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

GSA Is Not Monitoring Data from Access Card Readers to Identify Risks to GSA Personnel and Federal Property

Report Number A210069/P/6/R23005
February 21, 2023

Executive Summary

GSA Is Not Monitoring Data from Access Card Readers to Identify Risks to GSA Personnel and Federal Property

Report Number A210069/P/6/R23005
February 21, 2023

Why We Performed This Audit

GSA access cards are used to access GSA-managed facilities and information technology systems. On November 4, 2020, our office issued an audit report on GSA's management of contract employee access cards that detailed findings related to the recovery and tracking of access cards.[1] During the course of that audit, our office was informed that GSA personnel inappropriately shared their access cards with individuals who did not possess a valid credential of their own to give those individuals access to secured space. We included this audit in our *Fiscal Year 2021 Audit Plan* to determine if GSA is monitoring access card use for physical access to GSA-managed facilities in accordance with federal regulations, policies, and guidance.

What We Found

GSA is not monitoring access card data from GSA card readers to identify risks to GSA personnel and federal property. For the 2-year audit period ended February 28, 2022, data collected from access card readers in GSA-managed facilities showed 32,179 failed access attempts. Failed access attempts could be an indication of attempted unauthorized access to federal facilities and secured areas. Federal guidance on access cards and electronic physical access control systems recommends monitoring access card activity to assess the risk and determine if additional oversight is needed. However, we found that GSA is not actively using data collected from access card readers to identify and assess the risks to its personnel and federal property.

What We Recommend

We recommend that the GSA Administrator:

1. Develop and implement procedures for monitoring access card data to identify repeated, failed access attempts that require follow up.
2. Use the access card data that is being collected to produce trend data to inform building security stakeholders of individuals with a significant number of failed attempts over a specified period of time.
3. Create and disseminate guidance addressing how building security stakeholders should handle repeated, failed access attempts.

The GSA Administrator agreed with our recommendations and provided general comments on the timing of our audit. These comments did not affect our finding and conclusions. GSA's written comments are included in their entirety in ***Appendix B***.

[1] *GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk* (Report Number A190085/A/6/F21001).

Table of Contents

Introduction

We performed an audit of GSA's monitoring of access card use for physical access to GSA-managed facilities.

Purpose

We included this audit in our *Fiscal Year 2021 Audit Plan* because the misuse of access cards remains a concern for our office. We focused on GSA's monitoring of access card use for physical access to GSA-managed facilities for the 2-year audit period ended February 28, 2022.

Objective

The objective of our audit was to determine if GSA is monitoring access card use for physical access to GSA-managed facilities in accordance with federal regulations, policies, and guidance.

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

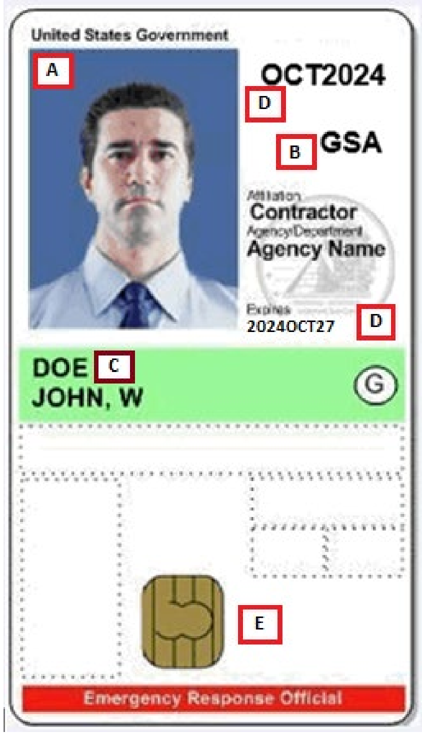
Background

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12), was issued August 27, 2004, mandating 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.

GSA Access Cards

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

Figure 1 – Example of a GSA Access Card



A GSA access 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 access cards are primarily used to access physically secured federal areas and information technology 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 Access Card Readers

According to GSA Order ADM 5900.1, *Physical Access Control Systems in U.S. General Services Administration Controlled Space*, GSA is responsible for managing HSPD-12-compliant physical access control systems (PACS) within facilities under its custody and control. The PACS in these facilities allow for access to controlled space, including restricted or secured areas. GSA is also responsible for the replacement of existing legacy perimeter PACS in GSA-controlled space with fully compliant ("end-to-end") PACS in coordination with the U.S. Department of Homeland Security's Federal Protective Service, the Facility Security Committees (FSCs), and tenant agencies.[2]

The task of administering and managing PACS in GSA facilities is performed by the GSA Office of Mission Assurance (OMA). OMA provides Agency-wide leadership and coordination for

[2] The Interagency Security Committee's *The Risk Management Process for Federal Facilities* requires FSCs for buildings with two or more federal tenants. FSCs are responsible for addressing building-specific security issues and approving the implementation of recommended countermeasures and practices. The FSCs include representatives of all federal tenants in the buildings, as well as the Federal Protective Service and GSA.

emergency management and security policy. This includes occupant emergency planning, response and recovery, personal identity verification, physical security, personnel security, and suitability activities.

GSA access card readers are present in 132 GSA-managed facilities. An electronic card reader can be used to control access to federal personnel and property. To enter space secured by a GSA access card reader, an individual must have been granted the appropriate permissions and have an active access card; otherwise, the cardholder will receive an error and not be allowed to enter.

Each time a GSA access card is scanned at a card reader, specific data is recorded in GSA's Enterprise Physical Access Control System (E-PACS) database. The PACS Branch, within OMA, is responsible for managing this access card database. The data can be extracted into various reports based on available fields and the needs of the user. One available field recorded by the access card reader and included in the data is "event type," which denotes additional information about the card used and access attempt. We identified four event types in the access card data that signify a failed access attempt. *Figure 2* gives a brief explanation of these four E-PACS event types.

Figure 2 – E-PACS Event Types That Signify a Failed Access Attempt

E-PACS Event Type	Definition
No Zone Privilege	The cardholder does not have the access permissions required to access the area.
Unauthorized Card	The cardholder's access permissions were disabled; therefore, the access card is suspended in E-PACS.
No Access At This Time	The cardholder attempted to access an area outside of the approved time parameters of their access card.
Expired PIV Card	The access card is expired.

PACS Security Control Guidance

On December 24, 2020, the PACS Modernization Working Group issued *Security Control Overlay of Special Publication 800-53 Revision 5: Security Controls for electronic Physical Access Control Systems* (Federal Guidance on PACS Security Controls). GSA assisted in developing this guidance to help agencies identify core controls for a PACS.

According to the Federal Guidance on PACS Security Controls, access control systems are critical parts of security programs. Many agencies rely on PACS to maintain security of sensitive information, facilities, and other critical assets. Exploitation of an improperly administered PACS can lead to unauthorized or unaudited access to such information, facilities, or other sensitive resources. Some applicable PACS controls outlined in the Federal Guidance on PACS Security Controls are to:

- Review and analyze system audit records for indications of organization-defined inappropriate or unusual activity;
- Report findings to organization-defined personnel or roles; and
- Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

The Federal Guidance on PACS Security Controls further states that access card data from PACS databases provides the capability to analyze and correlate audit logs from various components, devices, cardholder interactions, or archived sources. These logs can be provided to other teams within an organization, to assist them in monitoring for insider threats and information technology security threats and securing federal facilities and resources.

GSA Office of Inspector General Reports

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

- GSA does not consistently collect and destroy inactive GSA contract employee access cards;
- Contract employees used expired access cards to access GSA-managed facilities;
- GSA does not comply with access card issuance requirements; and
- GSA Credential and Identity Management System (GCIMS) data is inaccurate and incomplete.[3]

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.[4] 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;

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

[4] Assessment of GSA's Major Management Challenges for Fiscal Years 2017 through 2022.

- Significant deficiencies exist in GSA's process for managing GSA access cards for 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 our November 4, 2020, audit report, we reported that GSA was mismanaging contract employee access cards.[5] As a result of its mismanagement, GSA was unable to account for approximately 15,000 access cards issued to contract employees. We also found that:

- Unreliable data continues to limit GSA's ability to track access cards;
- GSA does not have adequate access card recovery procedures; and
- GSA has not implemented necessary oversight to ensure access cards are recovered from contract employees.

In response to these reports, GSA agreed to address vulnerabilities associated with building-specific facility access cards and GSA access cards. According to GSA, it has completed all corrective actions designed to address the findings and recommendations included in these reports.

[5] *GSA's Mismanagement of Contract Employee Access Cards Places GSA Personnel, Federal Property, and Data at Risk* (Report Number A190085/A/6/F21001).

Results

Finding – GSA is not monitoring access card data to identify risks to GSA personnel and federal property.

Failed access attempts could be an indication of attempted unauthorized access to federal facilities and secured areas. Federal guidance on access cards and electronic physical access control systems recommends monitoring access card activity to assess the risk and determine if additional oversight is needed. However, we found that GSA is not actively using data collected from access card readers to identify and assess the risks to its personnel and federal property.

Failed Access Attempts at GSA-Managed Buildings

For the 2-year audit period ended February 28, 2022, data collected from access card readers in GSA-managed facilities showed 32,179 failed access attempts. While the access card data shows that the average GSA-managed building had 244 failed access attempts during the audit period, six buildings had over 1,000 failed access attempts on doors secured by access card readers, including one building with 4,164 failed access attempts. Further, while the average access card user during our audit period had 2 failed access attempts, we found that 200 users had at least 25 failed access attempts. This included one user who had 1,963 failed access attempts.

These failed access attempts may have potential security implications. Eight of the top 10 buildings with the most failed access attempts contain child-care facilities or security-sensitive agencies, such as the Federal Bureau of Investigation, U.S. Social Security Administration, and U.S. Department of Homeland Security. The safety and security of the tenants and children in these buildings are a major concern.

Federal Guidance Related to Monitoring Failed Access Attempts Using Access Cards

Failed access attempts could be an indication of attempted unauthorized access to federal facilities and secured areas. In fact, federal guidance on access cards and electronic physical access control systems from the National Institute of Standards and Technology and the PACS Modernization Working Group recommend monitoring access card activity to assess the risk and determine if additional oversight is needed.

- According to National Institute of Standards and Technology Special Publication 800-116, Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access*, if a pattern of access card activity raises suspicions of fraudulent use, the security office of the issuing agency, or of the cardholder's duty station, should be notified and the security office should determine if further investigation is warranted and if the access card should be revoked.

- According to the PACS Modernization Working Group's Federal Guidance on PACS Security Controls, controls should be implemented to:
    - Review and analyze system records for indications of unusual activity;
    - Report these findings to appropriate personnel; and
    - Adjust the level of review, analysis, and reporting within the system when there is a change in risk.

GSA Is Not Actively Using the Access Card Data to Identify and Assess the Risks to Its Personnel and Federal Property

We found that GSA is not actively using the access card data to identify and assess the risks to its personnel and federal property. GSA access card readers are present in 132 GSA-managed facilities. The PACS Branch within OMA administers and manages these access card readers. The access card data from these readers can be extracted into various reports based on available fields and the needs of the user. However, as described below, we found that GSA is not actively using the data to identify and assess the risks to its personnel and federal property.

OMA is not reviewing the access card data to identify potential security threats. OMA's PACS Branch administers and manages the overall network of the access card readers in GSA-managed facilities. When we asked the PACS Branch Deputy Director about the data that was collected and how it was being used, he stated that the PACS Branch is not responsible for reviewing the data. The PACS Branch Deputy Director also stated that it would not be fair for the PACS Branch to review access records because it could give rise to concerns that employees are being monitored. However, when we asked four GSA building managers how they would expect to be notified of suspicious access data, three stated that they assumed the PACS Branch would inform them.

OMA is not providing access card data to building security stakeholders consistently—or in the most effective format—to identify and take action on repeated, failed access attempts. Of the 15 GSA building managers we contacted, 8 stated that they do not receive any access card data for their buildings. For the seven building managers who are receiving access card data from OMA, the data provided only lists the previous day's failed access attempts. The building managers do not receive any kind of trend analysis of the access card data, which could be used to identify suspicious access attempts. Access card data can be filtered to show records by building, door, region, date, individual, or event type. With this capability, it is possible to highlight higher-risk scenarios and show trends, such as an unauthorized cardholder repeatedly attempting to gain access to secured areas or an unauthorized cardholder who is repeatedly attempting to gain access to a facility outside of regular operating hours.

GSA has not issued written guidance to its building managers on how to use the access card data to identify high-risk activity. Of the seven GSA building managers who are receiving access card data, three said they were given non-definitive guidance from OMA. OMA told the building managers to use the data to follow up with cardholders or issue new access cards, but did not explain the risk factors building managers should look for to initiate these actions. GSA should provide guidance to help building managers identify patterns of access card activity that may be high-risk. The guidance should also establish who should be notified, by whom, and when, to mitigate the risk in a timely and effective manner.

In sum, GSA is not actively using data collected from access card readers to identify and assess the risks to its personnel and federal property. Because failed access attempts could be an indication of attempted unauthorized access to federal facilities and secured areas, GSA should monitor and use access card data to take appropriate follow-up actions.

Conclusion

GSA is not monitoring access card data from GSA card readers to identify risks to GSA personnel and federal property. For the 2-year audit period ended February 28, 2022, data collected from access card readers in GSA-managed facilities showed 32,179 failed access attempts. Failed access attempts could be an indication of attempted unauthorized access to federal facilities and secured areas. Federal guidance on access cards and electronic physical access control systems recommends monitoring access card activity to assess the risk and determine if additional oversight is needed. However, we found that GSA is not actively using data collected from access card readers to identify and assess the risks to its personnel and federal property.

In accordance with federal guidance, GSA should develop controls to monitor and use access card data to identify repeated, failed access attempts. GSA should also issue guidance to ensure that building security stakeholders know what steps to take to address repeated, failed access attempts identified through the data.

Recommendations

We recommend that the GSA Administrator:

1. Develop and implement procedures for monitoring access card data to identify repeated, failed access attempts that require follow up.
2. Use the access card data that is being collected to produce trend data to inform building security stakeholders of individuals with a significant number of failed attempts over a specified period of time.
3. Create and disseminate guidance addressing how building security stakeholders should handle repeated, failed access attempts.

GSA Comments

The GSA Administrator agreed with our recommendations and provided general comments on the timing of our audit. These comments did not affect our finding and conclusions. GSA's written 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
Daniel Riggs	Audit Manager
Andrew Kehoe	Auditor-In-Charge

Appendix A – Objective, Scope, and Methodology

Objective

We performed an audit of GSA's monitoring of access card use for physical access to GSA-managed facilities. We included this audit in our *Fiscal Year 2021 Audit Plan* to determine if GSA is monitoring access card use for physical access to GSA-managed facilities in accordance with federal regulations, policies, and guidance.

Scope and Methodology

This nationwide audit assessed GSA's monitoring of access card use for physical access to GSA-managed facilities. The scope of our audit included the data captured by E-PACS when individuals scanned access cards at GSA card readers during the 2-year audit period of March 1, 2020, through February 28, 2022.

To accomplish our objective, we:

- Reviewed federal regulations, policies, and guidance related to management of access card systems;
- Reviewed federal policies, procedures, and guidance related to access card use;
- Analyzed E-PACS data for the 2-year period ended February 28, 2022;
- Analyzed GCIMS data as of March 15, 2022;
- Assessed the access card data's reliability and validity through GSA interviews and data analysis;
- Submitted questions and data to 14 GSA building managers regarding E-PACS and access card use in their facilities;
- Conducted interviews of GSA building management personnel and OMA officials;
- Conducted interviews with personnel from the U.S. Department of Homeland Security's Federal Protective Service, the U.S. Department of Defense's Defense Counterintelligence and Security Agency, and the U.S. Office of Personnel Management; and
- Analyzed prior GSA Office of Inspector General audit reports and corrective actions that are significant to the audit objective.

Data Reliability

We assessed the reliability of the data by comparing overlapping access card data provided by the PACS Branch 4 months apart from each other and derived from different requests. We also conducted interviews with GSA personnel to define fields and request specific data. We determined that the data was sufficiently reliable for the purposes of this audit.

Sampling

During fieldwork, we selected a sample of buildings and individuals for further testing based upon the highest amount of failed access attempts during the 2-year audit period ended February 28, 2022.

Buildings – Our sample consisted of 14 buildings and comprised 53 percent of the failed access attempts at all GSA-managed facilities during our audit period. We included the 10 buildings with the highest number of failed access attempts, as well as an additional 4 buildings selected judgmentally based upon the highest number of failed access attempts, so that we had at least 1 building from each region included in our sample. Because we did not randomly sample the buildings, the results cannot be projected to the intended population.

Individuals – We submitted questions and corresponding data to the GSA building managers for each of the 14 buildings in our sample. The building managers' initial responses resulted in five follow-up interviews to gather additional information.

We conducted six additional interviews with individuals we judgmentally sampled based upon the highest number of failed access attempts in GSA's Heartland Region. This region was chosen for audit survey work because the audit team is also located in the Heartland Region and had easier access to the individuals and buildings, if necessary, due to the travel challenges caused by the COVID-19 pandemic.

While our judgmental samples do not allow for projection to the population, they did allow us to adequately address our audit objective.

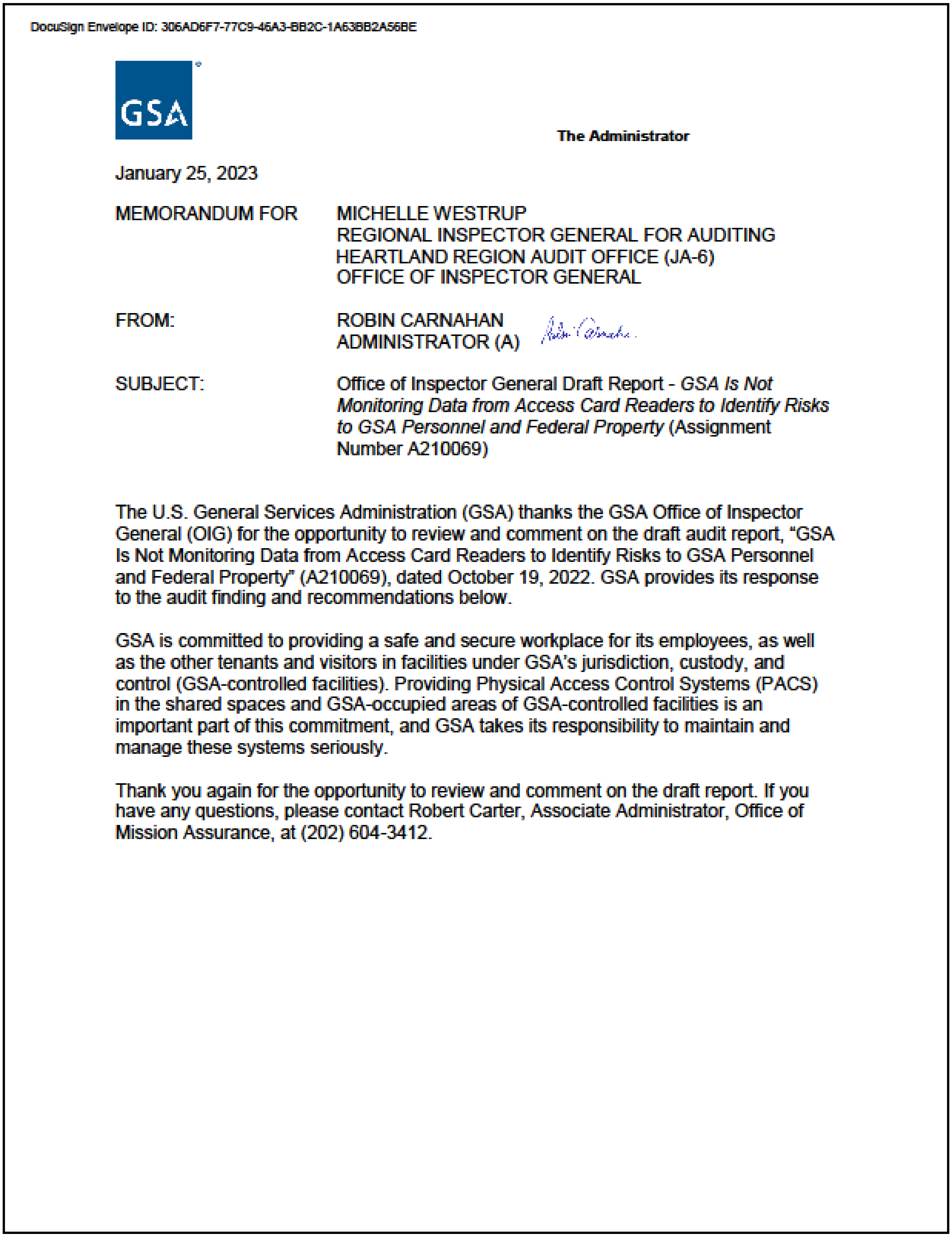
Internal Controls

We assessed internal controls significant within the context of our audit objective against GAO-14-704G, *Standards for Internal Control in the Federal Government*. The methodology above describes the scope of our assessment and the report finding includes any internal control deficiencies we identified. Our assessment is not intended to provide assurance on GSA's internal control structure as a whole. GSA management is responsible for establishing and maintaining internal controls.

Compliance Statement

We conducted the audit between July 2021 and June 2022 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 finding and conclusions based on our audit objective.

Appendix B – GSA Comments



DocuSign Envelope ID: 306AD6F7-77C9-46A3-BB2C-1A63BB2A56BE

GSA

The Administrator

January 25, 2023

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

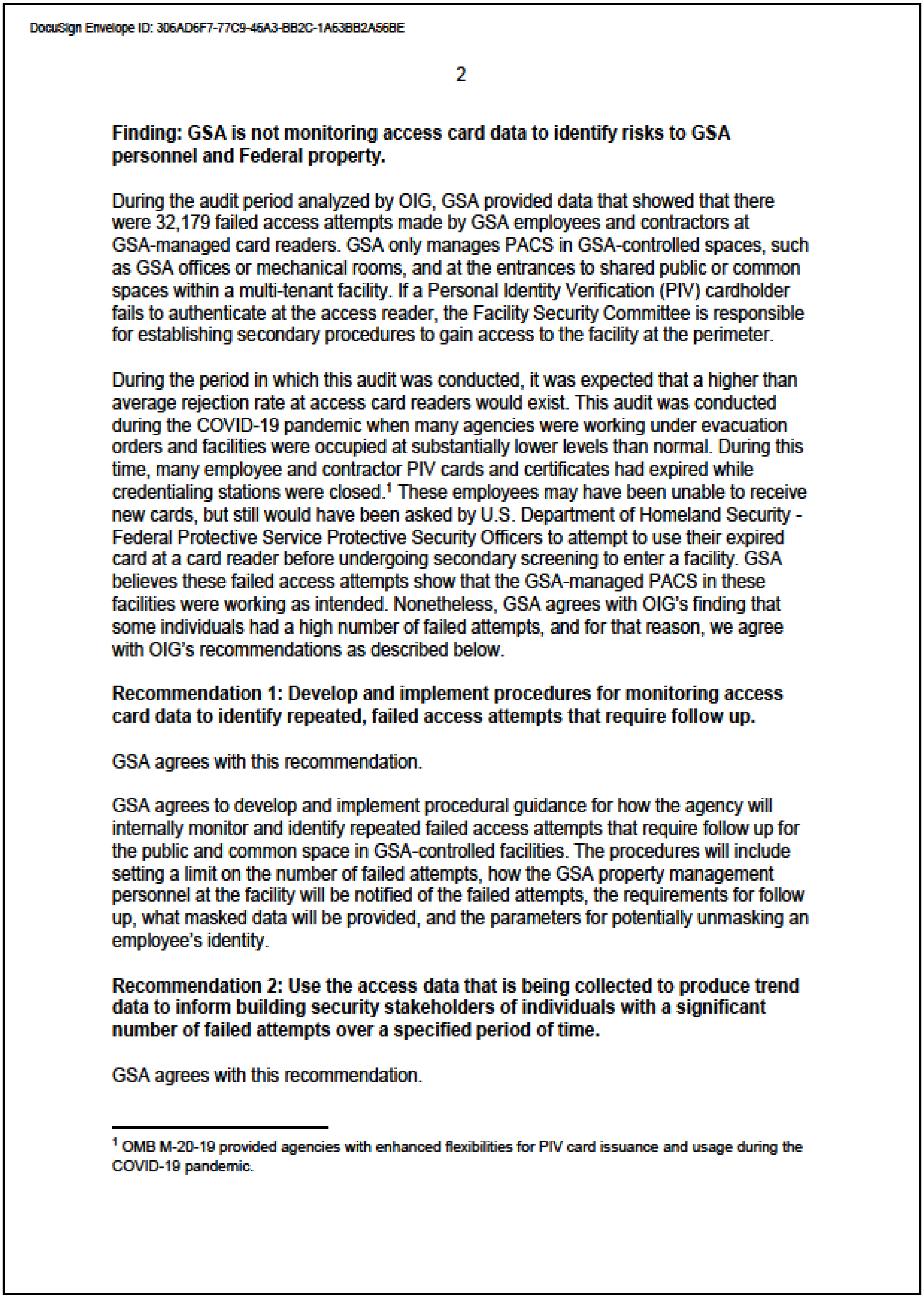
FROM: ROBIN CARNAHAN
ADMINISTRATOR (A)

SUBJECT: Office of Inspector General Draft Report - *GSA Is Not Monitoring Data from Access Card Readers to Identify Risks to GSA Personnel and Federal Property* (Assignment Number A210069)

The U.S. General Services Administration (GSA) thanks the GSA Office of Inspector General (OIG) for the opportunity to review and comment on the draft audit report, "GSA Is Not Monitoring Data from Access Card Readers to Identify Risks to GSA Personnel and Federal Property" (A210069), dated October 19, 2022. GSA provides its response to the audit finding and recommendations below.

GSA is committed to providing a safe and secure workplace for its employees, as well as the other tenants and visitors in facilities under GSA's jurisdiction, custody, and control (GSA-controlled facilities). Providing Physical Access Control Systems (PACS) in the shared spaces and GSA-occupied areas of GSA-controlled facilities is an important part of this commitment, and GSA takes its responsibility to maintain and manage these systems seriously.

Thank you again for the opportunity to review and comment on the draft report. If you have any questions, please contact Robert Carter, Associate Administrator, Office of Mission Assurance, at (202) 604-3412.



Finding: GSA is not monitoring access card data to identify risks to GSA personnel and Federal property.

During the audit period analyzed by OIG, GSA provided data that showed that there were 32,179 failed access attempts made by GSA employees and contractors at GSA-managed card readers. GSA only manages PACS in GSA-controlled spaces, such as GSA offices or mechanical rooms, and at the entrances to shared public or common spaces within a multi-tenant facility. If a Personal Identity Verification (PIV) cardholder fails to authenticate at the access reader, the Facility Security Committee is responsible for establishing secondary procedures to gain access to the facility at the perimeter.

During the period in which this audit was conducted, it was expected that a higher than average rejection rate at access card readers would exist. This audit was conducted during the COVID-19 pandemic when many agencies were working under evacuation orders and facilities were occupied at substantially lower levels than normal. During this time, many employee and contractor PIV cards and certificates had expired while credentialing stations were closed.[1] These employees may have been unable to receive new cards, but still would have been asked by U.S. Department of Homeland Security - Federal Protective Service Protective Security Officers to attempt to use their expired card at a card reader before undergoing secondary screening to enter a facility. GSA believes these failed access attempts show that the GSA-managed PACS in these facilities were working as intended. Nonetheless, GSA agrees with OIG's finding that some individuals had a high number of failed attempts, and for that reason, we agree with OIG's recommendations as described below.

Recommendation 1: Develop and implement procedures for monitoring access card data to identify repeated, failed access attempts that require follow up.

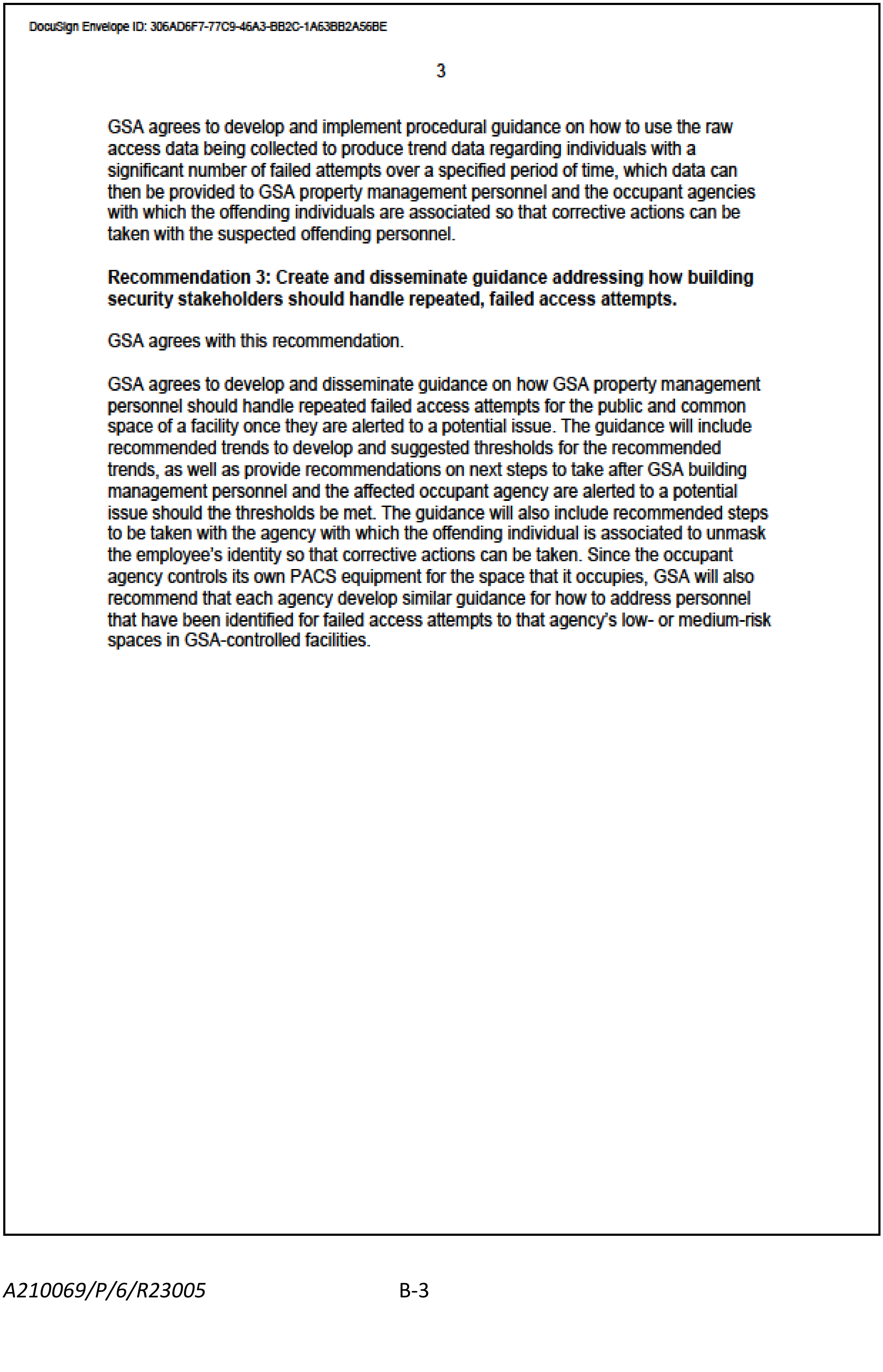
GSA agrees with this recommendation.

GSA agrees to develop and implement procedural guidance for how the agency will internally monitor and identify repeated failed access attempts that require follow up for the public and common space in GSA-controlled facilities. The procedures will include setting a limit on the number of failed attempts, how the GSA property management personnel at the facility will be notified of the failed attempts, the requirements for follow up, what masked data will be provided, and the parameters for potentially unmasking an employee's identity.

Recommendation 2: Use the access data that is being collected to produce trend data to inform building security stakeholders of individuals with a significant number of failed attempts over a specified period of time.

GSA agrees with this recommendation.

[1] OMB M-20-19 provided agencies with enhanced flexibilities for PIV card issuance and usage during the COVID-19 pandemic.



GSA agrees to develop and implement procedural guidance on how to use the raw access data being collected to produce trend data regarding individuals with a significant number of failed attempts over a specified period of time, which data can then be provided to GSA property management personnel and the occupant agencies with which the offending individuals are associated so that corrective actions can be taken with the suspected offending personnel.

Recommendation 3: Create and disseminate guidance addressing how building security stakeholders should handle repeated, failed access attempts.

GSA agrees with this recommendation.

GSA agrees to develop and disseminate guidance on how GSA property management personnel should handle repeated failed access attempts for the public and common space of a facility once they are alerted to a potential issue. The guidance will include recommended trends to develop and suggested thresholds for the recommended trends, as well as provide recommendations on next steps to take after GSA building management personnel and the affected occupant agency are alerted to a potential issue should the thresholds be met. The guidance will also include recommended steps to be taken with the agency with which the offending individual is associated to unmask the employee's identity so that corrective actions can be taken. Since the occupant agency controls its own PACS equipment for the space that it occupies, GSA will also recommend that each agency develop similar guidance for how to address personnel that have been identified for failed access attempts to that agency's low- or medium-risk spaces in GSA-controlled facilities.

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)

PBS Assistant Commissioner for Strategy & Engagement (PS)

Associate Administrator for the Office of Mission Assurance (D)

Chief of Staff for the Office of Mission Assurance (D2)

Chief Financial Officer (B)

Deputy Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

Deputy Assistant Inspector General for Acquisition Program Audits (JA)

Deputy Assistant Inspector General for Real Property Audits (JA)

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