Physical Access Control Systems (PACS) Customer Ordering Guide

June 2024

Physical Access Control Systems (PACS) Customer Ordering Guide

Table of Contents

Physical Access Control Systems (PACS) Customer Ordering Guide

Purpose

This document aims to create a comprehensive ordering guide that assists ordering agencies, particularly contracting officers, in effectively using the GSA Multiple Award Schedules (MAS) to purchase total solutions for Physical Access Control Systems (PACS). This Ordering Guide is not a stand-alone reference - it is recommended that the reader also become familiar with the https://www.acquisition.gov/far/part-8#FAR_Subpart_8_4; FAR 4.13; Federal Supply Schedules, and other source documentation listed on Reference Documents. This Ordering Guide may be revised from time to time. When updates to this publication occur, they will be available on the web in the PACS Customer Ordering Guide.

Additional information to assist ordering agencies in purchasing PACS solutions is available online in the GSA Security and Protection category. This site includes links to other useful GSA websites. Questions concerning this ordering guide should be directed to a Contracting Officer or Manager in the Schedule category Security & Protection/Security Systems, identified in the GSA Points of Contact section.

Background

Homeland Security Presidential Directive-12 [HSPD-12], dated August 2004, mandates the establishment of a government-wide standard for identity credentials for executive branch employees and contractors to improve physical security in federally controlled facilities. In February 2005, the Department of Commerce, National Institute of Standards and Technology (NIST) released the required standard as Federal Information Processing Standards Publication (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. The current version is FIPS 201-3, dated January 2022. The new smart card-based credential is called the PIV card, which employs microprocessor-based smart card technology and is designed to be counterfeit-resistant, tamper-resistant, phishing-resistant, and interoperable across Federal government facilities.

The General Services Administration (GSA) is responsible for supporting the adoption of Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. GSA operates and maintains the Federal Identity, Credential, and Access Management (FICAM) Evaluation Program as part of that responsibility. Vendor products evaluated and approved under this program are placed on the Approved Products List (APL) to enable procurement of conformant products by implementing agencies. Agencies can view the APL at www.idmanagement.gov/fips201/ and use GSA Schedules to purchase compliant solutions.

Recent Policy Announcements

On July 27, 2016, OMB released an update to its Circular A-130, *Managing Information as a Strategic Resource*. This memo sets policy and establishes guidance for managing Federal information resources. The previous version of Circular A-130 was published in 2000.

The following aspects of the update will be significant to customers involved with logical and physical access control, smart card technology, identity management, and associated Security & Protection/Security Systems:

Planning, budgeting, and funding - Agencies shall establish agency-wide planning and budgeting processes in accordance with OMB guidance. In addition, agencies shall plan and budget to upgrade, replace, or retire any information systems for which protections commensurate with risk cannot be effectively implemented. As part of the budgeting process, agencies must identify gaps between planned and actual cost, schedule, and performance goals and develop a corrective action plan to close such gaps.

Governance - In support of agency missions and business needs and coordination with program managers, agencies shall define, implement, and maintain processes, standards, and policies applied to all information resources at the agency in accordance with OMB guidance.

Leadership and Workforce - Agencies must designate a Senior Agency Official for Privacy (SAOP) with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks.

OMB Circular A-130 mandates that the General Services Administration, "*ensure that contract vehicles and services made available to agencies are cost-effective and provide for capabilities*

that are consistent with Government-wide requirements." To that end, we have prepared this PACS Customer Ordering Guide to assist our customer agencies with acquiring compliant, total PACS solutions available through our Multiple Award Schedules (MAS) program.

What is FICAM PACS?

In its basic form, a Physical Access Control System (PACS) is a collection of technologies that control physical access at one or more federal agency sites by electronically authenticating employees, contractors, and visitors and then making an access control decision. These technologies include PACS Infrastructure (Software and System controllers), Validation System software, and PACS PIV Readers (card readers capable of reading the data on a PIV/PIV-I/CAC credential (PIV Readers)). The combinations of these elements are defined as a "topology."

The GSA FIPS 201 Evaluation Program has four different PACS Topologies. They are listed below:

1. 13.01 Topology – This combines three separate PACS categories: PACS Infrastructure, Validation System, and PIV Reader.
2. 13.02 Topology – This combines PACS Infrastructure and Validation into a category called PACS Validation Infrastructure and PIV Reader.
3. 14.02 Topology – Mobile Handheld Validation Reader
4. 20.01 Topology – PACS Wireless Reader

This document will only cover the two primary topologies, the 13.01 and the 13.02, and their defined categories. The 13.01 and 13.02 are put through the same FRTC. The end solution should provide the same capabilities to the government.

The three categories defined by this topology are PACS Infrastructure, Validation System, and PACS PIV Reader. They are further described in the following sections.

The **PACS Infrastructure** is made up of many compatible and interoperable components. Typical components may include:

- PACS application and server (also called the head-end);
- Database and server (often an integral part of the PACS application and server);
- Controllers (also called field panels or door controllers); and
- Workstations (for administration, registration of individuals, help desk, etc.).

Generally, PACS Infrastructure consists of both software and hardware. It runs with field hardware that provides the door control, I/O, or alarm annunciation back to the PACS head end. Field Hardware can consist of I/O controllers, Alarm Controllers, Door Controllers, and Readers. Each component performs a certain function and, together, creates a PACS. Other approaches that meet the functional requirements are also valid.

PACS Infrastructure is a very diverse environment that interoperates with many different subsystems that are outside the scope of the FIPS 201 Evaluation Program. These include:

- Intrusion Detection Systems (IDS);
- Video Management Systems (VMS);
- Visitor Management Systems (also called VMS);
- Enterprise Identity Management Systems (E-IdM); and
- Physical Security Information Management Systems (PSIM).

A **Validation System** provides the necessary functions to identify and authenticate the bearer of a credential according to FICAM Authentication Methods. These methods and the controls necessary to implement them are defined fully in PIV in E-PACS. https://www.idmanagement.gov/docs/pacs-piv-epacs.pdf

A Validation System, as defined by the FIPS 201 Evaluation Program, is tightly integrated with the PACS Infrastructure and the PIV Reader. Typically, a Validation System is made up of several compatible and interoperable components that may include:

- PKI registration and management software.
- PKI validation software.
- Secure controllers (with or without caching capabilities).
- PKI revocation checking (OCSP responders and CRLs).

Validation Systems are generally made up of software and hardware. It may run as an integrated solution with another vendor's hardware, such as a PACS vendor's intelligent controller as in GSA APL topology 13.01, or it can be a single proprietary software and field hardware solution as in 13.02 topology. In some implementations, the field hardware is a secure controller that performs PKI validation (generally using cached information) and acts as an interface between the reader and the door controller. These components could be integrated with other third-party components or in a completely virtual environment. Many Validation Systems are backed by an enterprise PKI validation solution that determines trust anchors and required constraints on the PKI. These enterprise validation solutions may include high availability, consolidated OCSP responders, or SCVP servers. Other approaches that meet the functional requirements are also valid.

A **PIV Reader** is an accepting device, as defined in E-PACS, that provides the human interface, the card interface, and the communications to and from the Validation System. It is installed at a door, portal, or gateway. As an accepting device, a PACS PIV Reader may be a wholly integrated unit, or it may be an assembly of components including:

- Contact smart card reader.
- Contactless smart card reader.
- LCD.
- LED lights.
- Audio announcers.
- PIN pad.
- Biometric Sensors (Fingerprint, Iris, Facial, etc.)
- Communications to a validation system (e.g., Wiegand, RS-485, secure wireless, OSDP, Ethernet).

The PIV Reader is a device installed at the door that performs functions to interact with the credential bearer, the credential itself. This configuration can vary. The Reader must support at least one FICAM authentication

mode defined in PIV in E-PACS and NIST SP 800-116R1 but may also support multi-factor authentication. The Reader may also support optional legacy technologies and credential formats as defined in [FRTC]. Other approaches that meet the functional requirements are also valid.

NOTE: PIV readers are approved as part of a complete solution. Each approval letter lists the approved reader types, associated APL#, and tested PACS solution.

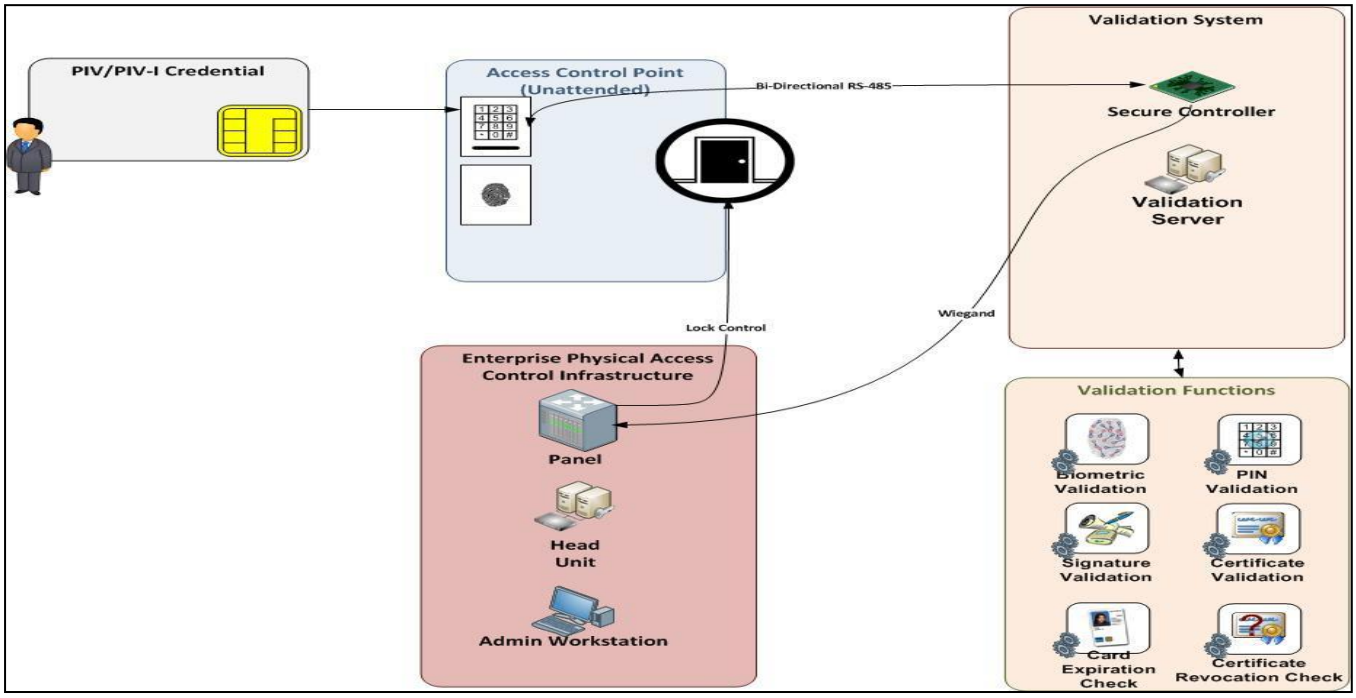


Figure 1 - Sample layout for an End-to-End PACS that incorporates the abovementioned three main categories

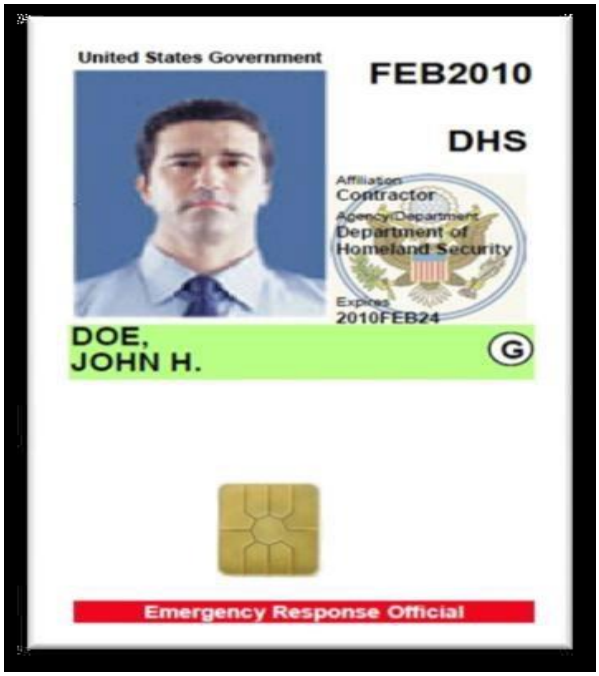


Figure 2 - A final component of an APL PACS is the employee's Personal Identity Verification (PIV) card.

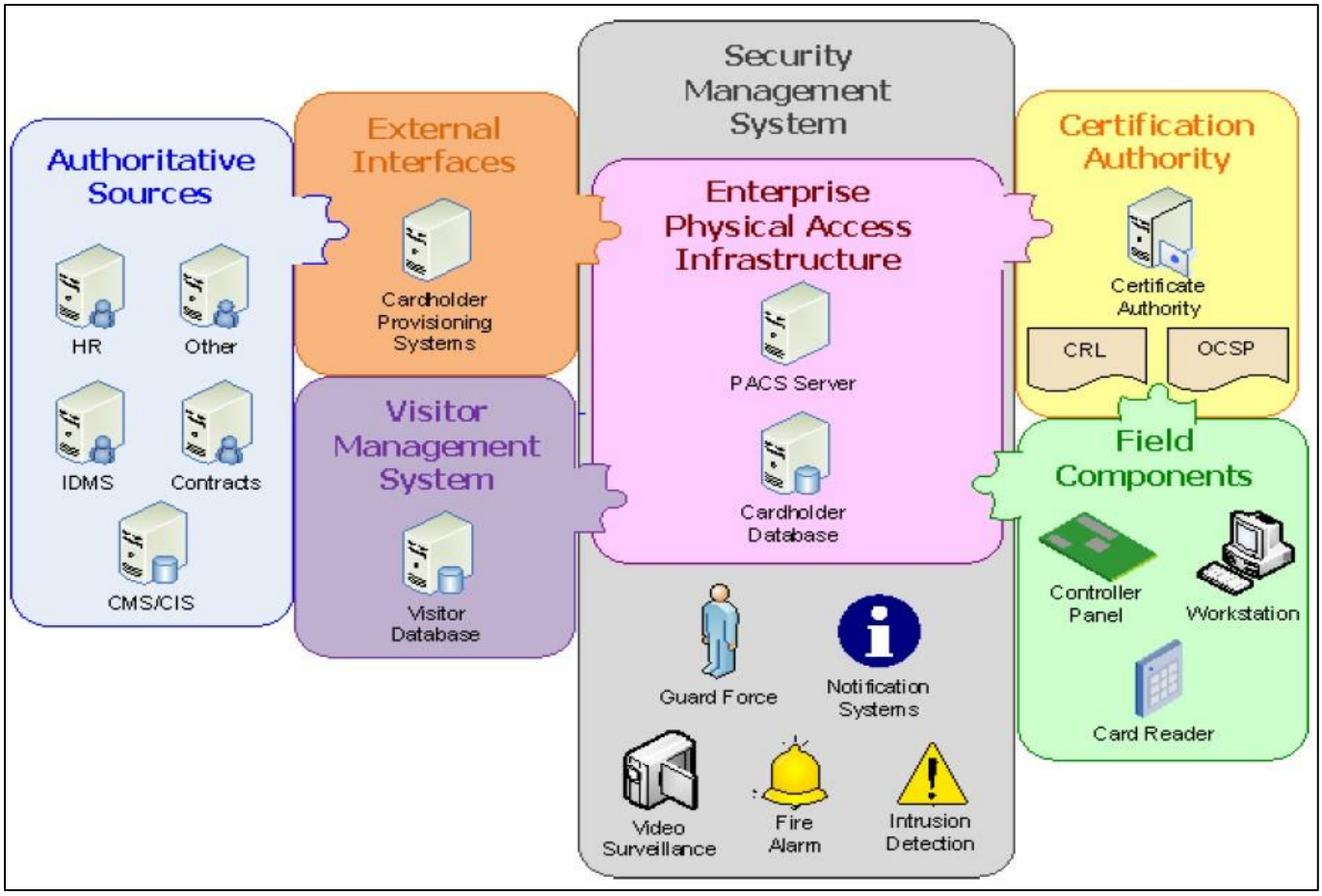


Figure 3 - Sample FICAM APL PACS solution implemented within the overall infrastructure of an agency.

As an end-user agency, where do I start, and what steps are involved?

During the past several years, Agencies developed strategies to modernize their PACS as required in FIPS 201-3.

Today, PACS technologies deployed in many (and growing) Federal buildings are modern FICAM solutions that are interoperable with identity credentials such as PIV, PIV-I, and DoD CAC that may be issued by other Federal Agencies.

A comprehensive step-by-step process that covers Planning, Budgeting, Site Preparations, Project Implementation, Procurement and Life Cycle Management, is available at no charge as a series of webinars:

> *"How to Plan, Procure and Deploy a pacs-Enabled Physical Access Control System* webinar training."

This may be located at: www.idmanagement.gov/university/pacs/

The purpose of the "Guide to GSA PACS An Ordering Guide" is to serve as a simple, reusable template that assists agency Procurement/Contracting professionals in the system section process and ensure that appropriate, GSA APL listed equipment is procured.

Before acquiring a new FIPS 201-3 approved PACS solution, an agency should review existing access control policies and ensure they comply with OMB Memorandum M-19-17. Next, the agency must perform an internal risk assessment of its existing access control systems. This step involves inventorying available equipment and identifying risks and vulnerabilities.

Once a risk assessment is complete, the next step is developing a *migration strategy* for moving facilities to the new APL PACS solution. Continuity of operations planning will be essential to migrating from a deployed PACS to a PIV-enabled PACS. Customers will need to be cognizant of the project budget and total cost of ownership.

Each agency has its unique operational environment. Agencies vary in size, organizational structure, and geographic location. An agency's PACS requirement is driven by its mission. The areas accessible via different access points within a facility do not have the same security requirements. A facility may need multiple authentication levels depending on the types of people in the building (visitors, employees, contractors). The designation of "*Controlled, Limited, Exclusion*" areas within a facility is typically used when drawing up a plan.

Table 1 - Mapping Authentication Factors to Controlled, Limited, and Exclusion Areas.

Security Areas	Number of Authentication Factors Required	Example	Acronym
Controlled	1 - Something you **HAVE** (PIV Card)	Public Key Infrastructure Card Authentication Key	PKI-CAK
Limited	2 - Something you HAVE + **KNOW** (PIV Card + PIN)	Public Key Infrastructure - with PIN number	PKI-AUTH
Exclusion	3 - Something you HAVE, KNOW, and **ARE** (PIV Card + PIN + Biometric)	Public Key Infrastructure - with PIN and Biometric	PKI-AUTH + BIO

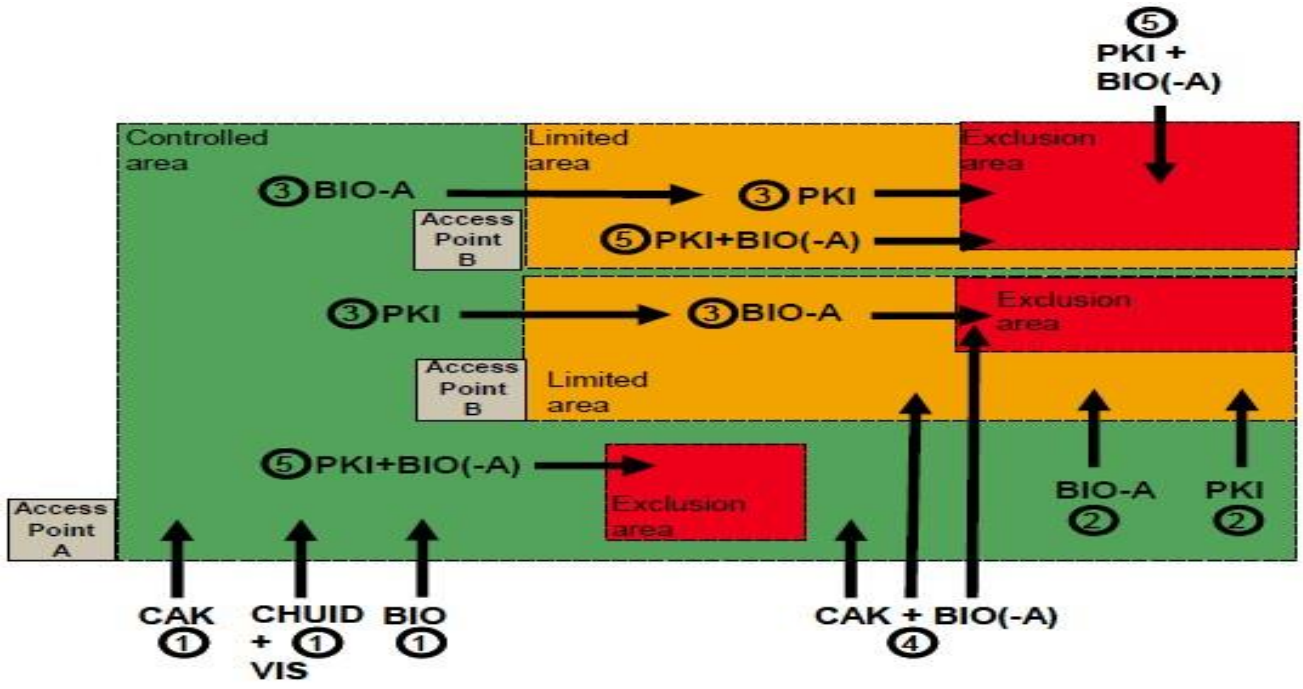


Figure 4 - Examples of Approved Authenticators to move between security zones.

The NIST Special Publication (SP) 800-116 Rev 1 provides more information on PIV authentication factors.

After identifying the appropriate security classification and acceptable authentication factors by access areas for the facility in question, a customer agency should draft a Statement of Work (SOW) that outlines all of the required system upgrades or replacements and then work to secure the necessary funding for the acquisition.

Agencies must procure a FICAM APL-compliant PACS solution in accordance with the Federal Acquisition Regulations (FAR). GSA has over 20 FIPS 201-Compliant solutions listed on the APL. For agencies not part of the Federal government's Executive Branch or HSPD-12 does not apply, legacy PACS solutions and services are available for agencies to purchase through our Multiple Award Schedules (MAS) Program. Please refer to FAR 8.4, Federal Supply Schedules, and the next topic.

In addition, the Ordering Agency IT Security Department shall guide specific FISMA policies as required by local or Agency policies to achieve the installed system's Authority To Operate and/or other IT-related certifications.

What firewall rules should I prepare as an end-user agency before PACS installation?

This is an overview of the firewall rules that should be implemented to revocation check USAccess-issued PIV cards. If the agency uses a different PIV Issuer, get their IP addresses. It assumes that the agency will use the public Internet to check revocations. Check with your agency's IT support, as they may prefer that connections be made to internal resources that provide the same information.

Network Time—Why is this important? Your agency may already have a time source; if not, NIST time is reliable. This helps keep all the PACS computers using the same time for logging, making it easier to find the records during an incident. TIME.NIST.GOV can be redirected to several different servers (IP addresses), so it is recommended that one or two be picked for configuration.

Source IP—These are the IP addresses for the PACS infrastructure involved in logging and revocation checking. They may be individual addresses or a range. Take this into account when submitting the firewall rules request.

Reason Description	Source IP	Destination IP	Protocol	Port	Purpose	FQDN/URL
Network Time Service[1]	Agency PACS IP	Multiple	UDP	123	NIST Time[2]	time.nist.gov
		132.163.96.6	UDP	123	NIST Time	time-e-b.nist.gov
PIV End Entity (user)	Agency PACS IP	23.44.253.48	HTTP	80	AIA Trust Path	sspweb.managed.entrust.com
		216.117.52.142	HTTP	80	AIA OCSP	ocsp.managed.entrust.com
		23.44.253.48	HTTP	80	CRL DP	sspweb.managed.entrust.com
Issuing CA (Intermediate Certificate Store)	Agency PACS IP	23.44.245.220	HTTP	80	AIA Trust Path	rootweb.managed.entrust.com
		216.117.52.142	HTTP	80	AIA OCSP	ocsp.managed.entrust.com
		23.44.245.220	HTTP	80	CRL DP	rootweb.managed.entrust.com
Cross-Certificate (Intermediate Certificate Store)	Agency PACS IP	18.238.192.11, 18.238.192.47, 18.238.192.80, 18.238.192.98	HTTP	80	AIA Trust Path and CRL DP	repo.fpki.gov
					AIA OCSP	None
Federal Common Policy Root CA (Trusted Root Store)	Agency PACS IP	18.238.192.11, 18.238.192.47, 18.238.192.80, 18.238.192.98	HTTP	80	SIA/AIA	repo.fpki.gov

A complete certificate bundle may be found on idmanagement.gov[3]

[1] https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings?tabs=config
[2] https://tf.nist.gov/tf-cgi/servers.cgi
[3] https://www.idmanagement.gov/implement/tools/CACertificatesValidatingToFederalCommonPolicyG2.p7b

Where do I purchase PACS Solutions from GSA?

GSA offers several FIPS 201-compliant and legacy PACS solutions and services for agencies to purchase through the Multiple Award Schedules (MAS) Program. The Secure Technology Alliance provides more information about the certified service component for PACS.

Before an agency customer issues its PACS security solicitation with GSA, it is important to consider the project's breadth and scope. As stated previously, PACS is used as an electronic security countermeasure to control employee and visitor access to a facility. In so doing, PACS is designed to safeguard government assets. For this reason, we direct customers to use the Security & Protection category, Security & Protection/Security Systems subcategory, as the main Schedule vehicle for PACS requirements.

Under **GSA Security & Protection/Security Systems**, the following Special Item Numbers (SINs) apply to PACS.

FIPS 201 Compliant and Approved PACS Components and Services

- 334290PACS Physical Access Control Systems (PACS) FIPS 201 APL
- 541330SEC Security System Integration, Design, Management, and Life Cycle Support
    - Includes the Certified System Engineer ICAM PACS (CSEIP) - labor for installation of APL PACS Solutions. More information about the certified service component for PACS can be found at the Secure Technology Alliance

Legacy PACS Components and Services (*Non-Executive Branch Agencies/Non-FIPS 201 Compliant*)

- 334290L Physical Access Control Systems (PACS)
- 541330L Security System Integration, Design, Management, and Life Cycle Support

How do I purchase a PACS Solution using GSA eBuy?

GSA's eBuy is an online Request for Quotation (RFQ) tool. eBuy is designed to facilitate the request for submission of quotations for a wide range of commercial supplies (products) and services, like PACS, under the GSA Schedules Program offerings.

Federal government agencies can use eBuy to post RFQs, and State and local government entities can use eBuy to post RFQs for certain GSA Schedule supplies and services under the Cooperative Purchasing Program.

When using GSA Schedules to request quotes for a PACS solution, first prepare an RFQ (including the SOW and evaluation criteria) in accordance with FAR 8.4 and post it on eBuy to afford all Schedule PACS contractors a reasonable amount of time and opportunity to respond. See a list of applicable SINs on the previous page. If a facility site visit is needed, please provide the date, time, location, and method to register for a visit properly.

After the RFQ has closed, evaluate all responses received using the evaluation criteria provided in the RFQ to the Schedule contractors. The ordering agency is responsible for considering the level of effort and the mix of labor proposed to perform a specific task being ordered and for determining that the total price offered is reasonable. Next, document the award rationale and issue the task order to the Schedule contractor that represents the best overall value to the Government. After the award, send out notifications of the award decision through eBuy or email. After vendors have received notification of the agency's award decision, be prepared to provide a brief explanation of the award rationale to any unsuccessful offerors upon request.

For detailed training on how to use the e-Buy system, please click here.

Frequently Asked Questions (FAQs)

What is the GSA Schedule Program?

The GSA Schedule program provides eligible ordering activities with a simplified process for obtaining supplies and services. Simply put, the Schedule comprises companies that supply commercial supplies and services through contracts awarded by GSA. With over 20,000 contracts in place, the program offers tremendous choice and flexibility. Schedule contracts are Indefinite Delivery/Indefinite Quantity (IDIQ) contracts awarded to responsible companies that offer commercial supplies or services at fair and reasonable prices. These contracts can be used by eligible ordering activities worldwide. After GSA awards the contracts, ordering activities are ordered from Schedule contractors, and deliveries are made directly to the customer.

FAR Subpart 8.4, Federal Supply Schedules, prescribes procedures that ordering activities must follow when issuing orders against Schedules. By placing an order against a Schedule contract, the ordering activity has concluded that the order represents the best value (as defined in FAR 2.101, Definitions) and results in the lowest overall cost alternative to meet the government's need.

Orders placed against a Schedule contract:

- Are not exempt from acquisition planning as required by FAR Part 7 and agency supplements
- Must follow the ordering procedures outlined in FAR 8.405-1 or -2 and FAR 4.13.
- May be set aside for small businesses at the discretion of the ordering activity Contracting Officer
- Are not exempt from an information technology acquisition strategy as required by FAR Part 39
- Are not exempt from the requirements for a bundled contract when the order meets the definition of "bundled contract" (refer to FAR 2.101 and 13.303-2(c)(3))

The terms and conditions, including all clauses, are available for viewing for the Schedule through the GSA eLibrary. An ordering activity may add terms and conditions to an order that do not conflict with the Schedule contract terms and conditions. Use caution when adding terms and conditions to a Schedule order to ensure no violation of CICA occurs.

What is the difference between the General Services Administration (GSA) Multiple Award Schedule and the Approved Products List (APL)?

GSA Schedule is a purchasing vehicle for a broad range of products and services. The resources on the GSA Schedule have pre-approved vendors and pre-negotiated ceiling rates. The APL lists products and services related to Federal Information Processing Standards 201 (FIPS 201) that have been evaluated per an approved NIST test procedure. An agency can use the GSA Security & Protection/Security Systems subcategory to purchase a compliant PACS Solution included in the APL.

How do I verify that I am obtaining a fully compliant FICAM APL PACS Solution?

The FICAM Testing Program is done so on an end-to-end solution basis, not individual components. This means every new vendor configuration of an approved PACS solution is unique from the others listed on the APL. A fully compliant PACS will have APL Certificate Numbers for each of the three (3) main areas of (1) Infrastructure, (2) Validation, and (3) PIV Card Readers, and must be installed properly by a CSEIP personnel. *See the example below from the APL.*

13.01 PACS Infrastructure:	**13.01 PACS Validation:**	**PIV Reader Name:**	
ABC Security Products - Miracle System	Miracle ABC Security with Validation System	Miracle PIV CAK Contactless Card Reader	Approved
APL #: 6701	APL #: 6702	APL #: 6703	
13.02 PACS Infrastructure and Validation:		**PIV Reader Name:**	
ABC Miracle PACS System and Validation		Miracle PIV CAK/PIV Auth Contact and Contactless Card Reader	Approved
APL # 6704		APL #: 6705	

See idmanagement.gov/fips201/

Who May Purchase from the GSA Schedule?

Federal agencies and other activities are eligible to use GSA sources pursuant to the Federal Property and Administrative Services Act of 1949 or other statutory authority. An eligible ordering activity is authorized to place orders or establish Blanket Purchase Agreements (BPAs) against GSA Schedule contracts. Additional information and a complete list of eligible users are located at www.gsa.gov/eligibilitytouse.

Statutory and Regulatory Foundation Statutory Authority for the MAS Program Title III of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 251 et seq.) and Title 40, U.S.C. 501, Services for Executive Agencies, are the two statutes that authorize the MAS program. The statute states that the use of the GSA Schedule is a competitive contracting procedure since participation in the program has been open to all responsible prospective contractors, and orders and contracts under such procedures result in the lowest overall cost alternative to meet the needs of the government.

The Federal Acquisition Regulation (FAR) provides the primary regulatory guidance for the GSA Schedule program. FAR Subpart 8.4, Federal Supply Schedules, prescribes procedures that federal government ordering activities must follow when issuing orders using the GSA Schedule. Orders placed following these procedures are considered to be issued using full and open competition. (See FAR 8.404(a).)

May State and Local agencies also purchase PACS from the MAS Program?

Yes, under GSA's Cooperative Purchasing Program, state, local, and tribal governments may purchase from Cooperative Purchasing approved industry partners under Security & Protection/Security Systems at any time, for any reason, using any funds available. The COOP PURCH icon and DISAST PURCH icon in both GSA eLibrary and GSAAdvantage indicate that authorized state and local government entities may purchase items from these contracts.

State and local government entities are encouraged to use existing Schedule ordering procedures (refer to FAR Subpart 8.4), but they are not required to do so. When purchasing via the Schedule, state and local governments must meet their own state or local purchasing and competitive requirements. State and local preference programs are not waived or otherwise affected by these regulations.

What are the competition requirements under the GSA MAS Program?

FAR 8.4 states that orders and BPAs placed against the Schedule program are considered to be issued pursuant to full and open competition as long as the ordering procedures are followed. The Schedule program meets the requirements of the Competition in Contracting Act (CICA). Reference 41 United States Code 259(b)(3)(A) and FAR 6.102(d)(3). An acquisition is considered to have been conducted under adequately competitive procedures when ordering activities follow the ordering procedures of FAR Subpart 8.4, Federal Supply Schedules. By placing an order against a Schedule contract, the ordering activity has concluded that the order represents the best value (as defined in FAR 2.101, Definitions) and results in the lowest overall cost alternative to meet the government's need.

GSA Points of Contact for PACS

Daniel Stafford, SSAC (R7) MAS Program Manager

Email: daniel.stafford@gsa.gov

Phone: 817-850-8278

Hannah Auer, Security & Protection Category, Contracting Officer

Email: hannah.auer@gsa.gov

Phone: 817-850-5508

OFFICE OF IT SCHEDULE PROGRAMS,
1800 F ST. NW, WASHINGTON, DC 20405
ITCSC@gsa.gov

Office of Government-wide Policy, Office of Technology Strategy, Identity Management Division
FIPS 201 Evaluation Program
FIPS201EP@gsa.gov

Reference Documents

APL	GSA Approved Products List (APL) on IDManagement.gov FIPS 201 Approved Products List - Physical Access Control System Components (idmanagement.gov)
ATO	**Authority To Operate: GSA Risk Management Process. IT Security Procedural Guide: Access Control (AC) CIO-IT Security 01-07.** https://www.gsa.gov/system/files/Access-Control-(AC)-[CIO-IT-Security-01-07-Rev-5]-08-18-2022.pdf
Circular	Office of Management and Budget (OMB) Revision of Circular No. A130, "Managing Information as a Strategic Resource," July 2016 https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-astrategic-resource
Memorandum	Office of Management and Budget (OMB) Memo M-19-17, May 2019 https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
Commentary	Secure Technology Alliance (formerly Smart Card Alliance): OMB Circular A-130 – Managing Information as a Strategic Resource http://www.smartcardalliance.org/publications-smart-card-alliancecommentary-omb-circular-a-130-managing-information-as-a-strategicresource/
DTM-09-012	Directive-Type Memorandums (DTM) Interim policy guidance for DOD physical access control; December 2009; Change 9 is dated August 2018 https://irp.fas.org/doddir/dod/dtm-09-012.pdf
FIPS 201-3	Federal Information Processing Standard 201-3,"Personal Identity Verification (PIV) of Federal Employees and Contractors", January 2022 https://csrc.nist.gov/publications/detail/fips/201/3/final

FIPS201EP	**FICAM Testing Program** **https://www.idmanagement.gov/fips201ep**
HSPD-12	Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors", August 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive12
M-05-24	Office of Management and Budget (OMB) M-05-24, "Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors", August 2005. https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-24.pdf
OMB M-19-17	**M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access** **https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf**
SP800-73-4	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-4, "Interfaces for Personal Identity Verification", May 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-734.pdf
SP800-116 Rev 1	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116 Rev 1, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)", November 2008 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800116r1.pdf

Sample Statement of Work (SOW)

Table of Contents

SAMPLE ACCESS CONTROL SOW

1 Scope of Work.

This is a contract to provide procurement and services to design, install, and configure to site-specific parameters an Enterprise Physical Access Control System, E-PACS, at the following location(s):

The system shall be GSA-approved and included on the GSA APL.

Agency	Street	City	State, Zip	PoC: E mail, Ph

Contracted service providers are held accountable to the Contractor, who, in turn, is responsible to the Government.

1.1. Description of Services – Introduction.

The Contractor shall provide all personnel, equipment supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform the procurement and installation of an Enterprise Physical Access Control System, E-PACS for the facilities listed above as defined in this Statement of Work, SOW. The Contractor shall perform

to the standards in this contract. Contractor deliverables include the removal of antiquated hardware.

1.2. Background.

The [Agency], to achieve compliance with Homeland Security Presidential Directive -12, HSPD-12, related requirements and technical standards [Agency at locations] are now [replacing, upgrading, installing new] PACS. This requires [X number of PACS Credential readers] at [X number of doors] as determined by the site Senior Security Specialist. The PACS components must be included in the GSA Approved Products List, GSA APL (see Technical Description Appendix A; Background & Requirements in Appendix B.)

1.3. Objectives.

The contractor will perform procurement of all required PACS system components, licenses, system design, installation, configuration, and acceptance testing of each credential reader of the PACS to ensure conformance with all parameters in the current version of NIST SP800-116 applied to access control points entering " Controlled", "Limited" and "Exclusion" areas. The system will be installed in locations listed below: [X no of buildings located on locations described above].

1.4. Scope.

The contractor shall provide equipment and services for Procurement, Installation, and Operator Training on [System] for Administration, Registration, Provisioning/De-provisioning, Alarm processing, and Event Log generation and show that registration, provisioning, and subsequent use of an employee's PIV/PIV-I/CAC Credential is completed with certificate validation. All equipment shall be new, unused, and covered under the manufacturer's warranty period. The warranty period shall be no less than 24 months and shall start at [time of installation].

1.4.1. The contractor shall provide a complete set of “As-Built" system drawings at each site. The system drawings shall clearly show each cable, PACS component, server, workstation (Client), and other equipment installed.

1.4.2. The contractor shall provide training to [Specify number and roles of system operators] to be proficient in normal system operations.

1.5. Period of Performance. [List the period of performance for each location]

1.5.1. The contractor is required to perform all work during normal Federal business hours.

Services shall be performed between 8:00 a.m. and 4:00 p.m. Monday through Friday, excluding federal holidays. The recognized Federal Government holidays are New Year’s Day, Dr. Martin Luther King’s Birthday, Washington’s Birthday, Memorial Day,

Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day.

1.6. System Acceptance.

The contractor shall show:

- Registration, provisioning, and subsequent use of an employee's PIV/PIV-I/CAC Credential are completed with certificate validation.

- Each alarm is processed, annunciated on the Alarm monitor in text for New Alarm and Acknowledged Alarm, Cleared Alarm

- Each camera is activated, and video from each camera is displayed on a designated video monitor. (Video surveillance is optional. See Appendix E for examples of optional video equipment. Subsequent references to video equipment may be deleted if not part of the requirement).

- Each event that triggers video from a designated camera causes the system to display video from the correct camera to the correct monitor; the video camera is released as per the established Security Specialist policy. (Video is optional; see Appendix E.)

- The system shall pass a predefined Quality Control test

1.6.1. Quality Control.

The contractor is required to demonstrate that the system runs without off-line errors, reader errors, and alarm errors for a period of 15 business days after the installation work is completed. System acceptance requires that this test is fully and successfully completed. For any equipment made deficient through contractor negligence, the contractor will be financially responsible and will be responsible for replacement.

1.6.2. Special Qualifications.

The contractor's on-site staff shall include at least one current Certified System Engineer ICAM PACS (CSEIP), certified as per GSA requirement (see IDManagement.gov website, HSPD-12 approved service providers).

The contractor on-site staff shall have valid PACS manufacturer training & certification.

1.6.3. Post Award Progress Meetings.

- The contractor agrees to attend any post-award meeting convened by the contracting activity or contract administration office in accordance with FAR as appropriate to review the contractor's performance. The contractor will appraise the Government of problems, if any.

- Appropriate actions shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

1.7. Contracting Officer Representative (COR).

The COR will be identified separately. The COR monitors all technical aspects of the contract and assists in contract administration; maintains written and verbal communications with the contractor; issues government-provided property, drawings, and site entry. The COR is not authorized to change the terms and conditions of the contract.

1.7.1. Government Key Personnel.

The following personnel are considered Key Personnel by the government for each Task Order:

[List Task Order, Key personnel and contact information]

Task Order	First Name	Last Name	Organization	PH:	E Mail

1.7.2. Contractor Key Personnel.

The contractor shall provide a contract manager responsible for the work's performance. The name of this person and an alternate who is authorized to, with full authority, act for the Contractor when the Manager is absent shall be identified in writing to the contracting officer.

The contract manager, or alternate, shall be available during business hours during the Task Order Period of Performance.

1.8. Contractor Travel. Fill out the specific agency/ contract policy language**.**

1.9. Specific requirements

1.9.1. Installation.

The contractor shall acquire and install an Enterprise Physical Access Control System (EPACS) that complies with all relevant HSPD-12 and NIST SP800-116 R1 requirements for card and cardholder authentication and standards for entry to Controlled, Limited, and Exclusion designated areas as determined by the Agency Senior Security Specialist and functions as described in NIST SP800-116 R1. The installation shall be completed one door at a time. No door shall be partially inoperable overnight.

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

1.9.2. Equipment.

All PACS equipment shall be proven to meet HSPD-12 requirements and be included on the GSA Approved Product List, GSA APL. (See IDManagement.gov Approved Product List) The contractor shall submit the GSA APL Approval number for PACS Infrastructure, Certificate Validation System, and Readers. See Appendix A. FAR 52.211-6; Brand Name or Equal is required and incorporated in this acquisition.

1.9.3. Contractor Staff.

At least one employee on the Contractor staff is involved with System Design, Installation, Configuration, Acceptance Testing, Corrective Maintenance, and Preventive maintenance (Life Cycle Management) shall have proven competencies and be certified HSPD-12 CSEIP Service providers. (See GSA IDManagement.gov website)**1.9.3.1. All** on-site install personnel and technical support will be U.S. Citizens and have a favorable U.S. Government National Agency Check or a State Issued Private Security Firm License

1.9.4. Some doors will be interfaced with video equipment for alarm assessment.

The contractor shall install video equipment, Cameras, cabling, storage, and monitor equipment so that a specific alarm event at each such location automatically activates

video equipment and displays the captured images on designated monitor equipment. See Appendix E for examples of optional video equipment.

2.0. General Requirements - Government Support.

The government will make available IP ranges and switch ports in identified communication closets for all required peripherals and network connectivity as required to achieve compliance with
GSA Evaluation Program for FIPS 201 Enterprise Physical Access Control Systems, E-PACS.

2.0.1. Programming.

All programming configurations, software installation, and maintenance will be done on-site.

2.0.2. On-Site programming only.

The contractor will not be authorized to have remote (client) access to network and access control systems to perform maintenance, troubleshoot problems, or apply software systems.

2.0.3. General Contractor responsibilities.

The contractor shall provide all supervision, tools, supplies, equipment, labor, non-personal services, installation, testing, and incidental training on the equipment to properly and successfully complete the work under this contract.

2.1. PACS Equipment.

The contractor will provide PACS card readers, software, cameras, and door hardware, such as electric locking devices, power supplies, controllers, electric door strikes, balanced magnetic door position switches, request-to-exit devices, associated hardware, wiring, and installation.

2.1.1. Connectivity.

2.1.1.1. PACS hardware shall be connected as per manufacturers' specifications.

2.1.1.2. CCTV hardware shall be connected using fiber-optic wiring. Some additional wiring and connectivity may be required. See Appendix E for examples of optional video equipment.

2.1.2. Door Details.

Door details include door locking hardware, Balanced Magnetic Door Position Switches (BMDPS), Request-to-Exit (REX) devices, and associated hardware.

2.1.2.1. **Electric Mortise locks.**

Electric Mortise locks shall be in fail secure mode, normally locked. A cylinder lock may be used to override key entry. The lever on the Exit side opens the door with or without a lock release. Request-to-Exit switch in door lever to mask door alarm (BMDPS). Hinge with electric power transfer for electric mortise lock and REX functions.

2.1.2.2. **Electric Door Strike detail.**

Electric strikes shall be quickly reversible from fail-safe to fail-secure. The strike shall be in fail-secure mode, normally locked. A cylinder lock may be used for key entry override. The request to exit switch may be separate or lever-actuated.

2.1.2.3. **Magnetic lock.**

The magnetic lock shall have a magnetic bond sensor. It may use internal or separate BMSDPS. The push bar provides free exit at all times, with or without lock release—a Request-to-Exit switch in the push bar bypasses the door alarm.

2.1.2.4. **Emergency Exit doors.**

Emergency door exits will include audible buzzers.

2.1.2.5. **Cameras. (Optional, see Appendix E for examples)**

Cameras will be mounted on the inside or outside of the building as determined by [**xxxxx]** and positioned to capture an image of anyone entering or exiting the building. Cameras will be PTZ and feature native digital motion detection to capture a specified target determined by the [xxxxx.]

2.1.3. **AC Connection.**

Install a direct, dedicated electrical connection to the camera from the power panel/source. Directly connecting the camera to an outlet where it can easily be unplugged is prohibited.

2.1.4. **AC Power back up.**

Video and PACS Server AC power circuit shall be connected to the emergency AC backup generator and shall be capable of sustained server operation for 72 Hrs.

2.2. PACS Reader version.

Readers shall be of the current GSA APL listed version as required to maintain compliance with the GSA APL Listing.

2.3. System Operation.

Option: Remote (On-Site client stations) will need to perform administrative capabilities, such as scheduling and viewing access control readers for readers associated with remote (On-Site client stations) stations.

2.3.1. Log-on passwords.
All user and administrator-level logins and passwords required for launching, updating, and manipulating all associated applications of the required software for operating access control and related Security and protection/Security Systems will be US government-owned.

2.4. Operator training.

The contractor will provide face-to-face initial operational training on software operation to System Administrators, System Operators, and Security Officers to gain sufficient knowledge to perform their assigned Role Duties properly.

2.4.1. The software shall include a self-help reference.

2.4.2. Option: to purchase telephonic assistance.

2.5. SOW Period.

The contract covers a period of sixty months (5 years) from the date of acceptance. Payments will be made within 30 days of submission of invoices into Invoicing, Receipt, Acceptance and Property Transfers (IRAPT). The Contractor shall provide detailed invoices to ensure proper payment for services rendered for each month of service.

2.5.1. Options.

The government can execute options with the contractor to expand the stated physical and technological coverage established in the currently listed facilities (EXHIBITS to be included) to any new construction or reconfiguration of currently established facilities.

3.0. Maintenance.

Maintenance actions are restricted to intrinsic equipment failures. Equipment damage due to Acts of God and lifecycle deterioration will be the responsibility of the Government. The Contractor will be responsible for providing a detailed list (MODEL, BRAND, SPECS) of all damaged equipment, including associated Uninterrupted Power Supply (UPS)/battery supply requiring replacement to [XXXX] before installation for Government funding. The remedy for equipment failure is the repair/replacement of the failed item through a written request for the equipment by the contractor for government funding. In addition to equipment failure, the contractor will be responsive to different aspects of service interruption or outage. These include the following:

3.0.1. Full Outage or system failure/non-responsive software/hardware that causes the PACS and/or CCTV not to operate.

3.0.2. Partial Outage, where one or more [XXXX] buildings or entrances/cameras are affected with complete or partial non-operational status.

3.0.3. Equipment-specific, where singular points of failure in equipment are identified, rendering the node in question inoperable and needing replacement/remediation before fully operational service can be restored.

3.1. Failure Reporting

Upon notification by the Contracting Officer Representative (COR) or designee of a failure, the contractor will respond no later than the next business day. The contractor will have technical support for consultation during normal business hours, which is reachable by telephone or email.

3.2. Corrective Maintenance priority scheduling

Downtime of the access control or the CCTVs will be kept to an absolute minimum. The contractor must notify the customer of all projected downtime and estimated time for repair.

3.3. Maintenance activities reporting

The contractor will provide a written report of all services rendered at the time of repairs. All covered equipment will be repaired within three business days. If equipment repair is expected to exceed the three-business-day response time, the contractor will provide written justification as to the nature of the delay in repair/replacement of identified equipment within 24 hours of system evaluation.

4.0. Technical Specifications

PACS Infrastructure consists of:

- One server per vendor specification, PACS application software license for unlimited users to access the server, ACS database, PACS door/reader controllers as required, and integration with PIV certificate system as per GSA APL approval letter.

PACS Readers

PACS base consists of [X indoor and X outdoor readers.] See completed Appendix A to show the proposed brand, number of readers, required authentication factors, number of controllers, certificate validation service, and GSA APL approval numbers.

Option: Increase the number of readers to a minimum of [NN] readers.

4.1. Door Hardware

Strike locks will be fail-secure and have Panic Door Devices/push bars

4.1.1. Emergency Exits.

Emergency exit door hardware shall include buzzers.

4.1.2. Door strikes.

Door strikes shall be quickly reversible from fail-safe to fail-secure.

4.1.3. Emergency Entry Override.

Each facility will have at least one entry override—a key or cipher entry. The method for override entry must protect against simple force impact or surreptitious entry.

5.0. Maintenance Schedule Quality Assurance Plan

The Contractor will propose a maintenance schedule and life-cycle replacement for systems and equipment. The government will approve the plan.

5.1. [XXX] will periodically evaluate the contractor's performance by appointing a representative(s) to monitor performance to ensure services are received. [XXX] representative will evaluate the contractor's performance through intermittent on-site inspections of the contractor's quality control program and receipt of complaints from [XXX] personnel. [XXX] may inspect each task as completed or increase the number of quality control inspections if deemed appropriate because of repeated failures discovered during quality control inspections or because of repeated COR complaints. Likewise, [XXX] may decrease the number of quality control inspections if performance dictates. [XXX] will also receive and investigate complaints from various customer locations. The contractor shall be responsible for initially validating COR complaints. However, the [XXX] representative shall research the validity of complaint(s) in cases of disagreement with the contractor's resolution.

5.2. When all pre-final inspection discrepancies have been corrected, the COR will conduct the final inspection with all or, as necessary, some of the following: program manager, [XXX] representatives, the Contractor, and any subcontractors. The acceptable quality level is 100%.

5.3. All systems will receive quarterly preventive maintenance and warranties (included in the Contract and covered by the contractor). The acceptable quality level is 100%.

5.4. Documented processes performed and any deficiencies found upon maintenance completion will be submitted to COR within five working days. The acceptable quality level is 100%.

5.5. Components found not to operate properly or exceed their lifecycle during preventive maintenance will be repaired or replaced by the contractor, who will submit a written estimate to the COR. The acceptable quality level is 100%.

5.6. A written request for government funding must be approved before the contractor initiates matters beyond inclusive contracted actions, warranties, upgrades, updates, and licenses. The acceptable quality level is 100%.

5.7. The maintenance report will include the following minimum information: the date and time of the service call, the location of the access control system or CCTV, the repairs performed, and the name of the technician performing the repairs. The acceptable quality level is 100%.

6. Protection, Security, and Safety Policies.

6.1. Access and General Protection/Security Policy and Procedures.

The contractor shall be responsible for meeting the access and general protection security policies and procedures for [XXXX. XXXX] and Security personnel will assist when requested by the Servicing Company.

6.2. Physical Security.

The contractor shall safeguard all Government equipment, information, and property provided for contractor use. Government facilities, equipment, and materials shall be secured at the close of each work period.

6.3. Sensitive Information.

The contractor shall not disclose and must safeguard procurement-sensitive information, computer systems and data, Privacy Act data, and government personnel work products obtained or generated in the performance of this contract. This includes the dissemination of protocols and papers not generally available through the protocols and papers not generally available in public literature.

6.4. Disclosure of Information.

The contractor may be required to access data and information proprietary to another Government agency, another Government contractor, or of such a nature that its dissemination or use other than as specified would be averse to the Government's interest. The contractor employees shall not divulge or release data or information developed or obtained under this contract except to authorize Government personnel or upon written approval of the COR. The contractor will not copy or duplicate the information in the administrator's workstation for system management and IAW the Privacy Act of 1974. Information contained in the system for badge/organizational license production will not be downloaded for any purpose.

Unauthorized disclosure of information in the system for access to [XXXX] facilities is prohibited and will require immediate documented reporting upon discovery by the contractor to [XXXX] for processing. The contractor shall not use, disclose, or reproduce proprietary data with a restrictive legend. The contractor shall obtain written permission from the originator before releasing any information. Under Title 18, Sections 793 and 798, the contractor and the contractor employees are liable for any improper release of proprietary government information. The contractor shall direct to the COR all inquiries, comments, or complaints arising from matters observed, experienced, or learned as a result of or in connection with the performance of the contract, the resolution of which may require the dissemination of official information.

6.5. Information Assurance.

If contractor personnel support IA functions, the contractor shall obtain the appropriate agency-approved IA baseline certification before being engaged. The contracting officer will ensure that contractor personnel are appropriately certified and that training is documented. The organization receiving service may provide additional training on local or system procedures. Information Assurance Contractor Training and Certification (JAN 2008).

6.5.1. The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with site requirements. The Contractor shall meet the applicable information assurance certification requirements, including- (1) approved information assurance workforce certifications appropriate for each category and level as listed in the current version of [Agency Policy] and (2) Appropriate operating system certification for information assurance technical positions as required.

6.5.2. Upon the Government's request, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

6.5.3. Contractor personnel without proper and current certifications shall be denied access to DoD information systems to perform information assurance functions.

6.6. System updates.

The contractor will ensure the entire system maintains current Army IA updates to keep in [Agency] compliance. When required by the contracting technician, the contractor will provide a written description of all system updates or upgrades to [Agency] within 5 working days before the scheduled service. The contractor will also provide written notification of all periodic system upgrades/updates that do not require physical assistance by a technician upon the system's initial setup.

6.7. iWATCH Training. (Optional)

The contractor and all associated sub-contractors shall brief all employees on the local iWATCH[4] program (training standards provided by the requiring activity Anti-Terrorism Officer (ATO). iWATCH training will inform employees of the types of behavior to watch for and instruct them on reporting suspicious activity to the appropriate personnel, such as persons taking pictures, watching them, and what buildings have access control, etc. The government will provide an iWATCH training package to the contractor and associated sub-contractor for execution upon acceptance of a contract award. iWATCH training shall be completed within 30 calendar days of contract award and before commencing work performance. Training results (number of employees trained) are to be reported to the COR before work performance.

6.8. Safety.

The contractor and associated subcontractors shall provide a safe and healthful work environment for their employees as prescribed in FAR 52.236-14, 29 CFR Part 1910, pertinent AR 385-10 provisions, and local regulations, policies, and SOPS. They shall safeguard public and government personnel, property, equipment and avoid interruption of Government Operations. The Contractor will report accidents or losses to the Contracting Officer as relevant regulations and standards specify. Whenever the Contractor becomes aware of serious or imminent danger to the Government, civilian or Contractor personnel, the Contractor shall take immediate corrective action.

6.8.1. The contractor shall maintain work areas in a neat, clean, and safe condition. The Contractor shall be responsible for providing, installing, and removing any temporary signage, barriers, barricade tape, etc., which may be required to control pedestrian and/or vehicle traffic in the work area.

[4] https://www.mepcom.army.mil/Home/Contractors/

6.8.2. The contractor shall collect all generated trash, debris, refuse, garbage, etc., and place it in appropriate containers. The aforementioned materials shall be removed from the site by appropriate means daily unless otherwise approved by the COR. Disposal may be outside the limits of government property.

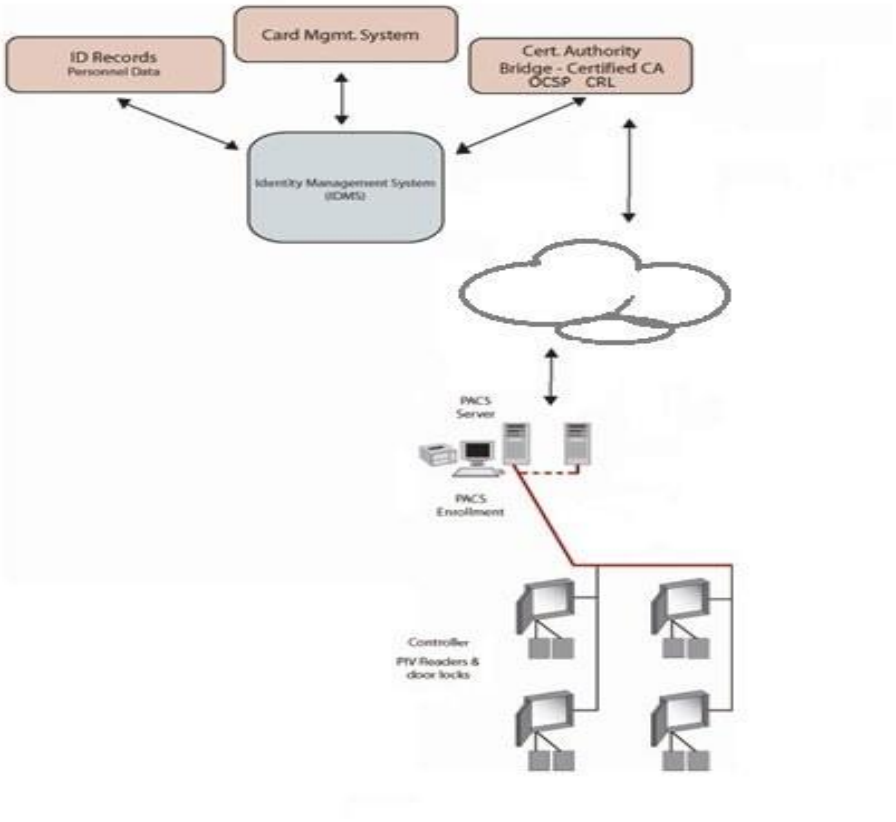
6.9. Applicable Documents.

The Contractor shall ensure all construction for this project is completed within 29 CFR (Code of Federal Regulation) 1910, OSHA General Standards, and 29 CFR 1926, including OSHA Construction Standards, Unified Facilities Criteria (UFC) 3-580-01 Telecommunications Building Cabling Systems Planning and Design, Unified Facilities Criteria (UFC) 3-600-01 Fire Protection Engineering for Facilities, UFC 4-010-01 Minimum Antiterrorism Standards for Buildings, International Building Code, and Uniform Mechanical Code, and DA Technical Guide for Installation Information Infrastructure Architecture (I3A) July 2008. Furthermore, all electrical work shall comply with NFPA Life Safety Code 101, the latest edition of NFPA 70, (National Electric Code) and NFPA standards for communications.

Appendix A - GSA FICAM Approved PACS

Below is an example of a typical small system with a Server, an Internet connection for the Certificate Validation Service, and four two-door controllers. Additional equipment such as workstations (Clients) and video components may be added as required per site-specific policies.

Solicitation from the government shall include the below example:



Item 1: RFI is requesting information for small site FICAM PACS. The site conforms with "NIST SP800-116, Rev 1: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)" Security Area definitions as below:

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

CSEIP Certification is a pre-requisite to respond. Please submit the name(s) of CSEIP Certified staff.

[First Name, Last Name]. (Add rows and columns as required.)

First Name	Last Name	Company	CSEIP Exp. Date

GSA FICAM PACS Approved Products with Certificate Validation are used for each access control point listed below.

FICAM PACS Infrastructure RFI Syntax from Agency:

[Item 1: PACS Infrastructure. Shows location for components and the total number of users in the system]

[Item 2: PACS PIV Certificate Validation System. It shows the location and number of units and describes how PIV Certificates are validated during PACS Registration and subsequent use at door entry points. Show location of Registration Reader]

[Item 3: 1 FA Readers for entry to *Controlled* area. Shows location and number of users at each];

[Item 4: 2 FA Readers for entry to. *Limited* area. Shows locations and number of users at each];

[Item 5: 3FA Readers for entry to *Exclusion* area. Shows Location and number of users at each;]

[Item 6: Readers for movements between areas located inside *Controlled* or *Limited* areas. See SP800-116 for details Number of PACS door/reader controllers, if any]

[Item 7: Number of PACS door/reader controllers, if any. (Some brands of PACS door controllers may incorporate the PIV Certificate Validation system) Vendor to provide details]

[Item 8: CSEIP Certified Staff List Name(s) Include blank spreadsheet above]

Example: TO: 00033, Agency ABC, 100 Main St, Anycity, NG. 00222

[Item 1: PACS Infrastructure for One Server/ Administrator Workstation to Support Eight PIV Readers]

[Item 2: Certificate Validation System for specified PACS. Certificate Validation during Registration and subsequently at each access door as illustrated]

[Item 3: Three at South Entrance, 300 users; Two at North Entrance, 200 users. All are turnstiles.]

[Item 4: One, Security Room, 15 Users]

[Item 5: One, IT Server Room, 40 Users]

[Item 6: No readers for movements between areas located inside *Controlled* or *Limited* areas]

[Item 7: Number of controllers, if any: For responders to complete]

[Item 7: PIV Auth. certificate validation is done with 3 FA Validation during PIV PACS registration]

[Item 8: CSEIP Certified people: Person 1; Person 2; .....]

Agency provided information in RED Underlined text. Responder Provided Information BLUE text.

Site location	**TO 00033**	**Agency ABC**			
100 Main St	**Anycity**	**Anystate**	**Zip 00222**	**USA**	
Gov Contact	**First name**	**Last name**	**Agency**	**E Mail**	**Phone**
Vendor Contact #1	**First name**	**Last name**	**Company**	**E Mail**	**Phone**
Vendor Contact #2	**First name**	**Last Name**	**Company**	**E mail**	**Phone**

Table 2 - Example: Floor plan showing desired reader locations.

Location	Reader type	Total at entry point
South Entrance, 3 turnstiles	1 FA reader at each turnstile	3
North Entrance, 2 turnstiles	1 FA reader at each turnstile	2
West Hallway entrance	1 FA reader at hallway entry	1
1st floor, Security Room	2 FA reader at Security room	1
1st floor IT Server Room	3 FA reader at IT Server room	1

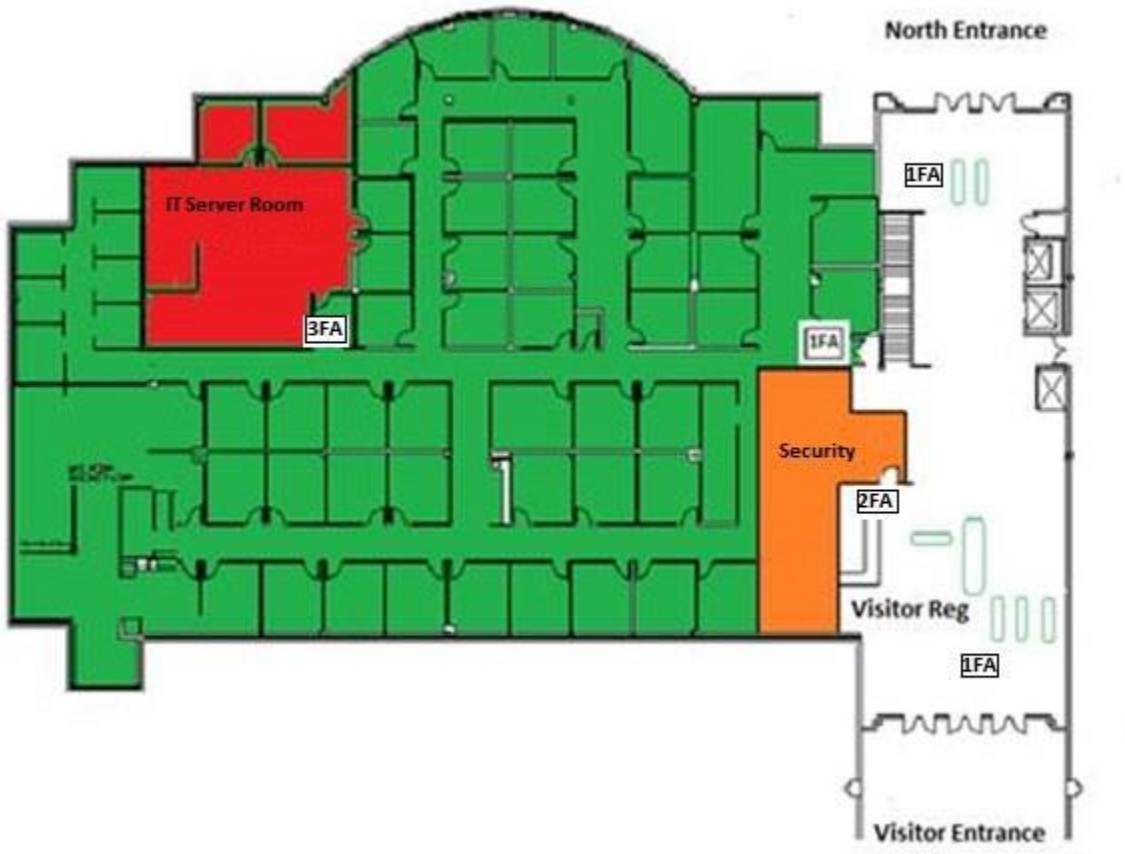


Figure 5 - Sample Floor Plan.

Sample PACS Ordering Spreadsheet Template G2B (Government to Vendors)

The agency provided information in RED Underline text.

Item	Equipment	Brand	APL No. & CSEIP No.	Qty	GSA Price, ea.:	Price total
01	PACS Infrastructure			01		
02	PIV Certification System for PACS Includes Certificate Validation at PACS Registration and at each door as per current version of SP 800-116			NN		
03	Reader to "Controlled" area			06		
04	Reader to "Limited" area			01		
05	Reader to "Exclusion" area			01		
06	Reader for Internal movement "Same to Same" (See current version of SP 800-116)					
07	PACS Controller(s)					
	Professional Services					
	Labor	**Function**	**CSEIP Expiration date**	**Qty**	**GSA Price, ea.:**	**Price total**
08	Labor Category, CSEIP Services System Engineering & Documentation Hrs.					
09	Labor Category CSEIP Services System Design Hrs.					
10	Labor Category CSEIP Services On-site System configuration, Hrs.					
11	Labor Category, CSEIP Services, Corrective & Preventive maintenance (Lifecycle Services) Hrs.					
12	Labor Category, CSEIP Services Project Management, Hrs.					

Note: Basic hardware installation staff does not require CSEIP Certification Response from vendor shall include the following:

Sample PACS Ordering Spreadsheet Template B2G (Return from Vendor/Responder Instructions)

1. **Indicate if your proposed system is a 13.01 or a 13.02 topology when you complete Item 1 and Item 2 on the Ordering form.**

Definition of Topology 13.01 and 13.02

Topology 13.01: PACS infrastructure and Validation System are separate products from different manufacturers integrated into a FICAM-compliant solution. See Item 1 example 13.01 ABC Security Miracle System and Item 2: 13.01 PACS Validation System Miracle ABC Security Validation System.

Topology 13.02: PACS infrastructure and Validation System are one single product. PACS Infrastructure with Validations System Embedded from one manufacturer. When a 13.02 system is offered, in Item 2, "PACS Certificate Validation, Registration System ", enter: "13.02 N/A".

2. **Example of Responder Provided Information for the above project using a 13.01 Product:**

Item 1: 13.01 PACS Infrastructure
13. Brand name: 13.01 ABC Security, Miracle System APL approval number: 6701 with Server configured as per GSA APL letter of approval.

Item 2: 13.01 PACS Validation System
Brand Name:13.01 Miracle ABC Security Validation System

3. **Example of Responder Provided Information for the above project using a 13.02 Product:**

Item1: 13.02 PACS Infrastructure & Validation System
Brand Name: 13.02 DBEST Super PACS and Validation System

Instruction for Vendor Response to Government FICAM PACS Response Syntax:

Item 1: [PACS Infrastructure Brand Name, 13.01 or 13.02 topology, and APL Approval number and Approval Letter]

Item 2: [(Only used with 13.01 systems) PIV Certificate Validation System Brand and APL Approval number and Approval Letter]

Item 3: [Number of 1FA Readers with APL Approval Number and Brand Name]

Item 4: [Number of 2FA Readers with APL Approval Number and Brand Name]

Item 5: [Number of 3FA Readers with APL Approval Number and Brand Name]]

Item 6: [Number of Readers for access to rooms within Controlled and Limited Areas. This Product category does not require APL# or No]

Item 7: [Number of Controllers with Brand Name, Model, Version, and Reader Capacity] Item

8: [CSEIP Certified Staff]

All the above information is available on the GSA web site:

Buy Identity Products and Services (idmanagement.gov)

Example:

[Item 1: PACS Infrastructure Product Name 1: 13.01 ABC Security Products – Miracle System APL #: 6701, Approval letter attached];

[Item 2: Certificate Validation System for PACS Infrastructure Product Name & Quantity: 13.01 Miracle ABC Security with PIV Auth. Certificate Validation during Registration and at the door to all relevant areas APL 6702, Approval letter attached]

[Item 3: Readers to Controlled Area (1FA) Product Name & Quantity: Five ea. PIV 1FA Readers, Miracle PIV CAK Card Reader, APL #: 6703, Approval letter attached];

[Item 4: Readers to Limited Area (2FA) Product Name & Quantity: One ea. PIV 2FA Readers, Miracle PIV Auth. Card + PIN, APL #: 6704, Approval letter attached];

[Item 5: Readers to Exclusion Area (3FA) Product Name & Quantity: One ea. PIV 3FA reader Miracle PIV AUTH BÍO, APL# 6705, Approval letter attached]

[Item 6: Reader for entry to areas of the same security level within “Controlled” or “Limited” areas

Quantity 0 ea.]. Product category does not require APL # or Approval letter]

[Item 7: APL #: 6701 includes: PACS Infrastructure Door controllers. Each door controller has a capacity for Eight PIV readers. Each door controller includes internal Certificate Validation Service for each connected 1, 2, or 3 FA PIV Readers. Product Name Miracle Door Controller. APL # 6701]

[Item 8 – 12: Labor categories]

The agency provided information in RED UNDERLINE Text. The Responder provided information in BLUE no-underline text showing the Responder's response from the 13.01 example above.

Item	Equipment	Brand	APL No	Q	GSA Price, ea.:	Price total
01	PACS Infrastructure. Used for 13.01 and 13.02.	13.01. ABC Security Products Miracle System	6701	1	$14,500.00	$14,500.00
02	PIV Certificate Validation & Registration System as per current NIST SP800-116 Used with 13.01 only	13.01 Miracle ABC Security includes: -- 01: PIV Registration ABC Miracle, Part #: PIV –Reg. - - 02: PIV Certificate Validation Service Part #: PIV Cert - 03: PIV Active Authentication Service, Part #: PIV- DR Part# PIV DR RDA 5.0	6702	1	$11,000.00	$11.000.00
03	Reader to "***Controlled***" area	Miracle PIV 1FA reader (CAK) reader	6703	5	$335.00	$1,675.00
04	Reader to "***Limited***" area	Miracle PIV 2FA reader PIV Auth (Card + PIN)	6704	1	$355.00	$355.00

05	Reader to "***Exclusion***" area	Miracle PIV 3FA reader PIV Auth + Bio. (Card + PIN + BIO) reader	6705	**1**	**$475.00**	**$475.00**
06	Reader for Internal movement "Same to Same"	Miracle PIV Card Reader	N/A	**0**		
07	PACS Controller(s)	**Miracle Super Eight, Eight door capacity**	**6701**	**1**	**$4000.00**	**$4,000.00**
	Professional Services					
	Labor	**Activity**	**CSEIP Exp**			
08	Labor Category CSEIP Services System Engineering & Documentation Hrs.	**System Engineering includes component communication, bandwidth calculations and system documentation**	**Dec 2025**	**6**	**$270.00**	**$1,620.00**
09	Labor Category CSEIP Services System Design Hrs.	**Equipment location and design as per site specific security policies**	**Dec 2025**	**7**	**$270.00**	**$1,890.00**
10	Labor Category CSEIP Services On-site System configuration, Hrs.	**On site system configuration and acceptance test**	**Oct 2025**	**4**	**$275.00**	**$1,100.00**
11	Labor Category, CSEIP Services, Corrective & Preventive maintenance (Life Cycle Services) Hrs.	**On site preventive and corrective maintenance. X hr weekday on site response to CM**	**Jan 2026**	**1**	**$275.00**	**$275.00**
12	Labor Category CSEIP Services Project Management, Hrs.	**Project management and coordination on site and relevant locations**	**Dec 2025**	**2**	**$275.00**	**$550.00**

Note: Basic hardware installation staff does not require CSEIP Certification

---

CSEIP Services: Design, Commissioning, Acceptance Testing, System Documentation.

Responder provided CSEIP Certified Staff: First Name, Last Name, CSEIP Certificate Date

First Name	Last Name	Company	CSEIP exp date
George	Washington	ABC Miracle System	Sept 2026
Andrew	Jackson	ABC Miracle System	Aug 2026
John	Adams	Wonderful Electronics	July 2025

Certificate Validation System:

FICAM APL listed Certificate Validation Service for certificate validation at PACS Registration and at each entry point. Specific to the PACS infrastructure brand.

CSEIP Services:

Professional services by CSEIP Certified Staff for system installation, on-site configuration, commissioning, documentation, and acceptance tests.

Comments:

In a growing number of systems, the Certificate Validation System will reside in the controller and may support all readers connected to the same controller.

Appendix B: GSA Evaluation Program, Approved Product List & Compliance.

Background
The General Services Administration (GSA) supports the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard 201 Evaluation Program (Program) and its Approved Products List (APL), as well as services for Federal Identity, Credentialing and Access Management (FICAM) segment architecture conformance and compliance.

The program provides testing of Enterprise Physical Access Control Systems (E-PACS) for listing on the APL that fully support both Personal Identity Verification (PIV) and PIV Interoperable (PIV-I) credentials. Performance-based requirements for using PIV and PIV-I in E-PACS are detailed in the FIPS 201 Evaluation Program Functional Requirements and Test Cases [FRTC] document.

Office of Management and Budget (OMB) established the authority for these activities in the following memoranda:

OMB Memorandum M-05-24 [M-05-24], Question 5.

"A. **Requirement to use federally approved products and services** – To ensure governmentwide interoperability, all departments and agencies **must** acquire products and services that are approved to be compliant with the Standard and included on the approved products list. B. **Use of GSA Acquisition Services** – The third paragraph states:

Departments and agencies are encouraged to use the acquisition services provided by GSA. Any agency making procurements outside of GSA vehicles for approved products **must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components.**"

This gives GSA the authority to act as executive agent for OMB to ensure that the Program serves the needs of the federal enterprise in an inclusive manner, adhering to the various standards, requirements, interoperability, and conformance as applied within the execution of HSPD-12.

The Program is not the only place that is focused on improvements to E-PACS as a FICAM conformant solution. The latest Federal Information Security Management Act (FISMA) guidance in NIST SP 800-53-5, dated 09/23/2020. [SP800-53-5] adds a new focus to FICAM conformance and security. It now includes E-PACS and focuses on its importance as a

cybersecurity initiative of the Federal enterprise. One of the core controls guiding FICAM conformance in using PIV and PIV-I is:

> IA-5(2) AUTHENTICATOR MANAGEMENT; PKI-BASED AUTHENTICATION The information system, for PKI-based authentication:
>
> (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information;
>
> (b) Enforces authorized access to the corresponding private key;
>
> (c) Maps the authenticated identity to the account of the individual or group; and
>
> (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network".

Per [M-05-24] Question 5. B paragraph 3, Departments and agencies must use products and services selected from the GSA APL.

"Any agency making procurements outside of GSA vehicles for approved products must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components."

> The Program's [FRTC] meets this requirement for E-PACS solutions. It is recommended that the [FRTC] be used as the baseline for any agency's testing program should the agency seek to certify E-PACS products and services independently of the APL.

Appendix C – Normative References

- **[HSPD-12]** Homeland Security Presidential Directive 12, August 27, 2004 https://www.dhs.gov/homeland-security-presidential-directive-12

- **[FIPS 201]** Federal Information Processing Standard 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors https://csrc.nist.gov/publications/PubsFIPS.html

- **[Common]** FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 2.7, February 7, 2024 https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

- **[FBCA]** X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 3.4, February 2, 2024 https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf

- **[APL]** GSA Approved Products List https://www.idmanagement.gov/fips201/

- **[E-PACS]** FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0, March 26, 2014 https://www.idmanagement.gov/docs/pacs-piv-epacs.pdf

- **[FRTC]** FIPS 201 Evaluation Program Functional Requirements and Test Cases https://www.idmanagement.gov/fips201ep/

- **[M-05-24]** Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005 https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-24.pdf

- **[M-19-17]** OMB Memorandum M-19-17, May 21, 2019 https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

- [SP800-37 R2] Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy

- **[SP800-53-4]** National Institute of Standards and Technology (NIST) Special Publication

  (SP) 800-53r5, Security and Privacy Controls for Information Systems and Organizations, 12/19/2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- **[SP800-116 R1]** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116 R1, June 2018 https://csrc.nist.gov/publications/sp

- **Appendix D – Equipment list 1.0 Physical Access Control System: GSA Approved components Ordering Form Template**
  https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwo

Product Category Ordering Template Form, Part B.

Item	Equipment	Brand	APL No	Qty	GSA Price, ea:	Price Total
01	PACS Infrastructure (13.01 & 13.02)					
03	PACS Validation System (13.01 only) PACS Registration include certificate validation as per SP800-116 R1					
03	Reader to "***Controlled***" area					
04	Reader to "***Limited***" area					
05	Reader to "***Exclusion***" area					
06	Reader for Internal movement "Same to Same"					
07	PACS Controller(s)					
	Professional Services					
	Labor	**Activity**	**CSEIP**	**Qty**	**GSA Price, ea:**	**Price Total**
08	Labor Category CSEIP Services System Engineering & Documentation Hrs.					
09	Labor Category CSEIP Services System Design Hrs.					
10	Labor Category CSEIP Services On-site System configuration, Hrs.					
11	Labor Category, CSEIP Services, Corrective & Preventive maintenance (Life Cycle Services) Hrs.					

1.1 Physical Access Control System: General components.

Item No	Equipment	Brand Name	QTY	Unit Price	Total
1	24 VDC Fail Secure Electric strike				
2	24 VDC Power supplies				
3	Electric emergency exit door hardware				
4	Request to exit device Single gang push button momentary NC/NO				
5	Balanced Magnetic door position switch, surface mounted, tamper sensor				
6	Cable 1 Reader to controller	As per manufacturers specification			
7	Cable 2 Controller network to Server	As per manufacturer specification			
8	Cable 3 Door contact to controller	As per manufacturers specification			
9	Cable 4 Power supply to door lock	As per manufacturers specification			
10	Cable 5 Request to exit cable	As per manufacturers specification			
11	Labor category: Installer Hrs.				
12	Labor category: Cabling, termination Hrs.				

Responder provided CSEIP Certified Staff

First Name	**Last Name**	**Company**	**CSEIP exp date**

Appendix E: Example of Optional Video Equipment.

Video equipment is out of Scope for the GSA Approved Product List, APL. No video equipment is included on the list. The sample below is only intended as a generic example.

4.1. Video (CCTV) system.
The video system base consists of [NN] indoor and outdoor cameras.

4.1.1. Option: Identified camera placements to be integrated into the electronic access control system to allow selected video to be viewed and replayed by the PACS Operator

4.1.2. Option: Increase the number of cameras to a minimum of [NN] cameras.

4.1.3. Option: PACS and CCTV will have reserve power or Uninterrupted Power Supply (UPS) for at least six hours.

4.1.3. Option: Video system shall retain captured video for operator replay for [NN] cameras for [NN period of days/hrs.]

4.2. Cameras.
Cameras must be at least [Axis 214 High-Resolution Wide Angle Lens Color Cameras, Low Light Night Vision, Pan Tilt Zoom, Motion Detection Activation] Install [Axis 214 PTZ Hi-Res IP Cameras (or most current version] in all-weather housings on the exterior.

4.2.1. Camera enclosures.
Cameras will be housed in weatherproof enclosures to withstand temperatures below freezing, and interior cameras will be housed to reduce tampering.

4.3. Video programming.
Cameras will be set up and programmed to integrate into software, allowing video viewing, playback, and storage on servers, DVRs, and databases.

4.4. Camera resolution.
The cameras will be set to [4CIF (704 X 480)] resolution with an unlimited video stream and maximum frame rate for a period of [14 days].

****