GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM 5900.1
April 14, 2017

GSA ORDER

SUBJECT: Physical Access Control Systems in U.S. General Services Administration Controlled Space

1. Purpose. This Order establishes an agency-wide approach and policy to update, procure, and install compliant Physical Access Control Systems (PACS) in General Services Administration (GSA) controlled space.

2. Background. The memorandum titled "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. Given the enterprise level solution, which requires an agency-wide approach and specific functions for individual Offices, an Order encompassing all of GSA is necessary.

3. Scope and applicability. This Order applies to all GSA managed PACS in all facilities under the custody and control of GSA and any PACS procured under a delegation from GSA that GSA will manage. The provisions of this Order shall not be construed to interfere with or impede the legal authorities or independence of the Office of Inspector General (OIG) or the Civilian Board of Contract Appeals (CBCA).

4. Policy. This Order outlines a coordinated effort between PBS, the Office of GSA IT, the Office of Human Resources Management (OHRM), the 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. Any changes to a PACS must also integrate with an enterprise-level PACS that meets the Federal Identity Credential and Access Management (FICAM) and OMA National PACS Framework requirements capable of

reading and authenticating a Personal Identity Verification (PIV) Card for facilities nationwide.

5. Responsibilities. GSA is responsible for managing HSPD-12 compliant PACS within facilities under the custody and control of GSA, 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 the Department of Homeland Security – Federal Protective Service (FPS), the Facility Security Committees (FSC), and tenant agencies. Those responsibilities are outlined in Appendix A.

Within a reasonable timeframe of the Order's signature, OMA, in conjunction with those Offices, will release a GSA PACS Plan with a timeline and a list of targeted GSA buildings and timelines, and instructions for facilities management.

6. Authorities. A list of authorities and reference documents are listed in Appendix B.

7. Signature.

/S/_____
TIMOTHY O. HORNE
Acting Administrator

Appendix A. Standard Operating Procedures
Appendix B. References and Authorizing Documents

Appendix A. Standard Operating Procedures

All projects shall be a coordinated effort between PBS, the Office of GSA IT, and OMA as well as non-GSA entities, including FPS and FSCs for each facility, in the roles outlined in the Interagency Security Committee Risk Management Process.

a. PBS shall:

- Provide a project manager.
- Coordinate all aspects of facility management.
- Name a contracting officer.
- Determine site priority within each project phase.
- Work with OMA and GSA IT to meet all necessary policies, directives, guides, and mandates for a successful, compliant solution.

b. The Office of GSA IT shall:

- Provide network access, Government Furnished Equipment (GFE) laptops and support for the IT network infrastructure and GFE network hardware.
- Assign a Building & Energy (B&E) team representative to coordinate with PBS and OMA to review, comment, and ultimately approve the proposed infrastructure protection (IP) design to support the overall system design. The B&E representative, working with other necessary GSA IT team members, must coordinate shipping and configuration of necessary new network infrastructure equipment as well as configuration of any existing network infrastructure equipment that will be used to support the system. The B&E representative 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.
- Work with OMA and PBS to meet all necessary policies, directives, guides, and mandates for a successful, compliant solution.

c. OMA shall:

- Provide standardized contracting documents to the PBS project manager, technical assistance to the project team, 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 as requested by the PBS project manager.
- Liaise with the facility's FSC and FPS contacts for system use, training of Protective Security Officers, and for FSC approval 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 B&E team representative to ensure GSA IT requirements are satisfied regarding the network infrastructure to support the proposed system/site design.
- Work with the OMA national System Engineering team to configure system specific hardware and software to meet the site's requirements.
- Collaborate with PBS and the B&E 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.

d. OHRM shall:

- Assist PBS, GSA IT, OMA and OAS in conducting pre-decisional involvement activities if applicable.
- Consult with the lead GSA Service or Staff Office involved and with tenant 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 AFGE and/or NFFE, if applicable.

e. OAS shall:

- Assist PBS, GSA IT, OHRM, and OMA when applicable for GSA-controlled, GSA space.

Appendix B. References and Authorizing Documents

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

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

3. Federal Information Security Management Act of 2002, 44 Code of Federal Regulations, Part 3541, as amended December 18, 2014.

4. National Institute of Standards and Technology:

a. Federal Information Processing Standards 199 – "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

b. Federal Information Processing Standards 200 – "Minimum Security Requirements for Federal Information and Information Systems," March 2006.

c. Federal Information Processing Standards 201-2 – "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013.

d. Federal Information Processing Standards 140-2 – "Security Requirements for Cryptographic Modules," Change Notice 2, December 3, 2002.

e. NIST Special Publication 800-30 – "Guide for Conducting Risk Assessments," Revision 1, September 2012.

f. NIST Special Publication 800-37 – "Guide for the Security Certification and Accreditation of Federal Information Systems," Revision 1, June 5, 2014.

g. NIST Special Publication 800-53.4 – "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, January 22, 2015.

h. NIST Special Publication 800-57 – "Recommendation for Key Management, Part 1: General," Revision 4, January 2016.

i. NIST Special Publication 800-73-4 – "Interfaces for Personal Identity Verification," Revised February 8, 2016.

j. NIST Special Publication 800-76-2 – "Biometric Specifications for Personal

Identity Verification," July 2013.

k. NIST Special Publication 800-78-4 – "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," May 2015.

l. NIST Special Publication 800-116 – "A Strategy for the Use of PIV Credentials in Physical Access Control Systems," November 2008.

5. Office of Management and Budget:

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

b. E-Authentication Guidance for Federal Agencies (M-04-04), December 16, 2003.

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

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

e. Acquisition of Products and Services for Implementation of HSPD-12 (M-06-18), June 30, 2006.

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

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

6. Interagency Security Committee:

- The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 1st Edition, August 2013.

7. Federal Chief Information Officers Council and the Federal Enterprise Architecture:

a. Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, Version 2.0, December 2, 2011.

b. Federal Identity, Credential, and Access Management Personal Identity

Verification in Enterprise Physical Access Control Systems, Version 3.0, March 26, 2014.

c. Federal Identity, Credential, and Access Management Security Assertion Markup Language 2.0 Metadata Profile for Backend Attribute Exchange, Version 1.0.0, January 23, 2012.

d. Federal Identity, Credential, and Access Management Security Markup Language 2.0 Identifier and Protocol Profiles for Backend Attribute Exchange, Version 1.0.0, January 23, 2012.

e. Federal Identity, Credential, and Access Management Security Markup Language 2.0 Web Browser Single Sign-on Profile v 1.0.2, Version 1.0.0, March 12, 2014.

8. GSA IT:

a. GSA Order 2100.1J CHGE 1 CIO “GSA Information Technology (IT) Security Policy,” April 28, 2016.

b. GSA Order 2181.1 CIO P “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook,” October 20, 2008.

c. GSA OCIO Information Paper “GSA Response to OMB Request on Security and Privacy Needs,” January 31, 2007.

d. LACS/PACS Deployment Plan developed by the HSPD-12 Program Management Office and the PBS Security Division (dated October, 2009) and submitted to the Office of Management and Budget on February 22, 2010.

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

f. GSA Smart Buildings Implementation Guide, Version 1, March 6, 2015

g. GSA Building Technologies Technical Reference Guide, Version 1.2, September 29, 2016.

h. Configuration Management Guide (CIO IT Security 01-05), Revision 3, July 14, 2015.

9. GSA - Office of Mission Assurance:

- Physical Access Control Systems Memo, 2013.

10. GSA PBS, Office of Facilities Management:

    - Technology Policy for PBS-Owned Building Monitoring and Control Systems, March 31, 2011.