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

Alert Memorandum: GSA Cannot Account for Thousands of Personal Identity Verification Cards Issued to GSA Contract Employees

Memorandum Number A190085-2
November 22, 2019

NOTICE

THE OFFICE OF INSPECTOR GENERAL PREVIOUSLY ISSUED A RESTRICTED VERSION OF THIS MEMORANDUM ON NOVEMBER 22, 2019. THIS MEMORANDUM IS BEING PUBLICLY DISSEMINATED WITHOUT RESTRICTIONS.

November 22, 2019

TO: ALLISON F. BRIGATI
DEPUTY ADMINISTRATOR (AD)

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

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

The purpose of this memorandum is to inform you that GSA cannot account for approximately 15,000 Personal Identity Verification (PIV) cards issued to contract employees. This raises serious security concerns because these cards could be used to gain unauthorized access to GSA buildings or information technology (IT) systems, placing GSA personnel, federal property, and data at risk. GSA management should take immediate action to account for these cards.

Background

The 2004 Homeland Security Presidential Directive 12 (HSPD-12) mandated the development and implementation of a government-wide standard for secure and reliable forms of identification for federal and contract employees. To implement this policy, GSA's Office of Mission Assurance (OMA) established the HSPD-12 Branch to oversee identity, credential, and access card management for GSA.

The PIV card is the primary form of identification used within GSA. The PIV card includes a photo and lists the issuing agency, cardholder's name, and an expiration date—5 years from the date of issuance. Each card also has an embedded chip that can be scanned as an electronic credential to verify the authenticity of the card.

PIV cards are primarily used to access physically secured areas through visual authentication or a card reader. Visual authentication relies on a human guard to determine if the cardholder should be allowed into a secured area. A card reader is an electronic means to grant access based on whether a card's electronic credential is active. The electronic credential, when active, allows cardholders to access select physically secured areas and IT systems.

To track and monitor PIV card issuance, electronic credential status, and card collection, OMA maintains the GSA Credential and Identity Management System (GCIMS). As of August 2019, GCIMS included records for 91,072 cardholders, 70,845 of whom were GSA contract employees.

Any new PIV card applications, updates, and terminations are manually updated in the GCIMS database by one of OMA's five zonal help desks. GSA contracting officers are responsible for providing the OMA help desk with the GSA contract employee PIV card applications, as well as any updates to an existing cardholder's status. Contracting officers typically assign these duties to a contracting officer's representative, who assists in overseeing the day-to-day performance of a particular contract. The contracting officer or contracting officer's representative manages the closeout of expiring contracts, which includes accounting for contract employees' PIV cards.

In 2016, the GSA OIG's Office of Inspections issued an evaluation report on GSA's management of contractor PIV cards that found:[1]

- 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.

In July 2019, we initiated an audit of GSA's controls over the maintenance of access cards for contract employees. This audit is focused on PIV cards issued after February 1, 2017, when GSA completed its corrective actions taken as a result of the Office of Inspections' 2016 report.

GSA cannot account for thousands of PIV cards issued to GSA contract employees.

GSA activated 39,090 contract employee PIV cards between February 1, 2017, and August 31, 2019; however, according to GCIMS data, GSA cannot account for 14,928 (38 percent) of these cards. PIV cards can be used to gain unauthorized access to federal buildings, leased federal offices, and GSA IT systems. This presents a significant security risk to GSA personnel, federal property, and data.

Federal Acquisition Regulation 4.13, *Personal Identity Verification*, requires that agencies collect PIV cards as soon as a cardholder's employment ends, the contract they work under is terminated, or the contract is completed. Additionally, Federal Information Processing Standard 201-2 2.9.4, *PIV Card Termination Requirements*, requires that agencies terminate PIV cards, by disabling the electronic credential, when the agency determines that the cardholder is no longer eligible for a PIV card. This standard also requires that agencies terminate uncollected cards within 18 hours of notification that the card is uncollected.

[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).

To properly account for the PIV cards, GSA should have collected the cards, reported the cards missing, or updated GCIMS to show that the cardholder is working on an active contract. Additionally, GSA should have terminated the electronic credential for any card that remained uncollected.

However, the data in GCIMS indicates that GSA has not taken these actions. As detailed in *Figure 1,* GCIMS indicates that 14,928 PIV cards for contract employees are unaccounted for, including 10,820 with an active electronic credential.

Figure 1 – Unaccounted For Contract Employee PIV Cards

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

These PIV cards are a significant risk to the government. A cardholder with an uncollected PIV card with an active electronic credential may be able to obtain unauthorized access to secure federal buildings and IT systems. Likewise, a cardholder using an uncollected card with a terminated electronic credential could obtain unauthorized physical access to federal buildings that rely on visual authentication at building entrances.

Conclusion

We found that GSA could not account for 14,928 PIV cards issued to GSA contract employees. These cards can be used to gain unauthorized access to federal buildings, leased federal offices, and GSA IT systems. This presents a significant security risk to GSA personnel, federal buildings, and data. Accordingly, GSA management should take immediate action to account for these PIV cards and establish controls to ensure that PIV cards are properly accounted for.

Audit Team

This assignment is being 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

Memorandum Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Commissioner, PBS (P)

Acting Commissioner, FAS (Q)

Associate Administrator, Office of Mission Assurance (D)

Acting FAS Chief of Staff (Q0A)

Acting PBS Chief of Staff (WPB)

PBS Audit Liaison (PT)

Chief Administrative Services Officer (H)

Audit Management Division (H1EB)

Assistant Inspector General for Auditing (JA)

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