*;
    b. Implementing procedures, using the GCIMS, that track and monitor GSA's recovery of PIV cards and include communicating the results to the ROs and regional leadership;
    c. Requiring training on PIV card issuance and recovery for personnel with responsibilities in the PIV card process;
    d. Coordinating with DHS to establish emergency procedures (including when unfit determinations are made) for recovery of contract employee PIV cards, in accordance with FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; and
    e. Implementing the oversight of ROs and OMA personnel to ensure GSA maintains accurate contract employee data in the GCIMS and retrieves PIV cards.

GSA Comments

GSA agreed with our report finding and recommendations. GSA's comments are included in their entirety in ***Appendix B***.

Audit Team

This audit was managed out of the Heartland Region Audit Office and conducted by the individuals listed below:

Michelle Westrup	Regional Inspector General for Auditing
David Garcia	Audit Manager
Daniel Riggs	Auditor-In-Charge
Andrew Kehoe	Auditor

Appendix A – Scope and Methodology

This audit was included in our *Fiscal Year 2019 Audit Plan*. The audit focused on GSA's controls over the maintenance of PIV cards for contract employees.

To accomplish our objective, we:

- Reviewed federal regulations and policies, as well as GSA policies, procedures, and training materials related to the issuance and recovery of PIV cards;
- Analyzed GCIMS data as of September 6, 2019, for our audit period of February 1, 2017, through August 31, 2019, which consisted of 39,090 PIV cards issued to GSA contract employees;
- Analyzed updated GCIMS data as of July 16, 2020;
- Assessed the GCIMS data reliability and validity through GSA interviews, data analysis, and OPM inquiries;
- Selected a judgmental sample of 12 of the 1,498 buildings where contract employees were assigned PIV cards during our audit period. The PIV cards assigned to this sample of buildings account for 15 percent of the 39,090 contract employee PIV card records; and
- Conducted security testing and interviewed GSA personnel at the 12 sample buildings.

Additionally, we tested the following internal control components, which were relevant to our objective, by assessing:

- *Control activities*. We analyzed data and conducted interviews to see if GSA is deactivating PIV cards when they are no longer needed;
- *Information and communication.* We conducted interviews of 15 ROs to verify if GSA is communicating information to those who require it for the implementation of the contract employee PIV card process; and
- *Monitoring*. We evaluated monitoring activities to verify if GSA personnel are using the information available to them to deactivate and retrieve PIV cards from contract employees.

We conducted the audit between July 2019 and July 2020 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 finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Internal Controls

We determined that internal controls were significant to our audit objective. Accordingly, we assessed the design, implementation, and operating effectiveness of internal controls. The methodology above describes the scope of our assessment and the report finding includes any internal control deficiencies we identified.

Appendix B – GSA Comments

Deputy Administrator

October 16, 2020

MEMORANDUM FOR MICHELLE L. WESTRUP
REGIONAL INSPECTOR GENERAL FOR AUDITING
HEARTLAND REGION AUDIT OFFICE (JA-6)

FROM: ALLISON F. BRIGATI
DEPUTY ADMINISTRATOR (AD)

SUBJECT: Response to the Office of Inspector General (OIG) Draft Audit Report, *GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk* (A190085)

Thank you for the opportunity to comment on the subject draft audit report. GSA has reviewed the report and agrees with the findings and recommendations.

GSA has already started to take steps to address a number of the findings and recommendations in the draft audit report, including the following steps:

- On September 30, 2019, GSA created a contract dashboard to help track and monitor contracts and contractors throughout the Personal Identification Verification (PIV) card lifecycle. On February 2, 2020, GSA created an automated email notification to requesting officials 60 days, 30 days, and 0 days from the contract end date. These notifications will remind requesting officials to identify when contracts for which they are responsible end and take the necessary steps needed for closing out the contracts and retrieving PIV cards.

- Beginning January 30, 2020, GSA established a working group with stakeholders from across the Services and Staff Offices that routinely meet to ensure contract and contractor data is accurate and up-to-date. As a result, GSA has developed three contractor PIV card process flowcharts and finalized content for a mandatory GSA-wide Homeland Security Presidential Directive (HSPD)-12/PIV card training for the acquisition workforce.

- On February 12, 2020, I signed a memorandum directing GSA's Heads of Services and Staff Offices (HSSOs) to strengthen PIV card management by assigning specific roles and responsibilities and establishing oversight mechanisms to ensure accountability.

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

- On September 1, 2020, GSA's Chief Acquisition Officer and the Acting Chief Human Capital Officer issued Memorandum MV-55, a joint policy memo to improve contract administration in GSA. The memo establishes a new mandatory standard (acquisition-related) critical element in all performance plans for GSA Contracting Officer Representatives (CORs) on active delegation. This memo will serve as a baseline effort to ensure that GSA requesting officials have the proper training with respect to their duties for managing PIV cards, that they are held accountable for those duties, and that management is aware of the related workload.
- On September 18, 2020, GSA updated internal resources for GSA acquisition professionals to identify all existing policies and resources related to PIV card management on the Acquisition Portal.

From November 2019 through March 2020, all GSA HSSOs worked closely with the Office of Mission Assurance (OMA) to remediate the issues raised in the November 22, 2019, OIG Alert Memo. In the Public Buildings Service (PBS), the Office of Acquisition Management has placed process improvement and PIV card retrieval as a top priority to ensure proper management and oversight of all PIV cards. PBS worked closely with PBS requesting officials to ensure all 37,000 contractor PIV card entries attached to 5,700 PBS contracts in the GSA Credential and Identity Management System (GCIMS) associated with the November 22, 2019, OIG Alert Memo were properly assigned to an active, valid contract. Contractor PIV cards listed as "active" but associated with expired contracts that could not be updated or assigned to an active, valid contract were collected and destroyed, or made "inactive" in GCIMS. IT credentials for all collected, destroyed, and "uncollected" contractor PIV cards were terminated. PBS sent automated, standardized letters to 3,900 contractors, some of which had multiple outstanding PIV cards, requesting that they arrange for the immediate return of expired and "uncollected" PIV cards to requesting officials. PBS addressed the remaining 1,700 contracts with expired data by updating contract completion dates using the Contactor Information Worksheet and submitting the information to OMA.

A national effort is ongoing to collect outstanding PIV cards, have contractors provide updates on the status of outstanding PIV cards, and notify GSA and vendor POCs of expiring information in GCIMS. To support these efforts, a working group with Service and Staff Office stakeholders was established that routinely meets to discuss short- and long-term initiatives to improve PIV card tracking and ensure contract and contractor data is accurate and up-to-date through monthly reporting to OMA. Measures are being implemented that GSA is confident will streamline the management, retrieval, and reassignment to active, valid contracts of PIV cards while improving data collection.

For the Federal Acquisition Service (FAS), the Office of Policy and Compliance worked closely with all FAS portfolio requesting officials to ensure all 388 FAS contractor PIV card entries in GCIMS associated with the November 22, 2019, OIG Alert Memo were properly assigned to an active, valid contract. Contractor PIV cards listed as "active" but associated with expired contracts that could not be updated or assigned to an active, valid contract were collected and destroyed, or made "inactive" in GCIMS. IT credentials

for all collected, destroyed, and "uncollected" contractor PIV cards were terminated. FAS also sent automated, standardized letters to contractors requesting they arrange for the immediate return of expired and "uncollected" PIV cards to requesting officials. FAS has also published a new Policy and Procedure, 2020-03, *FAS Contracting Officer's Representative Function Standard Operating Procedures*, to ensure consistency in COR execution of HSPD-12 functions and contractor PIV card oversight.

GSA has a number of additional actions planned for fiscal year 2021 and looks forward to working with the OIG to discuss these plans going forward. If you have any questions, please contact Robert J. Carter, Associate Administrator, Office of Mission Assurance, at 202-604-3412.

Attachment: Signed GSA Response to OIG Alert Memo A190085-2

Deputy Administrator

January 21, 2020

MEMORANDUM FOR R. NICHOLAS GOCO
ASSISTANT INSPECTOR GENERAL FOR AUDITING (JA)

FROM: ALLISON FAHRENKOPF BRIGATI
DEPUTY ADMINISTRATOR (AD)

SUBJECT: Response to Alert Memorandum: *GSA Cannot Account for Thousands of Personal Identity Verification Cards Issued to GSA Contract Employees* (A190085-2)

This is in response to the November 22, 2019, Alert Memorandum: *GSA Cannot Account for Thousands of Personal Identity Verification Cards Issued to GSA Contract Employees.*

GSA's Office of Mission Assurance (OMA) is actively working with Contracting Officers/Contracting Officer Representatives (COs/CORs) from all Services and Staff Offices to review and update the status for all contractors listed as "active" in the GSA Credential and Identity Management System (GCIMS) database. Research has determined that some contracts listed as "active" in the database have expired and/or are past the reported period of work. As such, OMA has broken down the data by Service or Staff Office to review and accurately update. The appropriate GSA Requesting Officials are already reviewing the data to determine whether the accurate contract and contractor status is listed in GCIMS. Once a determination has been made for each contract/contractor, the decision will be sent to OMA for processing the GCIMS update and additional action if appropriate.

For contractors determined to be working on an active GSA contract, the CO/COR will submit a new Contractor Information Worksheet to OMA to update the status in GCIMS. For contractors determined to no longer be working on an active GSA contract, the necessary Service or Staff Office will notify OMA and the CO/COR will contact the vendor to initiate the recovery of the Personal Identity Verification (PIV) card. Once returned to OMA, the PIV cards will be destroyed. Finally, OMA will immediately deactivate any electronic certificates on all expired PIV cards, which will prevent them from being used to access any electronic physical access control system infrastructure or Government IT systems.

All GSA Services and Staff Offices are still working to complete this review. GSA will notify the Office of Inspector General upon completion of this review and recovery effort, as well as GSA's efforts to establish additional controls to account for PIV cards in the future. In the meantime, please do not hesitate to contact me with any questions or concerns.

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Appendix C – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

PBS Commissioner (P)

PBS Deputy Commissioner (PD)

PBS Chief of Staff (PB)

PBS Deputy Chief of Staff (PB)

FAS Commissioner (Q)

FAS Deputy Commissioner (Q1)

FAS Chief of Staff (Q0A)

Associate Administrator for Mission Assurance (D)

Deputy Associate Administrator for Mission Assurance (D1)

Chief of Staff for Mission Assurance (D2)

Chief Administrative Services Officer (H)

Audit Management Division (H1EB)

Assistant Inspector General for Auditing (JA)

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