GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Use of Facility Specific Building Badges

JE16-003
March 30, 2016

The Office of Inspector General (OIG) of the General Services Administration (GSA) found widespread use of facility-specific building badges at GSA-managed facilities. These building badges are often issued by GSA to employees and contractor employees instead of, or in addition to, the required Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) cards. The OIG's Office of Inspections and Forensic Auditing reviewed GSA's use of local building badges to determine if there is an increased risk of unauthorized access to GSA-managed facilities where PIV cards are not required for entry.[1]

Despite issuance of HSPD-12 over 10 years ago, GSA continues to issue facility-specific building badges with unique designs, data elements, and security features. In the GSA facilities where building badges are permitted, GSA employees and contractor employees usually have the option to use either their PIV card or building badge to access the facility.

Unlike PIV cards, which employ strict controls established by the National Institute of Standards and Technology (NIST), building badges are more susceptible to identity fraud, tampering, counterfeiting, and exploitation, and they cannot be rapidly authenticated electronically.[2] According to NIST, most bar code, magnetic stripe, and proximity cards (including building badges) can be easily copied and the technology used in their creation offers little or no authentication assurance.[3] This is a serious security risk because some building badges provide unescorted and unscreened access to federal facilities.

GSA's credentialing policy outlines specific and limited circumstances in which GSA may issue building badges, such as for temporary contractor employees, some non-U.S. citizens, childcare workers, and visitors.[4]

---

[1] We observed the use of building badges during our evaluation of GSA's process for issuing, managing, and terminating HSPD-12 PIV cards to contractor employees (GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Management of Contractor HSPD-12 PIV Cards (JE16-002)). Our evaluation found significant deficiencies in GSA's processes for managing GSA-issued PIV cards and for ensuring the completion of contractor employee background investigations. In addition, we found deficiencies in GSA's tracking and maintenance of contractor employee background investigation data stored within GSA's Credential and Identity Management System (GCIMS).

[2] See NIST Federal Information Processing Standards Publication 201-2 (FIPS-201-2), which specifies the architecture and technical requirements for a common identification standard for federal employees and contractor employees.

[3] NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008. The vulnerabilities are addressed further in NIST Draft SP 800-116 Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, December 2015.

[4] GSA Order CIO P 2181.1, *Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing*, October 20, 2008.

However, GSA lacks policies or guidance for (1) standardizing the security features of building badges, (2) ensuring the security of the systems that support the issuance and maintenance of building badges, (3) establishing controls for identity verification for building badge issuance, (4) requiring background investigations prior to issuing building badges, and (5) establishing training requirements for the staff managing building badge systems. In practice, GSA issues building badges to employees and contractor employees in a multitude of different formats with varying levels of security features.

We surveyed management officials in each of GSA's 11 regions, and conducted onsite inspections of four regions, including 14 GSA-managed facilities. We found that building badges are unsecure, unregulated, and in frequent use at these facilities. We found serious security risks with the use of building badges in GSA-managed facilities, including:

- Contractor employees found to be "unfit" as the result of unfavorable background investigations who nevertheless had active building badges;[5]
- Inactive contractor employees who had active building badges;
- Building badges without expiration dates issued by GSA to contractor employees;
- Instances where non-GSA tenant agencies had issued building badges to GSA contractor employees;
- Staff who were inadequately trained on the issuance of building badges; and
- Building badge IT systems that were unsecure.

We also found that GSA cannot determine the extent of these problems because it does not centrally monitor the management of building badges issued by its staff.

The widespread use of building badges and the weak internal controls over building badge systems increase the risk of unauthorized access to GSA-managed facilities. Unauthorized access to a federal facility increases the risk of a security event, such as an active shooter, terrorist attack, or theft of government property, as well as exposure of sensitive and proprietary information.

The OIG makes four recommendations to address security risks associated with the continued use of building badges (see page 14). The Associate Administrator of the Office of Mission Assurance agreed with our recommendations and initiated corrective actions. Management's comments can be found in their entirety in the Appendix.

[5] An "unfit" finding means the Federal Protective Service has concluded that a contractor is unsuitable for work on GSA contracts.

HSPD-12, issued in August 2004, addressed the need to eliminate the "[w]ide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks."[6] The directive established a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractor employees in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 directed the Secretary of Commerce to develop a federal standard for secure and reliable identification for gaining physical access to federal facilities and logical access to federal information systems.[7] The Department of Commerce's NIST published the first such standard in February 2005.[8] Also in 2005, the Office of Management and Budget (OMB) required all Executive branch agencies and independent establishments to issue PIV cards to all employees and long-term contractor employees, defined as those engaged for more than six months.[9]

In 2011, the Department of Homeland Security (DHS) reported that the majority of the federal workforce had PIV credentials and directed agencies to issue, by March 31, 2011, implementation plans requiring the use of PIV credentials for access to agency facilities and information systems.[10] OMB M-11-11 incorporated DHS's plan of action for agency implementation, which specified, among other things, that effective the beginning of fiscal year 2012, agencies must upgrade existing physical and logical access control systems to use PIV credentials before using development and technology refresh funds to complete other activities.[11] DHS's plan included partnering with GSA and its Public Building Service (PBS) regarding implementation of physical access requirements for federal buildings under PBS's purview.[12]

[6] *Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

[7] *Id*., at Section 2.

[8] Federal Information Processing Standard (FIPS) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, February 2005 (superseded in 2013 by FIPS 201-2).

[9] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* August 5, 2005, Attachment 1 at § 1.

[10] OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011, p.2 (OMB M-11-11). OMB M-11-11 incorporated and attached a DHS Memorandum on the same subject dated February 3, 2011. DHS is assigned operational responsibility for federal agency information systems. OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and DHS*, July 6, 2010. As noted below, DHS also has responsibilities related to security measures for physical access to federal facilities.

[11] *Id*., Attachment at 2.

In multiple-tenant federal facilities managed by GSA, decisions regarding building security policy and procedures, including physical access control systems, are made by Facility Security Committees.[13] These committees take their guidance from standards issued by DHS's Interagency Security Committee.[14] *The Risk Management Process: An Interagency Security Committee Standard*, August 2013, defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides physical security countermeasures for all non-military federal facilities. Using this standard, the Federal Protective Service (FPS) conducts facility security assessments of GSA facilities and rates them on a scale of one (lowest risk) to five (highest risk). FPS assessments are based on security evaluation factors that include mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. Based on the security level determination, FPS assigns a rating and recommends specific countermeasures to address the facility's risks.

According to May 2015 data, PBS manages 354 million rentable square feet in 8,603 buildings nationwide. GSA policy requires issuance of PIV cards to all agency employees and long-term contractor employees. GSA requires the use of PIV cards to log into agency workstations and access its IT systems and network, but it is still in the process of integrating the use of PIV cards with physical access control systems.[15]

While GSA issues PIV cards to most employees and long-term contractor employees, staff at some GSA-managed facilities also issue facility-specific building badges that are not HSPD-12 compliant but may allow the same unrestricted access to the facility. For example, we found in our related report, *GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Management of Contractor HSPD-12 PIV Cards* (JE16-002), that three of GSA's 11 regions permit exceptions to the PIV policy and do not issue PIV cards to certain types of contractors, such as those who do not require access to GSA IT systems. In such cases, GSA circumvents the policy that requires issuance of PIV cards to all long-term contractor employees by issuing non-PIV building badges.

[12] *Id.*

[13] GSA was directed to establish Building Security Committees (now called Facility Security Committees) by Presidential Memorandum issued in the aftermath of the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Memorandum of President William J. Clinton on Upgrading Security at Federal Facilities, June 28, 1995. See also The U.S. Department of Justice (DOJ) Vulnerability Assessment of Federal Facilities, June 28, 1995, at §§ 1.2, 4.1.2.

[14] The Interagency Security Committee was established by Executive Order 12977, Oct. 19, 1995, as a permanent oversight body under the GSA Administrator for the security and protection of non-military federal buildings and facilities in the United States. The Committee was transferred to DHS by Executive Order 13286 (February 28, 2003).

[15] GSA Order CIO 2182.1, *Mandatory Use of Personal Identity Verification (PIV) Credentials*, May 20, 2011, required that all new physical access control systems be compliant with the security standards established by HSPD-12.

In addition, many important security decisions regarding physical access to federally controlled facilities are left to the tenant agencies. If a federal building is occupied by a sole tenant, that agency will establish building security policies and procedures. For example, when GSA is the sole tenant in a facility, GSA has the authority to establish the building security policies and procedures.

Where more than one tenant agency is present in a GSA-managed facility, however, security decisions for physical access requirements are made through a Facility Security Committee, described above. Facility Security Committees, comprised of representatives from each tenant agency, determine facility-specific security countermeasures (such as physical barriers, security guard post orders, security cameras, approved credentials, and building access systems) using guidance from the DHS Interagency Security Committee and the FPS's security rating and recommendations.

Votes on the Facility Security Committee are weighted so that the larger federal tenants (by square footage of occupancy and number of employees) have the most influence in determining the security countermeasures, including the physical access requirements to the facility. Similarly, the larger federal tenants also pay a higher proportion of the cost of security countermeasures.

GSA often manages federal facilities in which it is not the majority tenant. If a Facility Security Committee votes to implement a security policy or fund a security countermeasure, all tenants (including GSA) must adhere to the security policy and pay their portion of the cost of the security countermeasure. Even as facility manager, GSA cannot overrule decisions made by a Facility Security Committee.

Facility Security Committees in some GSA-managed facilities have voted to allow the use of non-HSPD-12 compliant building badges to access the facility.[16] According to GSA staff, Facility Security Committees vote to allow building badges because of the costs associated with issuing PIV cards and the existence of legacy physical access control systems that are not compatible with PIV cards.

As the landlord of such facilities, GSA sometimes assumes the responsibility of issuing building badges and managing building badge systems. The GSA Office of Mission Assurance (OMA) and its regional staff provide agency-wide leadership and coordination for GSA security policy, including managing GSA's HSPD-12 PIV program. However, OMA provides only limited guidance for regulating the issuance of building badges. Unlike GSA's policy for the issuance of PIV cards, GSA's policy for issuing building badges does not incorporate background

[16] DHS Interagency Security Committee guidance does not specifically address HSPD-12 or facility access badges, which are governed by OMB M-11-11.

investigation requirements and does not describe minimum standard security features for building badges.[17] As a result, GSA issues building badges for each facility in different formats with varying levels of security features.

1 Building badges are unsecure, unregulated, and in frequent use in GSA-managed facilities.

Although HSPD-12 requires the use of a standardized, common federal identification (PIV card), GSA staff still issue building badges with unique formats, data elements, and electronic proximity features (see Figure 1).[18]

The primary purpose of HSPD-12 was to establish a common identification standard for federal employees and contractor employees. However, during our inspection visits to 14 GSA-managed facilities across four regions, we found 17 distinctly different building badges in use (see Figure 2). The number of building badges in use at the 8,603 federal facilities managed by GSA was unknown because OMA did not track such data.

[17] The implementing instructions for HSPD-12 require a minimum background investigation for all federal employees and long-term contractor employees. For the period covered by this evaluation, the Federal Protective Service (FPS) was responsible for conducting all background investigations for long-term GSA contractor employees. GSA contractor employees were permitted to begin work on a GSA contract after FPS issued a favorable initial fitness determination.

[18] A proximity card acts as an electronic key that is read by a sensor and allows access to a facility.

Figure 1. This graphic displays the essential differences in security features between PIV cards and building badges and provides a side-by-side comparison of a building badge that we observed in use and a standard PIV card.

Essential Differences Between Building Badges and HSPD-12 PIV Cards

	Building Badge Requirements	HSPD-12 PIV Card Requirements
Issued by an officially accredited provider?	✗	✓
Granted only after identity is verified?	✗	✓
Resistent to fraud, counterfeiting, and terrorist exploitation?	✗	✓
Provides rapid verification of identity?	✗	✓
Compatible with HSPD-12 compliant physical access control systems?	✗	✓
Grants access to federal IT systems?	✗	✓
Protects individual privacy?	✗	✓

Sample Building Badge vs. HSPD-12 PIV Cards

Examples of the characteristics of the building badges that we observed include (see figure 2):

- Different color schemes, backgrounds, GSA logos, holograms, and patterns to differentiate between contractor employees and employees.
- Varying inclusion of information such as building name, location, contractor name, expiration date, and authorizing official's signature.
- Varying quality of photos and clarity of text.
- Varying quality of materials used to produce the building badges.

During our inspection visits we found several examples of security weaknesses that were a direct result of reliance on building badges.

- At a Level IV facility, we found that GSA issued building badges to both employees and contractor employees with a proximity feature that opened unmanned doors. Through a review of building badge data, we also found 116 inactive contractor employees whose access through the building badge system had not been terminated.

Figure 2. This graphic shows the different types of building badges we observed in use during our onsite inspections.

- At the same Level IV facility, we found an individual who leased space in the building for a barbershop used a building badge issued by an agency that was no longer a tenant in the GSA-managed facility (see Figure 3). This individual had no background investigation on file with GSA and was able to routinely enter the facility using only this building badge.

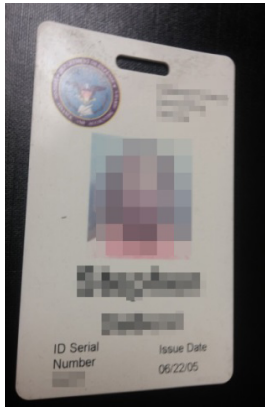

Figure 3

- At another Level IV facility, we found a tenant agency that issued building badges using card stock with the GSA logo (see Figure 4). The card stock was provided to the tenant agency by GSA.

Figure 4

- At another Level IV facility located in a major downtown area, we found an active contractor employee using an expired building badge with an indiscernible photo (see Figure 5).

Figure 5

- At three Level IV facilities, we found GSA issued building badges without expiration dates (see Figure 6). Further, two of these Level IV federal facilities permitted access through the main entrance with only a visual ("flash pass") inspection of the badge rather than passing them through an electronic point of access. Inactive contractor employees who keep this type of building badge after they leave the contract could use it to continue to access these types of federal facilities.

Figure 6

- At a Level III facility, we found a building badge in use that was made of low quality material and was easily reproducible (see Figure 7). Despite its poor quality and noticeable damage, this building badge allowed access to the facility. GSA staff created this badge by inserting a picture of the contractor into a word processing document, which was then printed on regular copy paper and laminated.

Figure 7

- We found instances where GSA regional staff issued multiple building badges to the same contractor employee. Unlike HSPD-12 systems, which use a unique numeric identifier for each individual, building badge systems have weak controls which allow individuals to be issued multiple building badges.

Tenants of these GSA-managed facilities included regional offices for federal agencies such as the Internal Revenue Service, Social Security Administration, Coast Guard, Army Corps of Engineers, Office of Personnel Management, Health and Human Services, and U.S. Immigration and Customs Enforcement. Other tenants included local offices for members of Congress. The examples above highlight the vulnerabilities of building badges and how they may increase the risk of unauthorized access to GSA-managed facilities.

2 GSA did not deactivate the building badges of some unfit and inactive contractor employees.

We compared data from a sample of building badge IT systems with background investigation data from FPS and GSA's Credential and Identity Management System (GCIMS), GSA's system of record for background investigation results and active employment status. We found seven contractor employees with unfit background investigation results who had active building badges. We also found over 170 contractor employees who had active building badges but were, according to GCIMS, not active contractor employees.

Allowing unfit and inactive contractor employees to retain active building badges increases the risk of unauthorized access to GSA-managed facilities.

3 GSA does not adequately train staff on how to operate the software that is used to issue building badges.

Many of the GSA staff responsible for issuing building badges and managing building badge IT systems at the 14 facilities we inspected had no formal training on such systems, even though many used the same commercial off-the-shelf software for producing building badges.[19]

At six of the 14 buildings we inspected, the staff responsible for issuing building badges received no formal training on how to operate the different IT systems that they used to issue building badges. For example, we found that some GSA staff responsible for issuing and managing badges could not perform basic querying functions to generate a report of individuals who have active building badges as well as ones with badges that are about to expire.

4 Building badge IT systems are unsecure.

During our 14 onsite inspections, we observed five building badge IT systems that were intentionally maintained as "stand alone" systems. According to GSA staff, these "stand alone" systems were not connected to the GSA IT network or managed by GSA IT staff due to privacy and security concerns. Since these "stand alone" systems were not connected to any GSA IT network, they did not receive regular system updates or network backup. This increases the risk of system crashes and data loss. For example, during our inspection, one facility was unable to provide requested building badge data due to a recent system crash.

Moreover, the locations of some building badge systems were not secure. We found a building badge system that was housed in an unlocked closet, in a GSA office that was not monitored by FPS contractor guards. Building badges created from this system allowed after-hours access to a Level III building and parking garage. The unsecure location of the building badge system increases the risk of unauthorized access to these areas.

[19] Managing a building badge system can include the responsibility for developing and implementing the internal controls over the issuance of building badges, determining the design of the badge (color schemes, backgrounds, GSA logos, holograms, and patterns to differentiate between contractor employees and employees), determining the information to include on the badge (building name, location, contractor name, expiration date, and authorizing official's signature), and assigning building badges access to specific doors/areas through proximity readers.

This evaluation found that building badges are unsecure, unregulated, and in frequent use at GSA-managed facilities. The lack of internal controls over the issuance of building badges and the management of building badge systems significantly increases the security risk of unauthorized access. Unauthorized access to a federal facility increases the risk of a security event, such as an active shooter, terrorist attack, and theft of government property, as well as exposure of sensitive and proprietary information.

In implementing physical access requirements for federal buildings, GSA works in coordination with the DHS Interagency Security Committee, the Federal Protective Service, and the Facility Security Committees, all of which have critical roles in securing multi-tenant federal facilities. Accordingly, we are providing copies of this report to the DHS Assistant Secretary for Infrastructure Protection, who serves as Chairman of the Interagency Security Committee; the Director of the Federal Protective Service; and the DHS Inspector General for their information.

1. For facilities where GSA is the sole or primary tenant, GSA should develop a policy to discontinue the issuance of local building badges to employees and contractor employees who are required to receive PIV cards.

2. GSA policy developed in response to recommendation #1 should include an implementation and transition plan to retrieve and destroy GSA-issued local building badges.

3. GSA should develop a secure solution for allowing physical access to GSA-managed facilities to those who are not required to receive PIV cards.

4. If the Facility Security Committees of facilities where GSA is not the sole or primary tenant decide to allow the use of building badges, GSA should not issue local building badges on behalf of tenant agencies.

The objective of this evaluation was to review GSA's use of building badges and determine if these building badges increase the risk of unauthorized access to GSA-managed facilities. In order to accomplish our objective, we:

- Conducted onsite inspections of 14 GSA-managed facilities in four regions;
- Interviewed agency management responsible for issuing and managing PIV cards and building badges, including selected GSA regional building and security managers, FPS guards, OMA staff, and HSPD-12 Managed Service Office staff; and
- Assessed the adequacy and compliance of GSA Central Office and regional offices' facility specific controls, policies, procedures, and guidance related to the issuance, maintenance, and destruction of building badges.

The testing samples for this evaluation were judgmentally selected and therefore cannot be generalized to the use of building badges nationwide. Although our findings are not generalizable, they are indicative of the serious security risks identified in this report.

Our evaluation was conducted from June 2014 through May 2015 in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation.*

GSA

OFFICE OF MISSION ASSURANCE

MAR 2 5 2016

Ms. Patricia D. Sheehan
Director
Office of Inspections and Forensic Auditing
Office of Inspector General
U.S. General Services Administration
1800 F Street, NW (JE)
Washington, DC 20405

Dear Ms. Sheehan:

The U.S. General Services Administration (GSA) appreciates the opportunity to respond to the GSA Office of Inspector General's (OIG) draft report entitled, *Draft Report - GSA Facilities at Risk: Security Vulnerabilities Found in GSA's Use of Facility Specific Building Badges.* In its report, the OIG issued four recommendations to GSA. The OIG recommends that the Administrator of GSA take the following actions:

- Recommendation 1 - For facilities where GSA is the sole or primary tenant, GSA should develop a policy to discontinue the issuance of local building badges to employees and contractors who are required to receive Personal Identity Verification (PIV) cards.
- Recommendation 2 - GSA policy developed in response to recommendation 1 should include an implementation and transition plan to retrieve and destroy GSA-issued local building badges.
- Recommendation 3 - GSA should develop a secure solution for allowing physical access to GSA-managed facilities to those who are not required to receive PIV cards.
- Recommendation 4 - If the Facility Security Committees of facilities where GSA is not the sole or primary tenant decide to allow the use of building badges, GSA should not issue local building badges on behalf of tenant agencies.

GSA agrees with the findings and recommendations of the OIG. GSA will implement corrective actions for the above-referenced recommendations; however, at the time of this audit review, GSA has already taken corrective measures on the following:

- GSA is drafting an Order currently entitled *Facility Access Cards Use and Accountability in GSA Owned and Leased Facilities* that incorporates corrective actions for recommendations 1, 2 and 3.

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

- GSA will work with the Interagency Security Council, Facility Security Committees, the U.S. Department of Homeland Security - Federal Protective Service and tenant agencies to develop processes to address recommendation 4.

If you have any questions, please contact me at (202) 604-3412.

Sincerely,

R. J. Carter

Robert J. Carter
Associate Administrator

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

OFFICE OF INSPECTOR GENERAL

U.S. General Services Administration

For media inquiries
OIG_PublicAffairs@gsaig.gov
(202) 273-7320

REPORT FRAUD, WASTE, AND ABUSE!

(800) 424-5210

Anonymous Web Form

fraudnet@gsaig.gov

Want to be aware of information the instant it becomes publicly available?

SUBSCRIBE