# Physical Access Control Systems (PACS) Customer Ordering Guide

Vn. 2.0. June 2018

# Physical Access Control Systems (PACS) Customer Ordering Guide

## Table of Contents


Purpose .....3
Background.....3
Recent Policy Announcements.....4
What is PACS? .....5
As an end-user agency, where do I start and what steps are involved? .....7
Where do I purchase PACS Solutions from GSA? .....9
How do I purchase a PACS Solution using GSA eBuy? .....10
Frequently Asked Questions (FAQs) .....11
GSA Points of Contact for PACS.....14
Reference Documents.....15
Sample Statement of Work (SOW) .....17
Appendix A - GSA FICAM Approved PACS simple illustration…… 31
Sample PACS Ordering Template Language, Syntax example……..……...32
Sample floor plan……...34
Sample PACS Ordering Spreadsheet Template G2B (Government to Vendors)…….35
Sample PACS Ordering Spreadsheet Template B2G (Return from Vendor) ….……..37
Appendix B - Background of GSA Evacuation Program……...…..40
Appendix C – Normative References ……...……43
Appendix D – Template for Ordering Spreadsheet…….…..44
Appendix E - Simple Video sample example……..46

# Physical Access Control Systems (PACS) Customer Ordering Guide

## Purpose

This purpose of this document is create a comprehensive ordering guide that assists ordering agencies, particularly contracting officers, to effectively use 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 MAS Desk Reference Version 7 and Federal Acquisition Regulations (FAR) 8.4, Federal Supply Schedules, and other source documentation listed on page 14, Reference Documents. This Ordering Guide may be revised from time to time. Updates to this publication, when they occur, will be available on the web, www.gsa.gov/firesecurity.

Additional information available to assist ordering agencies in purchasing PACS solutions is available online at http://www.gsa.gov/firesecurity; this site includes links to other useful GSA websites. Questions concerning this ordering guide should be directed to a Schedule 84 Contracting Officer or Manager, identified on page 13, GSA Points of Contact.

## 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, 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 201-2, dated August 2013. 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, and interoperable across Federal government facilities.

In February 2011, the Office of Management and Budget (OMB) released memo M-11-11 stating existing physical access control systems must be upgraded to use PIV credentials prior to the agency using development and technology funds to complete other activities." As of today, the issuance of the PIV credentials is virtually complete. Federal agencies are turning their attention to identifying and implementing changes to their physical access control systems (PACS) to support the new PIV card. This memo also required agency PACS transition plans to be in accordance with the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.

The General Services Administration (GSA) is responsible for supporting the adoption of Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the FICAM Testing Program. Vendor products are 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 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 85-page memo sets policy and establishes guidance for management of 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 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 in 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 are required to designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks.

Among other things, 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 that are available through our Multiple Award Schedules (MAS) program.

## What is PACS?

In its basic form, Physical Access Control Systems (PACS) are a particular type of access control system used as an electronic security counter-measure. PACS can be used to control employee and visitor access to a facility and within controlled interior areas. Within the federal government, compliant PACS solutions are made up of three distinct categories, which are the (1) Infrastructure, (2) Certificate Validation System, and (3) Personal Identity Verification (PIV) Card Readers. More information and diagrams about these major categories is discussed below.

The PACS **Infrastructure** is made up of many compatible and interoperable software and hardware components that may include the software application and server (head-end), database, panels, door controllers, and a workstation. The PACS Infrastructure typically interoperates with Intrusion Detection Systems (IDS), Video Management Systems (VMS), and Visitor Management Systems.

The **Certificate Validation System** provides the necessary functions to perform identification and authentication of the individual using the PIV ID card. It is made up of several compatible and interoperable components that may include: servers, validation software that acts as an interface between the card reader and the door controller, and registration and management software. Validation Systems are generally made up of software and hardware components. They can operate on a physical server or cloud-based solution.

The **PIV Card Reader** is an accepting device that performs functions to interact with the bearer of the credential, the credential itself via the Certificate Validation System. It is installed at an access point, door, portal, or gateway. A PIV Card Reader may be a wholly-integrated unit, or it may be an assembly of components including a smart card reader, LCD display; LED lights, audio, PIN pad, Fingerprint/biometric sensors, etc.

Figure 1: Sample layout for an End-to-End PACS that incorporates the three main categories described above.

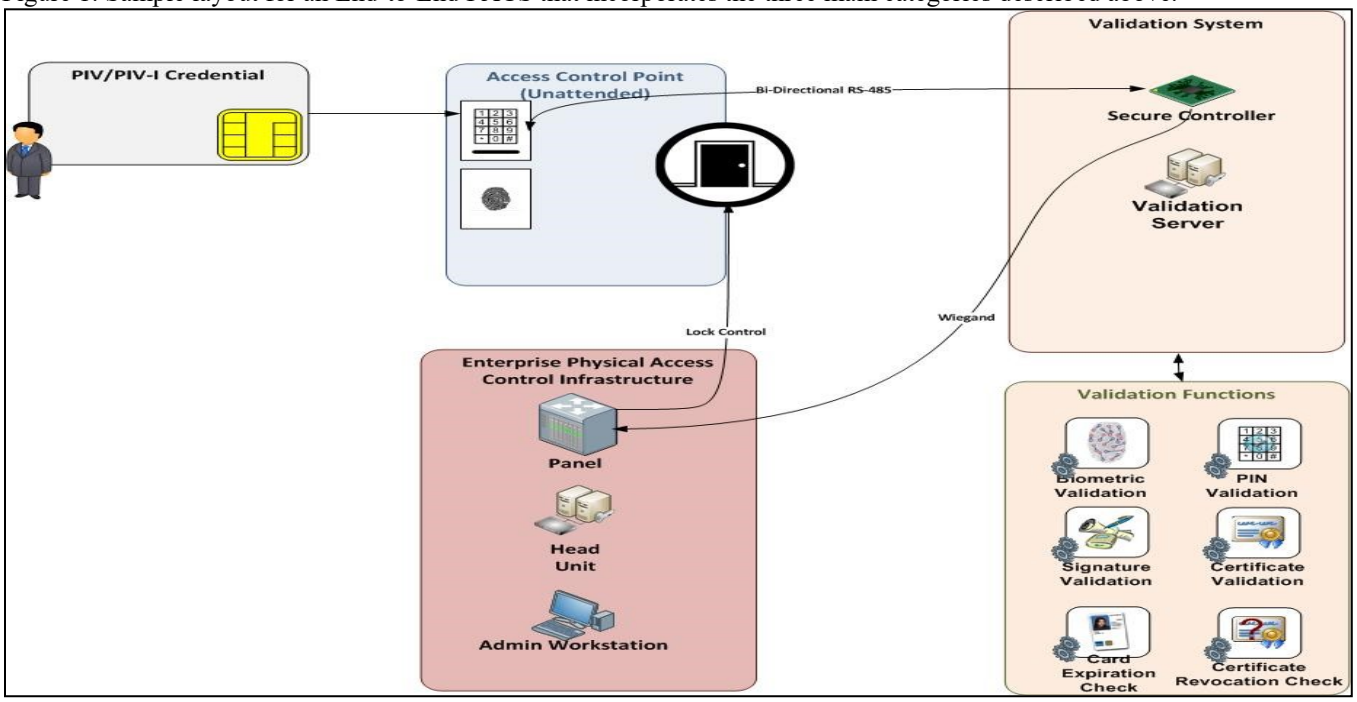
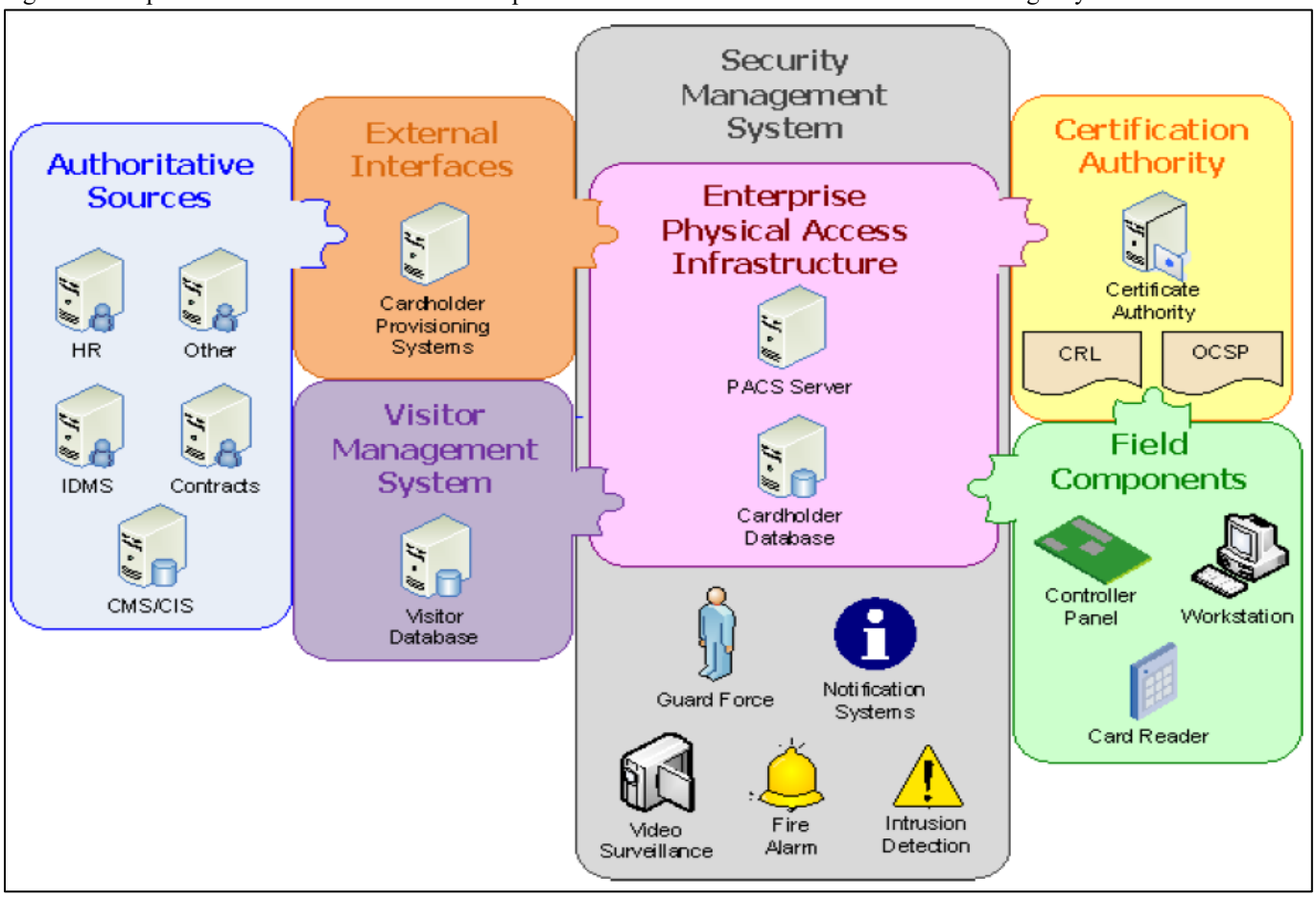


Figure 2: A final component of an APL PACS is the employee's Personal Identity Verification (PIV) card.

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?

The PACS technologies deployed in most Federal buildings are facility-centric and many are not interoperable with other systems. An identity credential issued by one PACS may not have capability to be used by another. It is essential that each agency develop strategies to modernize its PACS to standardized methods as required in FIPS 201-2.

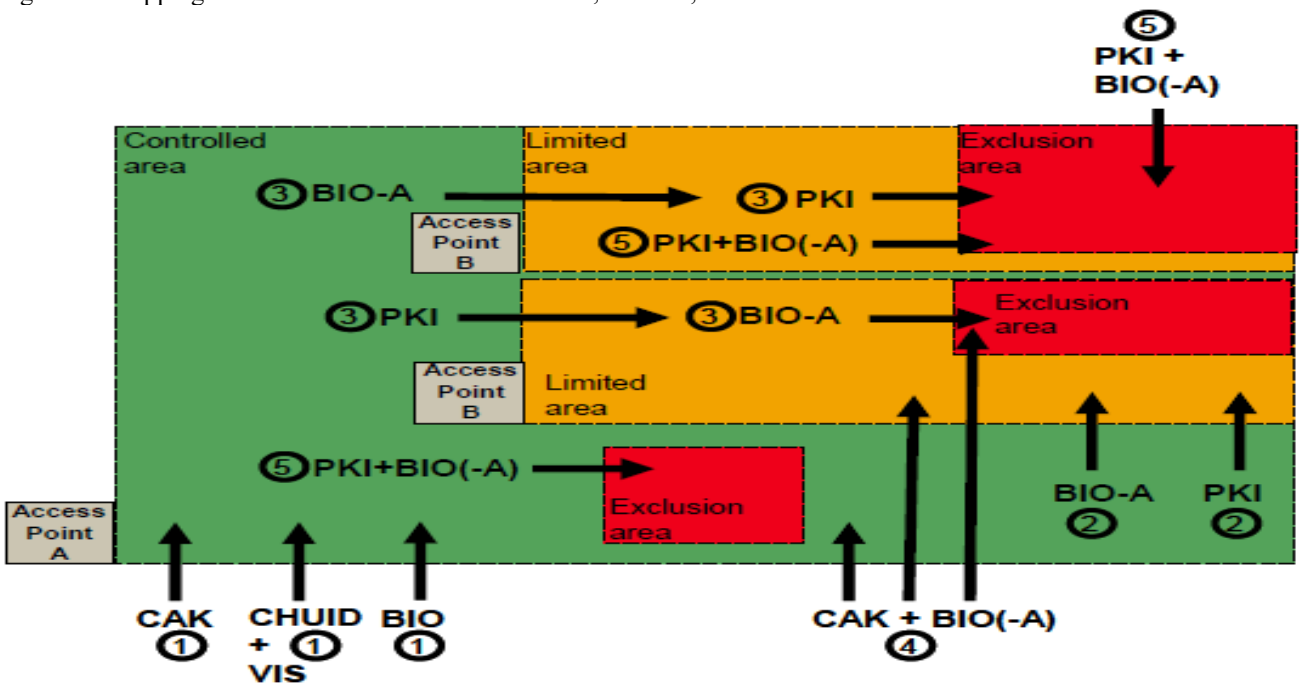
Before moving into the acquisition phase of acquiring a new FIPS 201-2 approved PACS solution, an agency should first review existing policies on access control and ensure it is in compliance with OMB Memorandum M-11-11. Next, an agency will need to perform an internal *risk assessment* of their existing access control systems. This step involves taking an inventory of available equipment, and identifying risks and vulnerabilities.

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

Each agency has its own unique operational environment. Agencies vary in size, organizational structure, and geographic locations. An agency's PACS requirement is driven by its mission. The areas accessible via different access points within a facility do not all 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, are typically used when drawing up a plan.

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

Figure 4: Mapping Authentication Factor to Controlled, Limited, and Exclusion Areas




More information on PIV authentication factors can be found at the NIST Special Publication (SP) 800-116.

After identifying the 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 replacement, and then work to secure the necessary funding for the acquisition.

It is necessary that agencies procure a FICAM APL compliant PACS solution in accordance with the Federal Acquisition Regulations (FAR). GSA has a whole host of FIPS 201 Compliant and legacy PACS solutions and services 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 on pages 9-10.

## Where do I purchase PACS Solutions from GSA?

GSA has a number of FIPS 201 Compliant and legacy PACS solutions and services available for agencies to purchase through the Multiple Award Schedules (MAS) Program. More information about the certified service component for PACS can be found at the Smart Card Alliance.

Before an agency customer issues its PACS security solicitation with GSA, it is important take time to consider the breadth and scope of the project. As stated previously, PACS are used as an electronic security counter-measure to control employee and visitor access to a facility. In so doing, PACS are designed to safeguard government assets. For this reason, we direct customers to use Schedule 84 Total Solutions for Law Enforcement, Security, Facilities Management, Fire, Rescue, Clothing, Marine Craft and Emergency/Disaster Response, as the main Schedule for PACS requirements.

Under **GSA Schedule 84**, the following Special Item Numbers (SIN) are applicable to PACS.

FIPS 201 Compliant and Approved PACS Components and Services

- 246 35 7 Physical Access Control Systems (PACS) FIPS 201 APL
- 246 60 5 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 Smart Card Alliance

Legacy PACS Components and Services (*Non-FIPS 201 Compliant*)

- 246 35 1 Physical Access Control Systems (PACS)
- 246 60 1 Security System Integration, Design, Management, and Life Cycle Support

Depending on the amount of additional IT products and services required, a customer may choose to include the following IT Schedule 70 SIN, along with the above Schedule 84 PACS SINs under the same eBuy RFQ to acquire a PACS solution from multiple vendors. If this strategy is taken, please add language to your SOW regarding **Contractor Teaming Arrangements (CTA)**. For more information on CTAs, please click here.

**IT Schedule 70** – SIN 132 62 Homeland Security Presidential Directive 12 Product and Service Components

## 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 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 list of applicable SINs on previous page. If a facility site visit is needed, please be sure to provide the date, time, location, and method to properly register for a visit.

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 award, send out notifications of the award decision through eBuy or via 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 a detailed training on how to use the e-Buy system, please click here.

## Frequently Asked Questions (FAQs)

**What is the GSA Schedules Program?**

The GSA Schedules program provides eligible ordering activities with a simplified process for obtaining supplies and services. Simply put, a Schedule is comprised of companies that supply comparable 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 order 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 set forth in FAR 8.405-1 or -2
- 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 each 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 Schedules order to ensure that no violation of CICA occurs.

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

GSA Schedules are purchasing vehicles for a broad range of products and services. The resources available on the GSA Schedules have pre-approved vendors and pre-negotiated rates. The APL is a list of Homeland Security Presidential Directive 12 (HSPD-12) related products and services that have been tested per an approved NIST test procedure. An agency can use the GSA Schedule 84 or 70 to purchase a compliant PACS Solution that is included on 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 that every new vendor configuration of a PACS solution that is approved 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 example below from the APL.*

| **PACS Infrastructure:** | **PACS Validation:** | **PIV Reader Name:** | |
|---|---|---|---|
| PACS Infrastructure for AMAG Symmetry | Validation System for AMAG Symmetry | Veridt Bio Dual Contact/Contactless Keypad Reader | Approved |
| APL # : 10087 | APL # : 10086 | APL # : 10031 | |
| **PACS Infrastructure:** | **PACS Validation:** | **PIV Reader Name:** | |
| PACS Infrastructure for AMAG Symmetry | Validation System for AMAG Symmetry | Veridt Stealth Dual Contact/Contactless Keypad Reader | Approved |
| APL # : 10087 | APL # : 10086 | APL # : 10032 | |

**Who May Purchase from the GSA Schedules?**

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 GSA Schedules 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 Schedules program. FAR Subpart 8.4, Federal Supply Schedules, prescribes procedures that federal government ordering activities must follow when issuing orders using GSA Schedules. 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 off the MAS Program?**

Yes, under GSA's Cooperative Purchasing Program state, local and tribal governments to purchase from Cooperative Purchasing approved industry partners under Schedule 84 and 70, 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 are not required to do so. State and local governments must meet their own state or local purchasing and competitive requirements when purchasing via Schedules. 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 Schedules program are considered to be issued pursuant to full and open competition as long as the ordering procedures are followed. The Schedules 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, Schedule 84 Section Chief**

**Email: daniel.stafford@gsa.gov**

**Phone: 817-850-8278**

**Jonathan Woodcock, Schedule 84 Senior Contracting Officer**

**Email: jonathan.woodcock@gsa.gov**

**Phone: 817-850-8373**

**Loren Kolba, Schedule 84 Contracting Officer**

**Email: loren.kolba@gsa.gov**

**Phone: 817-850-5558**

**Kevin Mitchell, Branch Chief, Schedule 84**

**Email:** Kevin.Mitchell@GSA.gov

**Phone: 817-850-5555**

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

## Reference Documents


**APL** GSA Approved Products List (APL) on IDManagement.gov
https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

**Circular** Office of Management and Budget (OMB) Circular No. A-130, "Managing Information as a Strategic Resource," July 2016
https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.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-alliance-commentary-omb-circular-a-130-managing-information-as-a-strategic-resource/

**DTM-09-012** Directive-Type Memorandums (DTM)
Interim policy guidance for DOD physical access control;
December 2009; Change 6 is dated November 2015
http://dtic.mil/whs/directives/corres/pdf/DTM-09-012.pdf

**FIPS 201-2** Federal Information Processing Standard 201-2," Personal Identity Verification (PIV) of Federal Employees and Contractors", August 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

**FICAM Testing Program**
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwi

**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-directive-12

**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. http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf

**M-06-18** Office of Management and Budget (OMB) Memorandum M-06-18, "Acquisition of Products and Services for Implementation of HSPD-12", June 30, 2006
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf

**M-11-11** OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors", February 3, 2011
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

**Roadmap** FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNNBAA4&field=File__Body__s

**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.800-73-4.pdf

**SP800-116** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)", November 2008
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-116.pdf

# Sample Statement of Work (SOW)

**Table of Contents**

1. Scope of Work, SOW.
2. General Requirements
3. Maintenance
4. Technical Specifications
5. Maintenance Schedule, Quality Assurance Plan
6. Protection, Security and Safety Policies
7. Appendix A - GSA FICAM Approved E-PACS
8. Appendix B - Full background & detail of GSA Evaluation Program, Approved Product

**List & Personnel Compliance.**

9. Appendix C - Normative reference documents
10. Appendix D - Example of Equipment List (Blank)

## SAMPLE ACCESS CONTROL SOW

### 1 Scope of Work.

This is a contract to provide procurement and services to design, install, configure to site specific parameters an Enterprise Physical Access Control System, E- PACS, at the following locations(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] in an effort to achieve compliance with Homeland Security Presidential Directive -12, HSPD-12, and 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 Product List, GSA APL (see Technical description Appendix A; Background & Requirements in Appendix B.)

**1.3. Objectives.**

Contractor will perform procurement of all required PACS system components, licenses, system design, installation, configuration, 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 manufacturer's warranty period. Warranty period shall be no less than 24 months and warrant period shall start at [time of installation].

**1.4.1.** The contractor shall provide complete set of "As-Built" system drawings at each site. 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 period of performance for each location]

**1.5.1. Contractor is required to perform all work during normal Federal business hours.**

Services shall be performed between the hours of 8:00 a.m. to 4:00 p.m. Monday through Friday excluding federal holidays. The recognized Federal Government holidays are as follows: New Year's Day, Dr. Martin Luther King's Birthday, Washington's Birthday, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day and Christmas Day.

## 1.6. System Acceptance.

The contractor shall show:

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

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

- That each camera is activated and video from each camera is displayed on designated video monitor

- That each event that shall trigger video from a designated camera causes system to display video from correct camera to correct monitor; video camera is released as per policies established Security Specialist policy.

- The system shall pass a predefined Quality Control test

### 1.6.1. Quality Control.

Contractor is required to demonstrate that the system run 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. Any equipment made deficient through contractor negligence, the contractor will be the financial responsibility and will be responsible for replacement.

### 1.6.2. Special Qualifications.

- The contractor on-site staff shall include at least one current System Engineer ICAM PACS, CSEIP, and Certification 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, site entry. The COR is not authorized to change 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 who shall be responsible for the performance of the work. 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 business hours during the Task Order Period of Performance.

**1.8. Contractor Travel.** Fill with 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, E-PACS that complies with all relevant HSPD-12, NIST SP800-116 requirements for card & cardholder authentication and standards for entry to Controlled, Limited and Exclusion designated areas as determined by Agency Senior Security Specialist and function as

described in NIST SP800-116. The installation shall be completed one door at the 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) Contractor shall submit 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.**

All Contractor staff involved with System Design, Installation, Configuration, Acceptance Testing , Corrective Maintenance, Preventive maintenance (Life Cycle Management) shall have proven competencies and be certified HSPD-12 CSEIP Service providers (See GSA IDManagement.gov web site)

**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.**

Contractor shall install video equipment, Cameras, cabling, storage and monitor equipment so that specific alarm event at each such location shall automatically activate video equipment and display the captured images on designated monitor equipment.

## 2.0. General Requirements - Government Support.

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 and software load, maintenance will be done on-site

### 2.0.2. On-Site programming only.

Contractor will not be authorized remote (client) access to network and access control systems to perform maintenance, trouble shoot problems, or apply software systems.

### 2.0.3. General Contractor responsibilities.

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.

PACS card readers, software, cameras, 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 will be provided by the contractor.

### 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.

### 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. Cylinder lock may be used for key entry override. Lever on Exit side opens door with or without 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. Strike shall be in fail-secure mode, normally locked. Cylinder lock may be used for key entry override. Request to exit switch may be separate, or lever actuated.

#### 2.1.2.3. Magnetic lock.

Magnetic lock shall have magnetic bond sensor. May use internal or separate BMSDPS. Push bar provides free exit at all times with or without lock release. Request -to- exit switch in push bar bypass door alarm

### 2.1.4. Emergency Exit doors.

Emergency door exits will include audible buzzers

### 2.1.5. Cameras.

Cameras will be mounted on either 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 direct, dedicated, electrical connection from power panel/source to camera. Use of direct connect of camera to an outlet where it can easily be unplugged will not be permitted.

### 2.1.4. AC Power back up.

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

## 2.2. PACS Reader version.

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

**2.3. System Operation.**

Option: Remote (On-Site client stations) will need to perform administrative capabilities, e.g., schedule setting and viewing access control readers for readers associated with remote (On-Site client) stations.

**2.3.1. Log- on passwords.**

All user and Administrator level login and passwords required for the launching; updating; and manipulation of all associated applications of the required software for operation of access control and related security systems will be US Government owned.

**2.4. Operator training.**

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 properly perform their assigned Role Duties.

**2.4.1.** Software shall include a self-help reference.

**2.4.2.** Option: to purchase telephonic assistance.

**2.5. SOW Period.**

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

**2.5.1. Options.**

The government will have the ability to execute options with 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 options.

**3.0. Maintenance.**

Maintenance actions are restricted to intrinsic equipment failures. Equipment damage as a result of Acts of God and lifecycle deterioration will be the responsibility of the Government. Contractor will be responsible for providing a detailed list (MODEL, BRAND, SPECS) of all damaged equipment to including associated Uninterrupted Power Supply (UPS)/battery supply requiring replacement to [XXXX] prior to 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 non-operation of the PACS and/or CCTV.

**3.0.2.** Partial Outage, where one or more [XXXX] buildings/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, thus rendering the node in question inoperable and in need of replacement/remediation before fully operational service can be restored.

**3.1. Failure Reporting**

Upon notification by Contracting Officer Representative (COR) or designee of a failure, the contractor will respond no later than the next business day. The contractor will have a 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 written report of all services rendered at time of repairs. All covered equipment will be repaired within three business days. If repair of equipment 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 as per Vendor specification, PACS Application software license for unlimited number of users to access the server, ACS Database, PACS door/reader controllers as required, 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 proposed brand, number of readers, required authentication factors, number of controllers, certificate validation service and GSA APL approval numbers.

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

**4.1. Door Hardware.**

Strike locks will be fail-secure and have Panic Door Devices/push bars or Panic Exit Device Entry Function Lever.

**4.5.1. Emergency Exits.**

Emergency exit door hardware shall include buzzers.

**4.5.2. Door strikes.**

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

**4.5.3. Emergency Entry Override.**

Each facility will have at least one entry override – key entry or cipher entry. Method for override entry must protect against simple force impact or surreptitious entry.

**5.0. Maintenance Schedule Quality Assurance Plan**

Contractor will propose 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 rumination of the validity of complaint(s) in cases of disagreement with 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. Acceptable quality level is 100%.

**5.3.** Preventive maintenance and warrantees (included in the Contract and covered by the contractor) will be performed on all systems quarterly. Acceptable quality level is 100%.

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

**5.5.** Components that are found not to operate properly or exceeds the components' lifecycle during preventive maintenance will be repaired or replaced by the contractor will submit a written estimate to the COR. Acceptable quality level 100%.

**5.6.** A written request for government funding must be approved before contractor initiates matters beyond inclusive contracted actions, warrantees, upgrades, updates and licenses. Acceptable quality level should be 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. Acceptable quality level should be 100%.

## 6. Protection, Security and Safety Policies.

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

The contractor shall be responsible for meeting each of 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 be responsible for safeguarding all Government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

### 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 which are obtained or generated in the performance of this contract. This includes dissemination of protocols and papers not generally available through the 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 adverse 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 contained 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 contained 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 that bears a restrictive legend. The contractor shall obtain written permission of the originator prior to 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,

experience, 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, contractor shall obtain the appropriate Agency approved IA baseline certification prior to being engaged. The contracting officer will ensure that contractor personnel are appropriately certified and training is documented. Additional training on local or system procedures may be provided by the organization receiving service. 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 request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

**6.5.3.** Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

**6.6. System updates.**

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

**6.7. iWATCH Training.**

The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Anti-Terrorism Officer (ATO). iWATCH training will be used to inform employees of the types of behavior to watch for as well as instruct employees on how to report 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 prior to commencing work performance. Training results (number of employees trained) are to be reported to the COR prior to work performance.

**6.8. Safety.**

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

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

**6.8.2.** Contractor shall collect all trash, debris, refuse, garbage, etc., which is generated 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.

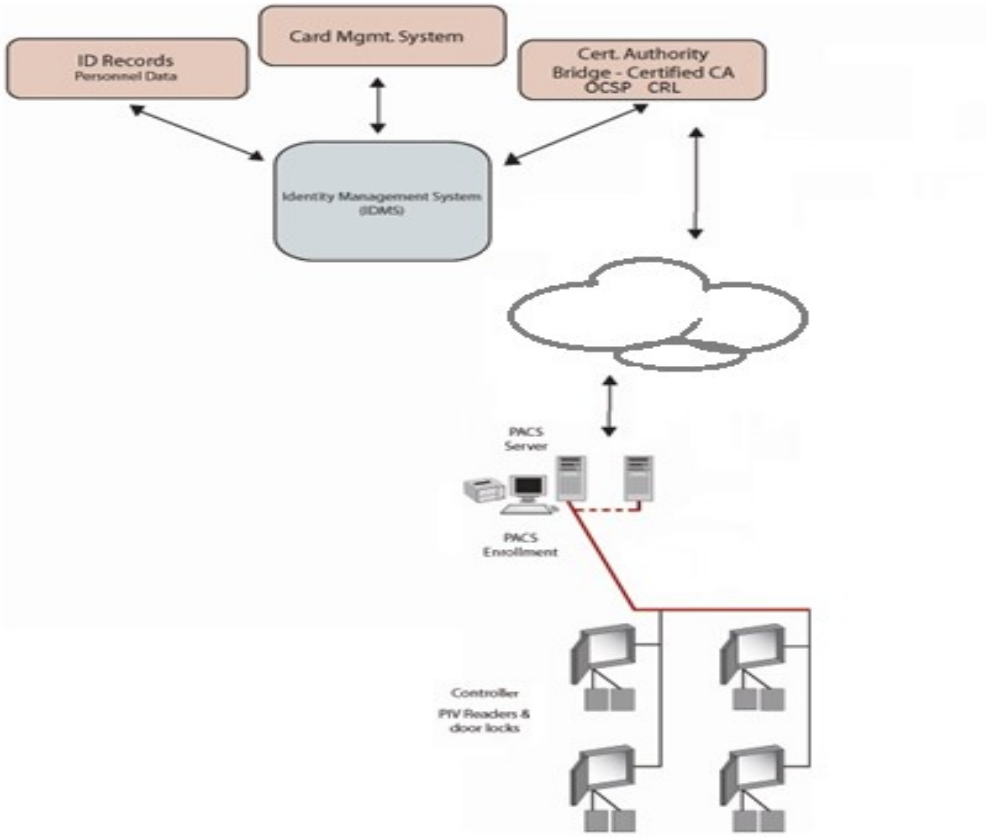
**6.9. Applicable Documents.**

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, to include 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, 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 government shall include the below example:




**Item 1: RFI requesting information for Small site FICAM PACS. Site conforms with "NIST SP800-116:** 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 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 in use for each listed access control point listed below.**

**FICAM PACS Infrastructure RFI Syntax from Agency**:

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

[Item 2: PACS PIV Certificate Validation System. Shows location and number of units and describe how PIV Certificates are validated during PACS Registration and at 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 brand of PACS door controllers may incorporate 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 RED 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** |
| | | | | | |

**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 |

**Agency provided information in RED text**

| Item | Equipment | Brand | APL No. & CSEIP No. | Qty | 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 | | | | | |
| 03 | Reader to "Controlled" area | | | **05** | | |
| 04 | Reader to "Limited" area | | | **01** | | |
| 05 | Reader to "Exclusion" area | | | **01** | | |
| 06 | Reader for Internal movement "Same to Same" (See current version of SP900-116) | | | **0** | | |
| 07 | PACS Controller(s) | | | | | |
| | | | | | | |
| | **Labor** | **Function** | **CSEIP Expiration date** | **Qty** | **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 | | | | | |
| 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:**

FICAM PACS Response Syntax:

Item 1: [PACS Infrastructure Brand Name and APL Approval number and Approval Letter]

Item 2: [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 within 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 above information is available on GSA web site:**

https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

## Example:

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

[Item 2: Certificate Validation System for PACS Infrastructure Product Name & Quantity: 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+BIO, APL# 6705, Approval letter attached]

[Item 6: Reader for entry to areas of 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 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]

**Template response of Responder Provided Information for above Example:**

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

**Agency provided information RED Text** **Responder provided information in BLUE text**

| Item | Equipment | Brand | APL No | Q | Price EA | Price total |
|---|---|---|---|---|---|---|
| 01 | PACS Infrastructure | 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 | **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** |
| | **Services** | | | | | |
| **07** | **Labor** | **Activity** | **CSEIP Exp** | | | |
| 08 | Labor Category CSEIP Services System Engineering & Documentation Hrs | **System Engineering includes component communication, bandwidth calculations and system documentation** | **Dec 2017** | **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 2017** | **7** | **$270.00** | **$1,890.00** |
| 10 | Labor Category CSEIP Services On-site System configuration, Hrs | **On site system configuration and acceptance test** | **Oct 2017** | **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 2017 Oct 2017** | **1** | **$275.00** | **$275.00** |
| 12 | Labor Category CSEIP Services Project Management, Hrs | **Project management and coordination on site and relevant locations** | **Dec 2017** | **2** | **$275.00** | **$550.00** |

**Note: Basic hardware installation staff does not require CSEIP Certification**

---

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

**CSEIP Certified Staff: First Name, Last Name, CSEIP Certificate Date**

| First Name | Last Name | Company | CSEIP exp date |
|---|---|---|---|
| George | Washington | ABC Miracle System | Sept 2020 |
| Andrew | Jackson | ABC Miracle System | Aug 2019 |
| John | Adams | Wonderful Electronic | July 2019 |

**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:**

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

## Appendix B

## Full background & detail of

## GSA Evaluation Program, Approved Product List & Personnel Compliance.

### 1. Background

The General Services Administration (GSA) is responsible for supporting 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 Program1 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 the use of 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 government-wide 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** - 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 provides GSA with 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 to the various standards, requirements, interoperability and conformance as applied within the execution of HSPD-12.

**OMB Memorandum M-06-18 [M-06-18],** Pages 3 and 4:

"Agencies that proceed with the acquisition of products and services for the implementation of HSPD-12 through acquisition vehicles other than GSA IT Schedule 70 must ensure that **only approved products/services from the Approved Product List are acquired and incorporated into system solutions** and ensure compliance with other federal standards and requirements for systems used to implement HSPD-12. In order to ensure government-wide interoperability, this applies for the lifecycle of the products, services, and/or systems being acquired."

In addition**, OMB Memorandum M-11-11** requires that all acquisitions be compliant with the FICAM Roadmap and Implementation Guidance [Roadmap] and that all E-PACS acquisitions be compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116. Specifically:

> "To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:
>
> Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.
>
> Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.
>
> Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.
>
> Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.
>
> The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov)."

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 800-53-4, dated April 2013 [SP800-53-4] adds new focus to FICAM conformance and security. It now includes E-PACS and provides focus on its importance as a Cyber Security 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 are required to 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 [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 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/PubsFIPS.html
- **[Common]** FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.21, December 18, 2012 http://idmanagement.gov/fpki-certificate-policies-cps
- **[FBCA]** X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.26, April 26, 2012 http://idmanagement.gov/fpki-certificate-policies-cps
- **[APL]** GSA Approved Products List http://idmanagement.gov/approved-products-list-apl
- **[E-PACS]** FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), DRAFT Version 2.0.2, May 24, 2012 http://idmanagement.gov/ficam-testing-program
- **[FRTC]** FIPS 201 Evaluation Program Functional Requirements and Test Cases http://idmanagement.gov/ficam-testing-program
- **[M-05-24]** Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005 http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf
- **[M-06-18]** Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006 http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf
- **[M-11-11]** OMB Memorandum M-11-11, February 3, 2011 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
- **[Roadmap]** FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011 http://idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance
- **[SP800-53-4]** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53-4, April 2013 http://csrc.nist.gov/publications/PubsSPs.html
- **[SP800-116]** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008 http://csrc.nist.gov/publications/PubsSPs.html

## Appendix D - Equipment list

### 1.0 Physical Access Control System: GSA Approved components

https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwo

| Item | Equipment | Brand | APL No | Qty | Price EA | Price Total |
|---|---|---|---|---|---|---|
| 01 | PACS Infrastructure | | | | | |
| 02 | PACS PIV Certificate Validation System | | | | | |
| 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) | | | | | |
| 08 | PACS Registration include certificate validation as per SP800-116 | | | | | |
| | **Labor** | **Activity** | **CSEIP** | **Qty** | **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.**

| tem 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 | | | | |

## Appendix E: Example of optional Video equipment.

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

**4.1. Video (CCTV) system.**
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 PACS Operator

**4.1.2.** Option: Increase 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 have weatherproof enclosures to withstand temperatures below freezing. Interior cameras will be housed so as to reduce tampering.

**4.3. Video programming.**
Set up and programming of cameras will be done so as to integrate into software in order to allow viewing of video, playback of video and storage of video on servers, DVR, and data bases.

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

*******