STATEMENT OF WORK (SOW)

FOR

AIR FORCE RESERVE COMMAND'S

PHYSICAL ACCESS CONTROL

SYSTEM (OPTION 1)

Table of Contents

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

1 Scope of Work.

This is a level of effort to provide procurement and services to design, install, and IT integration to site specific parameters of an HSPD-12/FIPS 201-2 compliant Physical Access Control System (PACS), at the following locations(s):

NOTE: *The system shall be GSA-approved and included on the GSA APL. The Govt will validate all contractor responses to this market research to ensure only GSA-approved HSPD 12/FIP 201-2 compliant PACS's and GSA APL-listed equipment are identified in contractor responses.*

Agency	Street	City	State, Zip	POC e-mail/Phone

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

Each RFI must provide a breakdown of costs by building. See Appendix A for more detail.

1.1 Description of Services – Introduction.
The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, IT integration support, supervision and other items as necessary to perform the procurement and installation of a PACS for the facilities listed above as defined in this SOW. The Contractor shall perform to the standards in this contract. Contractor deliverables include the removal of any antiquated hardware/equipment and full IT integration of the PACS with the Air Force's Identity Management System (DEERS).

1.2 Background.
AFRC, in an effort to achieve compliance with Homeland Security Presidential Directive-12 (HSPD-12), and related requirements and technical standards at Headquarters AFRC on Robins AFB, Georgia, intend to replace an existing PACS in Bldg 555 and install the same replacement PACS in the CMC Phase 2 facility (pending construction) with a new GSA-approved, category 334290PAC, PACS. The components associated with this procurement will be integrated into the CMC Phase 3 facility once constructed, a pending (yet-to-be identified) "hoteling" reservation system, and the facility's fire suppression systems. This effort will require a total of 108 PACS credential readers at 108 doors, as determined by the Agency Senior Security Specialist. All proposed PACS components must be included in the GSA's Approved Product List, GSA APL (see Technical description Appendix A; Background & Requirements in Appendix B.)

1.3 Objectives.

The Contractor shall perform procurement of all required PACS components, licenses, system design, installation, configuration, IT integration, and acceptance testing of each credential reader of the [system] 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. Work shall be performed in 2 separate buildings.

1.4 Scope.
The contractor shall provide equipment and services for: procurement, installation, IT integration, and operator training on [system] for administration, registration, provisioning/de provisioning, alarm processing, event log generation, issuance/creation of visitor credentials, and minor maintenance/troubleshooting of the software house and associated equipment. The Contractor shall also demonstrate system performance all of the aforementioned functions at a 100% success rate and IAW the functional requirements and test cases (FRTC) checklist. Tested PIV/PIV-I/CAC credentials must successfully complete real-time/near real-time CAC certificate validation with the Air Force's Identity Management System (DEERS). Additionally, the [system] shall provide both electronic and printed report for on-demand accountability of employees working within each of the facilities the [system] is installed in. All equipment shall be new, unused, and covered under manufacturer's warranty period. Warranty period shall be no

less than 24 months and warranty period shall start on the day the system is accepted by the government.

1.4.1 The Contractor shall provide complete set of “As-Built" system drawings for 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 proof the [system] has approved Authority to Operate (ATO) from an appropriate DoD Chief Information Officer or shall, as supported by the AFRC PACS ISSM and/or AFRC Cybersecurity Rep, successfully process an ATO for the [system] prior to government acceptance.

1.4.3 The Contractor shall provide training to System Administrators and System Operators to be proficient in normal system operations. Training shall be provided on-site after system acceptance and testing has successfully concluded. Training shall include administration, registration, provisioning/de-provisioning, alarm processing, event log generation, issuance/creation of visitor credentials, and minor maintenance/troubleshooting of the software house and associated equipment. The Contractor shall also show registration, provisioning and subsequent use of an employee’s PIV/PIV-I/CAC credential is completed with real-time or near real-time CAC certificate validation to the Air Force’s Identity Management System (DEERS). Training materials, including system administration, operation, and maintenance/troubleshooting guides, shall be provided in both electronic (compact disk, not thumb drive) and hard-copy formats.

1.5 Period of Performance. To be determined.

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

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

Services shall be performed between the hours of 8:00 am to 4:00 pm Monday through Friday excluding federal holidays. The recognized Federal Government holidays are: New Year’s Day, Dr. Martin Luther King’s Birthday, President’s Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran’s Day, Thanksgiving Day and Christmas Day.

1.6 System Acceptance.
The contractor shall demonstrate the following:
• Registration, provisioning and subsequent use of an employee's PIV/PIV-I/CAC credential is completed with certificate validation.
• Each alarm is processed and announced on the alarm monitor in text for new alarm, acknowledged alarm and cleared alarm.
• Visitor credentials can be produced and successfully function tested.
• Each individual door reader is functioning normally.
• Each established “Security Area” function operates with the applicable authentication factors. • PACS conforms with NIST SP800-116 and communicates with the Air Force’s Identity Management System (DEERS).

• Demonstrate report generation as determined by the Agency Senior Security Specialist. • Demonstrate the ability to complete a personnel accountability check of facility occupants. • Demonstrate the ability to perform a full and partial system door lockdown and reset. • Demonstrate to Fire Department staff any PACS-to-fire suppression system integration and all integrated [system] door locks/release mechanisms meets applicable and required OSHA and life safety standards.
• The system shall pass a Quality Control test IAW the FRTC checklist.

1.6.1 Quality Control.
The Contractor shall be 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 this test be fully and successfully completed. Any equipment made deficient through contractor negligence, will be the financial responsibility of the contractor, who will be responsible for replacement.

1.6.2 Special Qualifications.
• The Contractor shall have on-site staff Certified System Engineer ICAM PACS (CSEIP) per GSA requirements (see https://www.IDManagement.gov web site HSPD-12 Approved Service Providers). At least one contractor employee shall hold a CSEIP certification. • The Contractor shall have on-site staff valid PACS manufacturer training and certification.

1.6.3 Post Award Progress Meetings.
• The Contractor and Government to agree to attend a mutually agreed upon location for 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, 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 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:

Duty	First Name	Last Name	Organization	POC e-mail/Phone

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 act with full authority 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 Period of Performance.

1.8 Contractor Travel
This is subject to Federal Travel Regulations.

1.9 Specific requirements

1.9.1 Installation.
The contractor shall acquire and install a PACS that complies with all relevant HSPD-12, NIST SP800-116 requirements for card and cardholder authentication, CAC certification verification/validation, 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. All facility doors shall be secured to Limited access overnight.

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way
FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

Security Areas	Number of Authentication Factors Required
Controlled	1 (PKI-CAK)
Limited	2 (PKI-CAK & PIN)
Exclusion	N/A

1.9.2 Equipment.

All PACS equipment shall be HSPD-12 approved and included on the GSA Approved Product List (GSA APL). Also, see IDManagement.gov (Approved Product List). Contractor shall submit GSA APL approval numbers 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.
The Contractor shall involve its staff 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 https://www.IDManagement.gov web site.

1.9.4 Background Investigations/Licensing.
All on-site install personnel and technical support shall be U.S. Citizens and have a favorable U.S. Government Tier 1 background investigation or a State Issued Private Security Firm License.

1.9.5 Video Monitoring Capability.
PACS will be expendable to interface with video equipment for alarm assessment at a future date. PACS video monitoring capability shall be capable to automatically activating video equipment and display the captured images on designated monitor equipment for specific alarm events at each such location. The Contractor shall not be responsible for installing video equipment, cameras, and associated cabling, storage and monitor equipment at the time of installation.

1.9.6. Hoteling Reservation System Integration Capability.
PACS will be expendable to interface with hoteling reservation system equipment for conference room and office access at a future date. PACS capability shall be capable to automatically provisioning registered users access to reserved rooms/office areas. The Contractor shall not be responsible for installing hoteling reservation system equipment and associated cabling, storage and monitor equipment at the time of installation.

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 is required to achieve compliance with GSA Evaluation Program for FIPS 201-2 PACS. The Government will provide assistance and all necessary artifacts required for contractor to process and obtain the necessary ATO for the [system].

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

2.0.1 Programming.
All programming and software load maintenance shall be done on-site.

2.0.2 On-Site programming only.
The Contractor shall not be authorized remote (client) access to network and access control

systems to perform maintenance, trouble shoot problems or apply software upgrades.

2.0.3 System Scheduling
System controls must support access scheduling for single or multiple entry points on an hourly. Daily, weekly basis. Interior and exterior doors will be scheduled as prescribed by the Govt during installation. System shall allow for immediate administrator override of any previous scheduled configurations. PACS system administrators will coordinate with the contractor on initial system schedule settings for each entry control point.

2.0.4 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.
PACS readers, software, printer, and door hardware (including electric locking devices, power supplies, controllers, electric door strikes, balanced magnetic door position switches, request to exit devices, associated hardware, wiring and installation) shall be provided by the contractor. The Contractor shall be responsible for, and accomplish, any and all connections and interface between PACS readers and door hardware to provide a fully functional and operational access control system.

2.1.1 Connectivity.

2.1.1.1 PACS hardware shall be connected as per manufacturer's specifications.

2.1.2 Door Details.
Door details include (but are not limited to) the following devices and components: door locking hardware, Balanced Magnetic Door Position Switches (BMDPS), Request-to-Exit (REX) devices and associated hardware. The door devices and components shall support a capability to provide on-demand personnel accountability within facilities and office spaces.

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 locks shall have magnetic bond sensors. They shall use internal or separate BMSDPS. Push bar provides free exit at all times with or without lock release.

2.1.4 Emergency Exit doors.
Emergency door exits shall not require audible buzzers.

2.1.5 Cameras.
Cameras shall not be required.

2.1.6 AC Connection.
Install direct, dedicated, electrical connection to all PACS equipment. Use of direct connect of any PACS equipment to an outlet where it can easily be unplugged, thereby defeating/ disabling the PACS shall not be permitted.

2.1.7 AC Power back up.
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 and applicable to the environment (internal/external) they will be used in.

2.3 System Operation.

2.3.1 Log-on passwords.
All user and admin 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.
The Contractor shall provide on-site face-to-face in accordance with paragraph 1.4.3.

2.4.1 Software shall include a self-help reference.

2.4.2 Telephone customer support for troubleshooting user-level matters.

2.4.3 A schedule of available in-residence specialty training at the contractor's facility shall be provided.

2.5 SOW Period.

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

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 and programmed future complex expansion projects.

3.0 Maintenance.
Maintenance actions are restricted to intrinsic equipment failures. Equipment damage as a result of "Acts of God" and/or 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, including associated Uninterrupted Power Supply (UPS)/battery supply requiring replacement, to the COR 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.

3.0.2 Partial Outage, where one or more buildings/entrances 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 COR or designee of a failure, the Contractor shall respond no later than the next business day. The Contractor shall have technical support available for consultation during normal business hours, which is reachable by telephone or email.

3.2 Corrective Maintenance priority scheduling.
Downtime of the access control shall be kept to an absolute minimum. The Contractor shall notify the customer of all projected downtime and estimated time for repair.

3.3 Maintenance activities reporting.
The Contractor shall provide written report of all services rendered at time of repairs. All covered equipment shall be repaired within three business days. If repair of equipment is expected to exceed the three business day response time, the Contractor shall 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 software license for unlimited number of users to access the server.

4.0.1 PACS base.
PACS base consists of 83 interior and 25 exterior readers (108 total). 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.

4.1 Video (CCTV) system. N/A

4.2 Cameras. N/A

4.2.1 Camera enclosures. N/A

4.3 Video programming. N/A

4.4 Camera resolution. N/A

4.5 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 not 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 shall 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
The Contractor shall propose maintenance schedule and life-cycle replacement for systems and equipment. The government will approve the plan.

5.1 The COR will periodically evaluate the contractor's performance to monitor performance to ensure services are received. The COR will evaluate the contractor's performance through intermittent on-site inspections of the contractor's quality control program and receipt of complaints from HQ AFRC personnel. The COR 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 complaints. Likewise, the

COR may decrease the number of quality control inspections, if performance dictates. The COR will also receive and investigate complaints from various customer locations. The contractor shall be responsible for initially validating COR complaints. However, the contracting officer shall provide final resolution of the validity of complaint(s) in cases of disagreement with contractor's resolution.

5.2 Upon completion of all pre-final inspection discrepancies corrections, the COR will conduct the final inspection with all or as necessary some of the following: program manager, 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) shall 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 found to operate improperly or which exceed the components' lifecycle during preventive maintenance shall be repaired or replaced by the contractor. The Contractor shall submit a written estimate to the COR. **Acceptable quality level should be 100%.**

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

5.7 The maintenance report shall include the following minimum information: the date and time of the service call, the location of the access control system, the specific 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 Robins AFB, Georgia. The COR and AFRC access control staff 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 public literature.

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

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 shall not allow employees to 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 shall not copy or duplicate the information contained in the administrator's workstation for system management in accordance with 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 HQ AFRC facilities is prohibited, and shall require immediate documented reporting upon discovery by the contractor to the COR 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 Access to Government Information Systems
All contractor employees with access to government information systems shall be provisioned for access to the Air Force's Non-classified Internet Protocol Router Network (NIPRNet) by the COR at commencement of services and must successfully complete required Information Assurance (IA) awareness training prior to access to the information system and then annually thereafter. Additionally, personnel must annually sign the Acceptable Use Policy (AUP). Prior to issuance of network access, all contractor and associate sub-contractor employees shall complete training, sign the Acceptable Use Policy and any additional training as required. To maintain network access, all contractor and associate sub-contractor employees shall complete refresher and/or annual training as required. All IA workforce personnel shall be appointed and be registered.

6.6 Information Assurance (IA)
The Contractor personnel shall support IA functions, contractor shall obtain the appropriate DoD approved IA baseline certification prior to being engaged. The Government will ensure that contractor personnel are appropriately certified and training is documented. Additional training on local or system procedures may be provided by the AFRC organization receiving service.

6.6.1 The Contractor shall ensure that personnel accessing information systems have up-to-date and accurate information assurance certification to perform information assurance functions in

accordance with DoD Directive 8140. 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 DoDD

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

8570.01-M and (2) Appropriate operating system certification for information assurance technical positions as required.

6.6.2 Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

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

6.7 System Updates.
The Contractor shall ensure the entire system maintains current, approved IA updates to keep in FIPS 201-2 compliance. The Contractor shall provide written description of all system updates or upgrades to the COR within 5 working days before the scheduled service is required by the contracting technician. The Contractor shall also provide written notification of all periodic system upgrades/updates that do not require physical assistance by a technician after initial system setup.

6.8 Antiterrorism Training
The Contractor shall ensure all employees complete local Antiterorrism (AT) training (training standards administered by the requiring activity Antiterrorism Officer (ATO). AT Level I training shall be used to inform employees of the types of behavior to watch for as well as instruct employees for reporting suspicious activity to the appropriate Government personnel. The government will provide an AT Level I training to all on-site contractors. AT Level I 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.

6.9 Safety
The Contractor 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. The Contractor shall safeguard public and government personnel, property and equipment, as well as avoid interruption of Government Operations. The Contractor shall report accidents or losses to the Contracting Officer as specified in relevant regulations and standards. The Contractor shall as it becomes aware of serious or imminent danger to Government, civilian or contractor personnel, take immediate corrective action.

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

traffic in the work area.

6.9.2 The Contractor shall collect all trash, debris, refuse, garbage, etc., generated and place it in appropriate containers. The aforementioned materials shall be removed from the site by

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

appropriate means daily, unless otherwise approved by the COR. Disposal may be outside the limits of government property.

6.10 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.

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

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 and items:**FOR MARKET RESEARCH PURPOSES ONLY**

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

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 (PKI-CAK)
Limited	2 (PKI-CAK & PIN)
Exclusion	N/A

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

First Name	Last Name	Company	CSEIP No. / Issue Date

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

FICAM PACS Infrastructure RFI Syntax:
Item 1: TO (Task order # to be determined)

Item 2: [***"Controlled"*** area] To be determined by Senior Security Specialist

Item 3: [***"Limited"*** area] To be determined by Senior Security Specialist

Item 4: [***"Exclusion"*** area] N/A

Item 5: All readers will be capable of being programmed for ***"Controlled"*** and ***"Limited***" access

Item 6: N/A

Item 7: PIV Authentication certificate validation is done within the facility at the Access Control Desk during PIV Registration. DEERS is the Identity Management System.

Item 8: CSEIP Certified Staff List Name(s):

First Name	Last Name	Company Name	POC e-mail/Phone

First Name	Last Name	Company X	
First Name	Last Name	Company X	

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

Agency provided reader locations (General)

Bldg 555	Total # of Internal Readers	Total # of External Readers	Total # of Doors

Phase 2 Facility	Total # of Internal Readers	Total # of External Readers	Total # of Doors

Totals	Total # of Internal Readers	Total # of External Readers	Total # of Doors

Response from vendor shall include the following:

FICAM PACS Response Syntax:
Item 1: [Brand Name and APL Approval number and Approval Letter]
Item 2: [Number of 1FA Readers with APL Approval Number and Brand Name] Item 3: [Number of 2FA Readers with APL Approval Number and Brand Name] Item 4: [Number of 3FA Readers with APL Approval Number and Brand Name] Item 5: [Number of Readers for access to rooms within Controlled and within Limited Areas]
Item 6: [Number of Controllers with Brand Name, Model, Version and Reader Capacity]
Item 7: [Certificate Validation System Name and APL Approval Number] Item 8: [CSEIP Certified Staff]

All above information is available on GSA web site:
https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

Example:
[Item 1: Product Name 1: ABC Security Products - Miracle System APL #: 6701, Approval letter attached];
[Item 2: Five ea. 1 FA Readers, Miracle PIV Card Reader, APL #: 6705];

[Item 3: Two ea. 2 FA Readers, Miracle PIV Card+PIN, APL #: 6702];
[Item 4: not Applicable.]
[Item 5: One PIV 1FA reader inside Controlled Area]
[Item 6: One ABC Miracle Control Panel, Vn. 8.25.1, Eight Readers];
[Item 7: APL #: 76004, includes: PIV Registration ABC Miracle, Part #: PIV -Reg02, PIV Certificate Validation Service Part #: PIV Cert 02, PIV Active Authentication Service, Part #: PIV- DR Part# PIV DR RDA 5.0]
[Item 8 - 12: Labor categories]

Responder Provided Information for above Example:

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

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

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

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

Date Responder Provided Information for above Example:

First Name	Last Name	Company	CSEIP Exp Date

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.

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way

Appendix B

Full background and detail of GSA Evaluation Program, Approved Product List and 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 it's 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 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 must ensure that **only approved products/services from**

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

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." This is (available at www.idmanagement.gov). The Program is not the only place 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,

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

(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 strongly encouraged to use the [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 functional requirements and test cases [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.

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

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

FOR MARKET RESEARCH PURPOSES ONLY
This is not a solicitation intended to obligate the government in any way

Appendix D - Equipment list

1.0 Physical Access Control System: GSA Approved components
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000Sfwo

1.1 Physical Access Control System: General components.

FOR MARKET RESEARCH PURPOSES ONLY

This is not a solicitation intended to obligate the government in any way