U.S. General Services Administration (GSA)

GSA Order: Physical Access Control Systems (PACS) in GSA-Controlled Space
ADM 5900.1A
Office of the Administrator
omapolicy@gsa.gov

Purpose:

This Order establishes an agency-wide approach and policy to update, procure, and install compliant Physical Access Control Systems (PACS) in common space, perimeter space and GSA-occupied space in federally owned facilities under the jurisdiction, custody and control of GSA, and leased space where GSA is the occupant agency (GSA-controlled space).

Background:

The memorandum *GSA/Public Buildings Service (PBS) Physical Access Control Directive*, dated September 11, 2013, was signed by PBS and the Office of Mission Assurance (OMA). That memorandum established the implementation of fully compliant PACS and the migration of disparate PACS to an enterprise-level, fully compliant Homeland Security Presidential Directive-12 (HSPD-12) PACS within GSA-controlled facilities.

A key component to complying with this memorandum involved establishing an agency-wide approach and policy. ADM 5900.1, *Physical Access Control Systems in U.S. General Services Administration Controlled Space*, dated April 14, 2017, achieved this. There have been changes to the security industry since ADM 5900.1 was originally issued as well as some confusion within GSA over how to apply ADM 5900.1. Those issues are addressed in this update.

As compliant PACS are installed, the need for separate access cards is eliminated. ADM 7640.3, *Termination Process and Oversight of General Services Administration (GSA) Issued Facility Access Cards in GSA Controlled Space in Both Owned and Leased Facilities*, dated September 16, 2016, was issued to define the oversight and termination process of GSA-issued Facility Access Cards (FAC) in GSA-controlled space. At this time, the majority of the requirements in ADM 7640.3 are complete. By incorporating the remaining items into this Order, all PACS-related information will be consolidated in a single Order.

Applicability:

This Order applies to all PACS in GSA-controlled space. In addition, per the terms of a lease, this order also applies to any lessor procured PACS that GSA will manage. This order does not apply to GSA delegated facilities.

This Order applies to all GSA employees in the performance of their duties, except for the employees in the following independent offices within GSA:

1. The Office of Inspector General.
2. The Civilian Board of Contract Appeals.
3. Presidential Transition space.

Cancellation:

This Order supersedes ADM 5900.1, *Physical Access Control Systems in U.S. General Services Administration Controlled Space* (April 14, 2017).

This Order Cancels ADM 7640.3, *Termination Process and Oversight of General Services Administration (GSA) Issued Facility Access Cards in GSA Controlled Space in Both Owned and Leased Facilities* (September 16, 2016).

Summary of Changes:

This Order has the following changes from the previous iteration:

1. Updated language to clarify this Order also applies to leased space where GSA is the occupant agency.

2. Incorporates outstanding elements of ADM 7640.3, *Termination Process and Oversight of General Services Administration (GSA) Issued Facility Access Cards in GSA Controlled Space in Both Owned and Leased Facilities* in order to consolidate PACS information into one directive.

3. Added definitions.

4. Updated terminology to reflect changes in the security industry.

5. Updated the format of the order to align with OAS 1832.1C, Internal Directives Management.

Roles and Responsibilities:

Further details of the coordinated efforts and the roles and responsibilities of different Staff and Service Offices (SSOs) can be found in sections 2 and 3 below.

Signature:

_______/s/_____________________ ____________________
Robin Carnahan Date
Administrator

Table of Contents

1. Definitions

1.1. GSA-controlled space

GSA-controlled space refers to common space, perimeter space and GSA-occupied space in federally owned facilities under the jurisdiction, custody and control of GSA, and leased space where GSA is the occupant agency.

1.2. Legacy perimeter PACS

Legacy perimeter PACS refers to an existing PACS that does not meet the Federal Identity Credential and Access Management (FICAM) and Office of Mission Assurance (OMA) National PACS Framework requirements capable of reading and authenticating a Personal Identity Verification (PIV) Credential for facilities nationwide.

1.3. Interagency Security Committee (ISC)

The ISC is a collaborative organization that leads nonmilitary federal security programs. The ISC standards apply to all federal facilities in the United States, including existing buildings, new construction, and leased facilities.

1.4. Federal Protective Service (FPS)

FPS provides law enforcement and related security services, as outlined in the Memorandum of Agreement (MOA) between the Department of Homeland Security (DHS), dated April 27, 2023, and GSA as may be amended from time to time.

1.5. Facility Security Committee (FSC)

An FSC is a committee established in accordance with the Interagency Security Committee (ISC) standards that is responsible for addressing facility-specific security issues and approving the implementation of above standard/basic security measures and practices in multi-tenant or single tenant facilities.

1.6. Government Furnished Information Technology Equipment (GFITE)

GFITE refers to agency-provided IT equipment, to include computers, software, printers, telephones, and telecommunication equipment.

1.7. Building Technology Services Division (BTSD)

The BTSD resides within the Office of GSA IT's PBS Public Buildings IT Services (PB-ITS) and specializes in IT Project Management support for building systems projects that depend on the GSA network or require remote connectivity. This includes new capital projects, system migrations and system upgrade projects.

1.8. PACS Project

A PACS Project is any project that includes updating, procuring, and/or installing compliant PACS in GSA-controlled space.

2. PACS Projects in GSA-Controlled Space

GSA is responsible for managing HSPD-12 compliant PACS within GSA-controlled space, which allows 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 FPS and the FSC. Those responsibilities are outlined below.

GSA legacy perimeter PACS systems are not authorized to be updated, and any changes to a PACS must also integrate with an enterprise-level PACS that meets the FICAM and OMA National PACS Framework requirements capable of reading and authenticating a PIV Credential for facilities nationwide.

2.1. Federally-Owned Facility GSA PACS Projects

All federally-owned facility GSA PACS projects shall be a coordinated effort between PBS, the Office of GSA IT, and OMA.

2.2. All Lease projects where GSA is the Occupant Agency

For lease projects, PBS will work with OMA to obtain the scope of work to be included in the solicitation package as special requirements. The lease project team will include OMA and GSA IT in the design of Tenant Improvements.

3. Compliant PACS require a coordinated effort across multiple SSOs.

This Order outlines a coordinated effort between PBS, the Office of GSA IT, Office of Human Resources Management (OHRM), Office of Administrative Services (OAS), and OMA to procure and to install as well as update existing non-compliant PACS components/systems with PACS that are compliant with HSPD-12, GSA IT, and GSA Network policies.

3.1. PBS

PBS must do the following:

- Coordinate all aspects of facility management in GSA-controlled space throughout any PACS project.
- Provide a project manager for each PACS project.
- Name a contracting officer for each PACS project.
- Work with OMA to review the scope of work for PACS and ensure its inclusion in the solicitation package as special requirements for all New, New/Replacing, and Superseding Leases where GSA is the occupant agency.
    - The lease project team will include OMA and GSA IT in the design of Tenant Improvements including the Technical Analysis/Evaluation for all PACS portions of proposals.
- Determine site priority within each project phase throughout any phased PACS project.
- Work with the OMA PACS Branch to configure system specific hardware and software to meet the site's requirements.

- Coordinate with OMA and the GSA IT/BTSD team throughout each PACS project to ensure completeness and compliance.

3.2. GSA IT

GSA IT must do the following:

- Provide GFITE, network access, and support for the IT network infrastructure for all Federal Facility PACS projects.

- Work with OMA and PBS to meet all necessary policies, directives, guides, and mandates for a successful, compliant solution.

- Assign a BTSD Technical Project Manager (PM) to coordinate with PBS, Network Operations (NetOps) and OMA to review, comment, and ultimately approve the proposed infrastructure protection (IP) design to support the overall system design.

    - The BTSD Technical PM–working with other necessary GSA IT team members–must coordinate shipping and configuration of any new or existing network infrastructure equipment that will be used to support the system.

    - The BTSD Technical PM must also coordinate with the PACS Information System Security Officer to obtain necessary system device level approval for connection to the GSA network and IP address range creation as needed.

3.3. OHRM

OHRM must do the following:

- Assist PBS, GSA IT, OMA and OAS in conducting pre-decisional involvement activities if applicable.

    - Consult with the lead GSA SSO involved and with occupant agencies if requested on the statutory bargaining obligations and recommended strategies for implementing the PACS Plan, as appropriate.

    - Advise and assist in meeting Labor Relations obligations, as appropriate, including providing required notices and leading the agency's negotiations teams with applicable unions, if applicable.

3.4. OAS

OAS must assist PBS, GSA IT, OHRM, and OMA including any necessary contracting as well as tenant communications where GSA is the occupant agency.

3.5. OMA

OMA must do the following:

- Provide standardized contracting documents to the PBS project manager, provide technical assistance to the project team, and assist PBS with coordinating with the vendor for site design, system engineering, system acceptance testing and system commissioning.

- Coordinate with the PBS project team and facility management office to gather site specific requirements as well as, where needed, assist in coordinating access at the site for site walkthrough(s)/survey(s) and system installation.

- Liaise with the facility's FSC and FPS contacts for system use, training of Protective Security Officers, and for system setup and use prior to deployment. System/site setup will consist of but is not limited to the following: access group definition, determining those access group owners, site base access hours, site general/public doors, etc.

- Coordinate with PBS, the vendor, and FPS for necessary Intrusion Detection System connections as needed.

- Work with the integrator to review and provide feedback for proposed system/site design.

- Work with the BTSD team representative to ensure GSA IT requirements are satisfied regarding the network infrastructure to support the proposed system/site design.

- Collaborate with PBS and the BTSD team where needed to address network infrastructure matters to ensure a successful installation that meets respective policies, mandates, directives, site needs and OMA guidance.

- Work with PBS and GSA IT to meet all necessary policies, directives, guides, and mandates for a successful, compliant solution.

- Work with PBS as part of the Technical Analysis/Evaluation team for all PACS portions of proposals.

- Provide access to executive branch employees in possession of a valid Government issued PIV Credential, as well as continue to provide access to legislative and judicial branch employees.

4. References and Authorizing Documents

4.1. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

4.2. DHS Policy Directive 3, Homeland Security Advisory System, March 12, 2002.

4.3. Federal Information Security Management Act of 2002, 44 United States Code , Section 3541 et seq., as amended December 18, 2014.

4.4. National Institute of Standards and Technology References

4.4.1. Federal Information Processing Standards 199 – “Standards for Security Categorization of Federal Information and Information Systems,” February 1, 2004.

4.4.2. Federal Information Processing Standards 200 – “Minimum Security Requirements for Federal Information and Information Systems,” March 1, 2006.

4.4.3. Federal Information Processing Standards 201-3 – “Personal Identity Verification (PIV) of Federal Employees and Contractors,” January 24, 2022.

4.4.4. Federal Information Processing Standards 140-3 – “Security Requirements for Cryptographic Modules,” March 22, 2019.

4.4.5. NIST Special Publication 800-30 – “Guide for Conducting Risk Assessments,” Revision 1, September 17, 2012.

4.4.6. NIST Special Publication 800-37 – “Guide for the Security Certification and Accreditation of Federal Information Systems,” Revision 2, December 20, 2018.

4.4.7. NIST Special Publication 800-53 – “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 5, December 10, 2020.

4.4.8. NIST Special Publication 800-57 – “Recommendation for Key Management, Part 1: General,” Revision 5, May 4, 2020.

4.4.9. NIST Special Publication 800-73-4 – “Interfaces for Personal Identity Verification,” Revised February 12, 2016.

4.4.10. NIST Special Publication 800-76-2 – “Biometric Specifications for Personal Identity Verification,” July 11, 2013.

4.4.11. NIST Special Publication 800-78-4 – “Cryptographic Algorithms and Key Sizes for Personal Identity Verification,” May 29, 2015.

4.4.12. NIST Special Publication 800-116 – “A Strategy for the Use of PIV Credentials in Physical Access Control Systems,” Revision 1 June 29, 2018.

4.5. Office of Management and Budget References

4.5.1. FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (M-10-15), April 21, 2010.

4.5.2. Implementation of Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors (M-05- 24), August 5, 2005.

4.5.3. Protection of Sensitive Agency Information (M-06-16), June 23, 2006.

4.5.4. Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials (M-07-06), January 11, 2007.

4.5.5. Enabling Mission Delivery through Improved Identity, Credential, and Access Management (M-19-17), May 21, 2019.

4.6. Interagency Security Committee References

4.6.1. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2021 edition.

4.7. Federal Chief Information Officers Council and the Federal Enterprise Architecture References

4.7.1. FICAM Architecture, Version 3.3, June 30, 2023.

4.7.2. Federal Identity, Credential, and Access Management Personal Identity Verification in Enterprise Physical Access Control Systems, Version 3.0, March 26, 2014.

4.8. GSA IT References

4.8.1. GSA Order 2100.1P “GSA Information Technology (IT) Security Policy,” January 31, 2024.

4.8.2. GSA Order 2181.1A ADM “Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing Policy, and Background Investigations for Contractor Employees” March 27, 2024.

4.8.3. GSA Telecommunications Distribution and Design Guide: Telecommunications and Infrastructure Standards, Version 8, August 6, 2016.

4.8.4. GSA Smart Buildings Implementation Guide, Version 1.2.1, April 29, 2022

4.8.5. GSA Building Technologies Technical Reference Guide, Version 3, May 1, 2024.

4.8.6. Configuration Management [CM] Guide [CIO IT Security 01-05, Rev. 5], March 1, 2022.

4.9. GSA Office of Mission Assurance References

4.9.1. Physical Access Control Systems Memo, 2015.

4.9.2. GSA HSPD-12 Personal Identity Verification and Credentialing Handbook, March 18, 2020.

4.10. GSA PBS Office of Facilities Management References

4.10.1. Technology Policy for PBS-Owned Building Monitoring and Control Systems, December 14, 2022.