SECURE TECHNOLOGY ALLIANCE

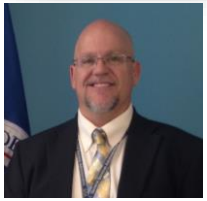
How to Plan, Procure & Deploy a PIV-Enabled PACS

Educational Institute & Access Control Council Webinar Series
Session Four: Develop Procurement Strategy

Introductions

Randy Vanderhoof, Secure Technology Alliance

Lars Suneborn, Secure Technology Alliance



Kevin Mitchell, General Services Administration

Daryl Hendricks, General Services Administration

Jason Rosen, U.S. Capitol Police

SECURE TECHNOLOGY ALLIANCE

Who We Are

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

SECURE TECHNOLOGY ALLIANCE

Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

Access Control Council

… focuses on **accelerating** the widespread **acceptance, use, and application of secure technologies** in various form factors **for physical and logical access control**. The group brings together, in **an open forum**, leading users and technologists **from both the public and private sectors.**

COUNCIL RESOURCES

White Papers

- Commercial Identity Verification (CIV) Credential: Leveraging FIPS 201 and the PIV Card Standards
- A Comparison of PIV, PIV-I and CIV Credentials
- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance Summary
- FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems
- FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience
- Guide Specification for Architects and Engineers for Smart Card-based PACS Cards and Readers for Non-government PACS
- Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses
- PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide
- Smart Cards and Biometrics
- Strong Authentication Using Smart Card Technology for Logical Access
- Supporting the PIV Application in Mobile Devices with the UICC

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

National Center for Advanced Payment and Identity Security

National Center for Advanced Payments and Identity Security

- **National Center for Advanced Payments and Identity Security** in Crystal City
- **Secure Technology Alliance Educational Institute** is part of the center.
- **Certifications Available**
  - **CSCIP**
  - **CSCIP/Payments**
  - **CSCIP/G**
  - **CSEIP**

SECURE TECHNOLOGY ALLIANCE

"Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems." *OMB A-130, 2016*

Procurement Strategy & Requirements Framework

PACS Procurement process:

- Federal Requirements
- What risks are we going to mitigate
  - Based on the facility characterization covered in last session
  - Design & Build
  - Respond to Agency design
- Contract Vehicles
- Budget
- Seek industry proposals
  - Equipment
  - System Design & Implementation services
- Contract award process

GSA's Role

GSA Evaluation Program

- Test and Approves Products, Approved Product List, APL
- Test and Certifies People, Certified System Engineers ICAM PACS

List of both are available at IDManagement.gov

FICAM (The Federal Identity, Credential, and Access Management):

Provides collaboration opportunities and guidance on IT policy, standards, implementation and architecture, to help federal agencies implement ICAM. They also:

- Manage the design, development and implementation of the Federal Public Key Infrastructure (PKI) Architecture in the Federal PKI Shared Service Provider Program; and
- Co-chair the interagency Federal PKI Policy Authority to uphold digital certificate standards for government-wide trusted digital identity and transactions.

GSA's Role Continued

Implementation Guidance

FICAM Roadmap and Implementation Guidance (PDF, December 2011)
https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf

FICAM Architecture Playbook : https://arch.idmanagement.gov/

PIV Usage Guides Playbook : https://piv.idmanagement.gov/

Federal PKI Guides Playbook: https://fpki.idmanagement.gov/

NIST Computer Security Resource Center: http://csrc.nist.gov/

GSA PACS Ordering Guide:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjJosaa7eHYAhWkl-AKHcYcD70QFggpMAE&url=https%3A%2F%2Fwww.gsa.gov%2Fcdnstatic%2FGuide_to_PACS_-_REVISED_060717.pdf&usg=AOvVaw1YfLwAtDzUQsPs1O4DVbyZ

GSA FIPS 201 Evaluation Program: Buyers Guide - GSA.GOV

Item	Equipment	Brand	APL No	Qty	Price EA	Price total
01	PACS Infrastructure	ABC Security Products Miracle System	6701	01	$14,500.00	$14,500.00
02	Certificate Validation System with validation during registration and at door locations. PACS Registration include certificate validation as per SP800-116	ABC Certificate Validation System Miracle ABC Security 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	67004	04	$2,150.00	$8,600.00
03	Reader to "Controlled" area	Miracle ABC PIV Card Reader	6705	05	$335.00	
04	Reader to "Limited" area	Miracle PIV Card+PIN	6702	02	$355.00	
05	Reader to "Exclusion " area	Miracle ABC Card+PIN+BIO	6707	01		
06	Reader for Internal movement "Same to Same"	Miracle PIV Card Reader	6705	01	$335.00	
07	PACS Controller(s)	Miracle Super Eight, Eight door capacity	6705	01	$4000.00	

Identify qualified solution providers

GSA FIPS 201 Evaluation Program Certification Program for People.

Registry of Certified System Engineer ICAM PACS (CSEIP)

A registry of active CSEIP members will be maintained on the Secure Technology Alliance web site for public verification of CSEIP status. Certified CSEIPs receive a certificate and a lapel pin.

Note: Click a table heading (Name, Company, or Certified Since) to sort the table by that column. Click twice to reverse the sort direction.

Name	Company	Certified Since	Expiry Date
Stephen Kellar	Defense Contract Management Agency	December 2017	December 2019
Jeffrey Drill	Communications Resource, Inc.	December 2017	December 2019
Collin Smith	Communications Resource, Inc.	December 2017	December 2019
Jorge Medina	TYCO Integrated Security	December 2017	December 2019
Rich Anderson	PSG Global	December 2017	December 2019
Clinton Eppler	Cam-Dex Security Corp	December 2017	December 2019
Eric Eddy	Johnson Controls	November 2017	December 2019
Richard McGinnis	Security Install Solutions, Inc.	October 2017	December 2019
Jason Greenwood	HEI Security	October 2017	December 2019
Jasen Vonheeder	MEI Systems Integrators	October 2017	December 2019
Jose Hernandez	OmniTech Services	October 2017	December 2019
Barry Mims	OmniTech Services	October 2017	December 2019
Sean Eaton	Johnson Controls	October 2017	December 2019
Scott O'Neal	Johnson Controls	October 2017	December 2019
Brandon Sutphin	Johnson Controls	October 2017	December 2019
Sean Reynolds	US Marshals Service	September 2017	December 2019
Jon Bybee	Parsons Corporation	September 2017	December 2019
Dan Burnell	Convergint Technologies	September 2017	December 2019
Edgar Freeze	Security Install Solutions, Inc	September 2017	December 2019
Cheri Pool	Integrated Environments	September 2017	December 2019
Richard Shafer	Xpect Solutions	August 2017	December 2019
Eric Johnson	US Marshal Service	August 2017	December 2019
Tom Owens	E2 Optics	August 2017	December 2019
Rob Weaver	Stanley Black & Decker	July 2017	December 2019

GSA FIPS 201 Evaluation Program: Services

	Labor	Activity	CSEIP Exp	Hrs	Hr Rate	Total
08	Labor Category CSEIP Services System Engineering & Documentation Hrs	System Engineering includes component communication, bandwidth calculations and system documentation	Dec 2017	60	$270.00	
09	Labor Category CSEIP Services System Design Hrs	Equipment location and design as per site specific security policies	Dec 2017	70	$270.00	
10	Labor Category CSEIP Services On-site System configuration, Hrs	On site system configuration and acceptance test	Oct 2017	40	$275.00	
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	10	$275.00	
12	Labor Category CSEIP Services Project Management, Hrs	Project management and coordination on site and relevant locations	Dec 2017	200	$275.00	

OMB's Role

OMB Memorandum M-05-24.

"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."

Who the directive applies to:

- Executive departments and agencies
- Employees of those agencies
- Contractors
- Federally controlled Facilities
- Federally controlled Information Systems

A full copy of the memo can be found at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

SECURE TECHNOLOGY ALLIANCE

Determining Stakeholder Responsibilities:

Building from the other sessions, Stakeholders should be inherent to their disciplines, but collaborate to understand integration requirements.

- **PHYSEC** – Determines types of PACS equipment; Head-in, controllers, readers, and associated systems such as IDS and CCVE.

- **Installation** – Must use GSA approved service providers per FAR 4.13. This includes GSA approved products for PACS and LACS.
  - Technical People from CIO/PHYSEC should be appointed as Contracting Officer's Representative (COR) and should be involved in the development of solicitation Exhibits. COR's should be fully engaged with Project Manager and Stakeholders to ensure progress and oversight.
  - Contracted installers shall have relevant staff be CSEIP Certified and listed on the GSA IDManagement.Gov Website

SECURE TECHNOLOGY ALLIANCE

Identify qualified PACS Products

GSA Evaluation Program

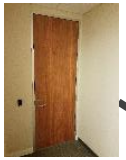
If you have this PACS infrastructure

- **Miracle System ABC**, **APL 6701**, and this

PACS PIV Certificate Validation System, APL 67004

- **ABC Validation System**, you can use these types of card **readers:**
  - ABC Contactless Reader (1FA) **APL 6705**
  - ABC Contact Reader + PIN (2FA) **APL 6702**
  - ABC Contact Reader + PIN + BIO (3FA) **APL 6707**

SECURE TECHNOLOGY ALLIANCE




North Entrance
IT Server Room
1FA
1FA
Main Facility
Security
Lab
Parking Garage
Employee Entrance

Key points of the solicitation

- **Configuration** – The FIPS requirements should be met in the end, however the agency's architecture on how this is accomplished is what varies. Requirements should be given to contractor, validated by owner.

- **Testing –** PLAN! CIO and PHYSEC should require a test plan to ensure not only FIPS compliance, but actual functionality. The test plan should have requirements from the system owner(s) and be developed by the contractor. DO NOT WAIT UNTIL THE END OF THE PROJECT!

- **Training** – DOCUMENT! Training requirements for the various end users must be identified as part of the scope of the installation. Who is doing it? Where it is? Remote/Onsite? Training Booklets

SECURE TECHNOLOGY ALLIANCE

Key points of the solicitation

- **Commissioning –** A commissioning plan should be documented to ensure all requirements are accepted.
- **Operation –** Standard Operating Procedures should be updated and established as per organization
- **Lifecycle management –** Everything has a duration. Years + Technology + Obsolete= Strategy SP800-64

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Contract Vehicles

Schedule 84 Offerings

GSA Schedule 84 offers a total PACS solution by allowing its industry partners to offer products, services, and storage under the following Special Item Numbers (SINs):

For Products – 19 Current Contractors

- **246 35 7** - Physical Access Control Systems (PACS), FIPS 201 APL –
  - Door and parking entry control by card access,
  - Biometrics (facial, iris, fingerprint, voice, etc.),
  - Digital, keyboard, keypad, etc.
  - Also includes vehicle arrest, security barrier, barricade, bollard systems and decorative barrier planters.

For Services – 20 Current Contractors

- **246 60 5** - Security System Integration, Design, Management, and Life Cycle Support
  - Includes any services covered under **246** 60 1 that are to be performed in conjunction with products/systems under **246 35 7** and are in compliance with current GSA FIPS 201 Evaluation Program requirements.
  - Technical evaluation criteria are:
    - Companies shall be listed at IDManagement.gov
    - Companies shall have at least one Certified System Engineer ICAM PACS (CSEIP) listed at IDManagement.gov

Schedule 84 Offerings Continued

For Ancillary Products and Services

246 1000 - Security, Alarm & Signal Systems - Ancillary Supplies and/or Services - Ancillary supplies and/or services are support supplies and/or services which are not within the scope of any other SIN on this schedule.

- These supplies and/or services are necessary to compliment a contractor's offerings to provide a solution to a ordering agency requirement.
- This SIN EXCLUDES purchases that are exclusively for supplies and/or services already available under another schedule.
- Special Instructions:
  - The work performed under this SIN shall be associated with existing SIN(s) that are part of this schedule.
  - Ancillary supplies and/or services shall not be the primary purpose of the work ordered, but be an integral part of the total solution offered.
  - Ancillary supplies and/or services may only be ordered in conjunction with or in support of supplies or services purchased under another SIN(s) of the same schedule.

Schedule 70 Offerings

For Products and Services

132 62 - Homeland Security Presidential Directive 12 Product and Service Components - Products and services for agencies to implement the requirements of **HSPD-12**, FIPS-201 and associated NIST special publications. The **HSPD-12** implementation components specified under this SIN are:

* PIV enrollment and registration services,
* PIV systems infrastructure,
* PIV card management and production services,
* PIV card finalization services,

- Physical access control products and services,
- * Logical access control products and services,
- * PIV system integration services, and
- * Approved FIPS 201-Compliant products and services.

SECURE TECHNOLOGY ALLIANCE

Draft Documents

Request for Information (RFI)

A **request for information** (**RFI**) is a document used to gather **information** from vendors or suppliers in order to create a shortlist of potential suppliers for a project. The purpose of an **RFI** is to collect **information** and compare businesses that are offering products or services that you require to complete a project.

Example Taken from the PACS Order Guide:

GSA PACS
Ordering Guide

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: 1FA] 1 FA Locations, Number of users at each; [Item2 : 2FA] 2FA locations, Number of users at each; [Item 3: 3FA] 3 FA Locations, number of users at each; [P4 PIV Number of users total in system]

Item 2: [Number of 1FA Access Control Points] Insert number of readers to enter "***Controlled***" area

Item 3: [Number of 2FA Access Control Points] Insert number of readers to enter "***Limited***" area.

Item 4: [Number of 3FA Access Control Points] Insert number of readers to enter "***Exclusion***" area

Item 5: [Number of readers for moving within Controlled and within Limited Areas Same to Same]

Item 6: [Number of Controllers, if any]

Item 7: [How is PIV Auth Certification validation done during PIV Registration]

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

Draft Documents Continued

After identifying the acceptable authentication factors by access areas for the facility in question, a ordering 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.

SOW/PWS – FAR 8.4 Guidance

Task Orders *exceeding* the micro-purchase (>$3K) threshold, but *less than* the SAT (<$150K):

- Ordering Agency must develop a SOW and evaluation factors
- Provide an RFQ to *at least three* MAS contractors (eBuy RFQ is preferred—Section 803 and 865 compliance). The RFQ must include the SOW, the weighted evaluation factors, and specify the type of order to be awarded, e.g. fixed-price, labor hour, T&M.
- Evaluate all RFQ responses using the criteria provided
- Consider the level of effort, labor category mix and determine that the total price is reasonable and the best overall value
- Minimal documentation
- Issue the order to the MAS contractor, service performed, inspection, acceptance, and payment.

Draft Documents Continued

SOW/PWS – FAR 8.4 Guidance

Task Orders *exceeding* the SAT (>$150K):

- Ordering Agency must develop an RFQ with a SOW and evaluation factors
- Shall post the RFQ on eBuy and provide it to as many schedule contractors as practicable to ensure that at least three reasonable quotes will be received.
- Evaluate all RFQ responses using the criteria provided
- May seek price reductions
- Consider the level of effort, labor category mix and determine that the total price is reasonable and the best overall value
- Minimal documentation
- Issue the order to the MAS contractor, service performed, inspection, acceptance, and payment.

SECURE TECHNOLOGY ALLIANCE

Draft Documents Continued

How do I purchase a PACS Solution using GSA eBuy?

GSA's eBuy - Online Request for Quotation (RFQ) tool 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.

- 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.
  - 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.
- Document the award rationale and issue the task order to the schedule contractor that represents the best overall value to the Government.
- Send out notifications of the award decision through eBuy or via email.
  - 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: https://www.gsaadvantage.gov/advantage/main/ebuy_tutorial.do?

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Funding

Obtain Funding

Key Funding Requirements:

- Procurement
  - Establish Fund Needs (Personl & Time)
  - ICE (i.e., independent cost estimate)
- Implementation
  - Design, planning, installation, pre/post testing
- Sustainment (System)
  - Maintenance through the system lifecycle
  - Periodic System Technical Refresh
  - Continuous (Single/Multi Fiscal Year)

Proposal Evaluation

- Establish Evaluation Timeline
- Determine Team Membership
  - Technical, Cost, Legal Evaluation Teams
  - Award Team
- Utilize Evaluation Criteria
  - Should be written and approved
- Score Proposals
- Build Team Consensus

Contract Award

- Criteria (Award)
  - Best Value
  - Technically Acceptable with Lowest Price (LPTA)
    - Past Performance Tradeoff
    - Full Tradeoff (i.e. LP, TA, Past Performance and Stated Criteria (difficult)
      1. May not be the lowest price
      2. Higher priced proposal with better requirements solution
      3. Service delivery judgment-based on a rational decision
- Award Decision (Final)
  - Teams – Technical and Cost
  - Legal
  - Executive Management
  - Others (?)
- Award Notifications
  - Contacting Officer/Buyer
  - Vendor Debriefs

Upcoming Sessions

Stakeholders	Session 1 10/19/2017	Session 2 11/30/2017	Session 3 1/11/2018	Session 4 2/22/2018	Session 5 3/15/2018	Session 6 4/19/2018
Acquisition	♦		♦	♦		♦
Budget	♦		♦	♦		♦
Customers / Tenants	♦	♦	♦		♦	♦
Engineering	♦				♦	♦
Executive Sponsors	♦	♦	♦	♦	♦	♦
Facility Management	♦	♦	♦		♦	♦
Information Technology	♦		♦		♦	♦
Legal	♦	♦		♦		♦
Personnel	♦		♦		♦	♦
Physical Security	♦	♦	♦	♦	♦	♦
Safety	♦	♦			♦	♦

SECURE TECHNOLOGY ALLIANCE

Resources and Contacts

http://www.securetechalliance.org

Lars Suneborn, CSCIP/G, CSEIP

Director, Training Programs, Secure Technology Alliance

lsuneborn@securetechalliance.org

Kevin Mitchell

Schedule 84 Branch Chief/GSA/FAS

Kevin.mitchell@gsa.gov

Daryl Hendricks

Daryl.Hendricks@gsa.gov

Jason Rosen

Jason.Rosen@uscp.gov

SECURE TECHNOLOGY ALLIANCE