

Interagency Advisory Board

Meeting Agenda, May 27, 2010

1. **Opening Remarks**
2. **PIV-I Status** (*Judy Spencer, GSA*)
3. **PIV Test Requirements** (*Dave Temoshok, GSA*)
4. **ICAM Progress at USDA** (*Owen Unangst, USDA*)
5. **PIV-I Discussion Panel** (*Jim Hatcher, Mike Mestrovich, Chris Loudon, Rebecca Nielson*)
6. **FIWG Status Update** (*Corinne Irwin, NASA*)
7. **LAWG Status Update** (*Bill Erwin, GSA*)
8. **Closing Remarks**



Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

Modernizing Logical Access

ICAM-SC Logical Access Working Group (LAWG)

Bill Erwin, GSA
Allison Scogin, DoD

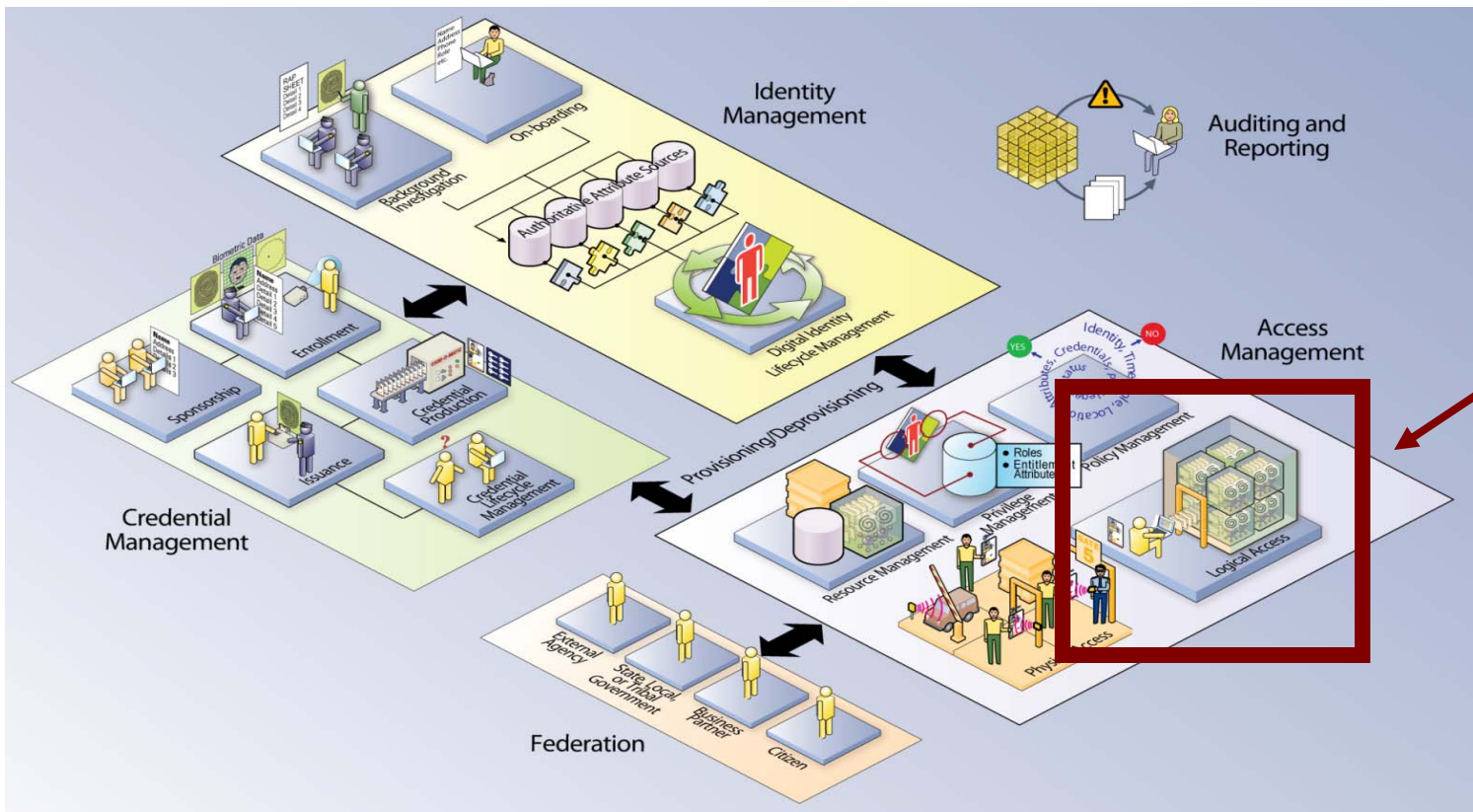
Interagency Advisory Board
May 27, 2010



Identity, Credential, and Access Management

Logical Access Working Group (LAWG) Scope

The Logical Access Working Group (LAWG) consists of representatives from 21 Federal agencies working collaboratively to develop guidance and best practices to assist all agencies in the implementation of logical access to federal systems and networks using the client certificates on the Personal Identity Verification (PIV) card.



**LAWG
Scope**



Benefits of PIV-Enabled Logical Access

- Increased security
 - Two-factor authentication
 - High assurance (level 4)
- Ease of use
 - No complex passwords to remember
- Increased efficiency
- Reduction of total costs
- Compliance with federal rules relevant to ICAM



Identity, Credential, and Access Management

LAWG Goals

Short Term Goals	Long Term Goals
<ul style="list-style-type: none">➤ Establish a platform for knowledge sharing and distribute existing guidance (lessons learned) ➤ Assist smaller agencies with best practices	<ul style="list-style-type: none">➤ Develop logical access implementation guidance as supplement to the FICAM Roadmap ➤ PIV-enable government-wide applications<ul style="list-style-type: none">▪ Employee Express, eTravel, TSP ➤ Standardize the technical implementation approach



Tentative Areas of Guidance





- Planning, Pilot, and Implementation
- Establishing a common infrastructure around PIV card for logical access control
 - Chain-of-trust through path validation
 - Client cert verification (e.g., revocation checking)
- PIV-enablement of:
 - Network (Operating System) Login
 - Remote Access
 - Intra-agency Web applications
 - Inter-agency Web applications (e.g., Employee Express)
- Performance/Failover considerations
- Procurement best practices





Identity, Credential, and Access Management

Progress To Date

Task	Complete
Revised implementation guidance outline to incorporate feedback from the LAWG and the FICAM Roadmap Development Team	
Assisted agencies knowledge sharing, vendor reach back and Increased membership by 15%	
Assisted agencies with getting ready for FISMA reporting (CyberScope) using PIV card access	
Developed a delivery schedule for the next version of the implementation guidance document	
Revise implementation guidance document to address comments from the LAWG & FICAM Roadmap Development Team	In Progress



Challenges

- Varied and changing technology landscape in agency network and web applications
- Effective contingency plans for card replacement preventing agencies from adopting mandatory PIV usage policy

Lessons Learned

- Increased awareness and willingness towards PIV enablement among agencies
- Take a phased approach. The entire infrastructure does not need to be PIV-enabled to start using PIV access



Recent Discussion Topics on the LAWG

- SHA 256
- Emphasis on PIV enabling Federal Applications
- Updating AD information for User connecting via VPN
- PIV on LINUX/Mac Workstations
- Transition towards ICAM and workflow based products

Next Steps

- Continue to refine LACS implementation guidance
- Continue to assist agencies with LACS implementation
- Set up a meeting to discuss SHA-256 with a NIST representative
- Continue to foster discussions, collaborations, and document sharing within the LAWG



Contact Information

Bill Erwin, GSA

ICAMO Program Manager

bill.erwin@gsa.gov

202-501-0758

Allison Scogin, DoD

DoD PKI PMO, Public Key Enablement Team

allison.scogin@disa.mil

703-882-1635