



Highlights & Key Takeaways

April 2014 ICAM Information Sharing Day and Vendor Expo

Through Agency Eyes: ICAM in Action!

Many federal agencies have actively implemented current ICAM requirements and guidance in order to address mission needs, support business requirements, and secure the enterprise. Below, federal agencies share their first hand experience and accounts of ICAM successes.

"A LARGE SECURITY ENABLER FOR OUR AGENCY WAS..."

establishing enterprise software to manage and streamline security identities, compliance, and security events across disparate physical security systems. Our solution checks the validity of the card holder's certificates every 18 hours and restricts physical access through all connected PACS servers if the system discovers revoked or suspended certificates."

- Department of Health and Human Services

"OUR AGENCY FOUND IT IMPORTANT TO..."

make leadership and management feel ownership and accountability for the success of their agency's ICAM program. One way to accomplish this is to tie any outcomes and accomplishments of the ICAM program specifically to the responsible individual's yearly performance plan."

- U.S. Department of Agriculture

"THE BIGGEST KEY TO OUR ICAM SUCCESS WAS..."

developing an adaptable and scalable business case, in collaboration with our stakeholders, to support the need for ICAM projects and funding."

- General Services Administration

"OUR AGENCY'S CURRENT FOCUS IS..."

to implement ICAM on the Secret Fabric through developing and deploying a strong foundation of Public Key Infrastructure and synchronizing with unclassified ICAM efforts."

- Department of Energy

Did you know that ICAM has helped federal agencies:

- ✓ **Reduce** mailing costs by **\$40,000** by using an electronic delivery option for investigation results.
- ✓ **Save** more than **\$48,000** per **100** users annually by implementing digital signatures to convert paper-based approval forms into electronic forms.
- ✓ **Save \$68** per PIV card by synchronizing card expiration with certificate expiration at 3 years.
- ✓ **Decrease** the number of successful intrusions by **46%** by requiring all personnel to log on to unclassified networks with a CAC.

For more information, please contact ICAM@gsa.gov

What's Going On in ICAM for 2014?

Breakout Session 1a: Mobility and ICAM

- Developed a **Mobile Pilot Solution Case Studies document**, which contains solution information and lessons learned from a collection of federal mobile authentication pilots.
- Conducted agency interviews to collect requirements for potential future testing of mobile products and solutions.
- Considering supplemental implementation guidance for PIV-derived credentials following finalization of NIST SP 800-157.

Breakout Session 2a: FCCX Updates

- Accelerates NSTIC and FICAM by allowing agencies to securely interact with a single “broker” to authenticate consumers.
- FCCX pilot design addresses privacy by generating and storing a different anonymous identifier for each web application.
- Agencies realize benefits such as cost reduction associated with credential issuance and management and simplified agreements with credential providers.
- The initial pilot integrators are VA, USDA, NIST, GSA – FCCX is seeking new interested agencies!

Breakout Session 3a: Addressing PACS Integration Challenges

- Released updated PIV in E-PACS guidance, containing detailed technical and security guidance for leveraging PIV and PIV-I authentication mechanisms in a federal agency PACS.
- GSA's Public Building Service (PBS) is working to upgrade PACS for federally-owned buildings.
- During 2013, the Testing Program focused on engineering Physical Access Control Systems (PACS) product testing.
- The Testing Program has approved 30 PACS configurations to meet FICAM Requirements.

Breakout Session 1b: Information Sharing and Federated Access

- Completed the Priority Objective #4 (PO#4) Implementation Plan, which delineates actions on each security domain to facilitate the federal information sharing environment.
- Recent updates to the FICAM Trust Framework Solutions (TFS) Document Suite are intended to provide agencies and Trust Framework Providers (TFPs) with a holistic view of the TFS Program.
- The TFS update introduces the Authority to Offer Services (ATOS), which allows TFP-approved organizations to apply to the TFS Program for approval to offer services directly to U.S. Government.

Breakout Session 2b: Testing Program, Procurement & LACS

- The FICAM Testing Program has been working to enhance the Approved Products List (APL) to address broader usability and security requirements.
- The program is working to engineer Logical Access Control Systems (LACS) product testing and is leveraging findings from interviews conducted across the Federal Government to make improvements.
- Agencies should refer to the latest version of the APL on idmanagement.gov for procurement of both PACS and LACS.

Breakout Session 3b: Impacts of NIST Standards and Specifications

- NIST recently released drafts of SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials and NIST IR 7981 Mobile, PIV, and Authentication.
- NIST has drafted SP 800-166, addressing testing requirements for Derived PIV Credentials, and is working on an accompanying test tool and updates to SP 800-79 to address accreditation for Derived PIV Credential Issuers.
- Draft updates to NIST SP 800-73-4 focus on new optional PIV card features (e.g., iris biometric, biometric on-card comparison).

Access April 2014 ICAM Information Sharing Day Event Materials at:
www.idmanagement.gov/