

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

Federation Interoperability Working Group (FIWG)

May 2010



Agenda

- What is the FIWG?
- Federal Identity Profile
- BAE
 - Federal agreements
 - Encryption/signing certs
- EGCA
- Physical Access
- Challenges



ICAM Mission

- Fostering effective **government-wide** identity and access management
- Enabling **trust** in online transactions through **common** identity and access management **policies and approaches**
- **Aligning federal agencies** around common identity and access management practices
- **Reducing the identity and access management burden** for individual agencies by fostering common interoperable approaches
- **Ensuring alignment** across all identity and access management activities that cross individual agency boundaries
- Collaborating with **external identity management** activities through **inter-federation** to enhance interoperability

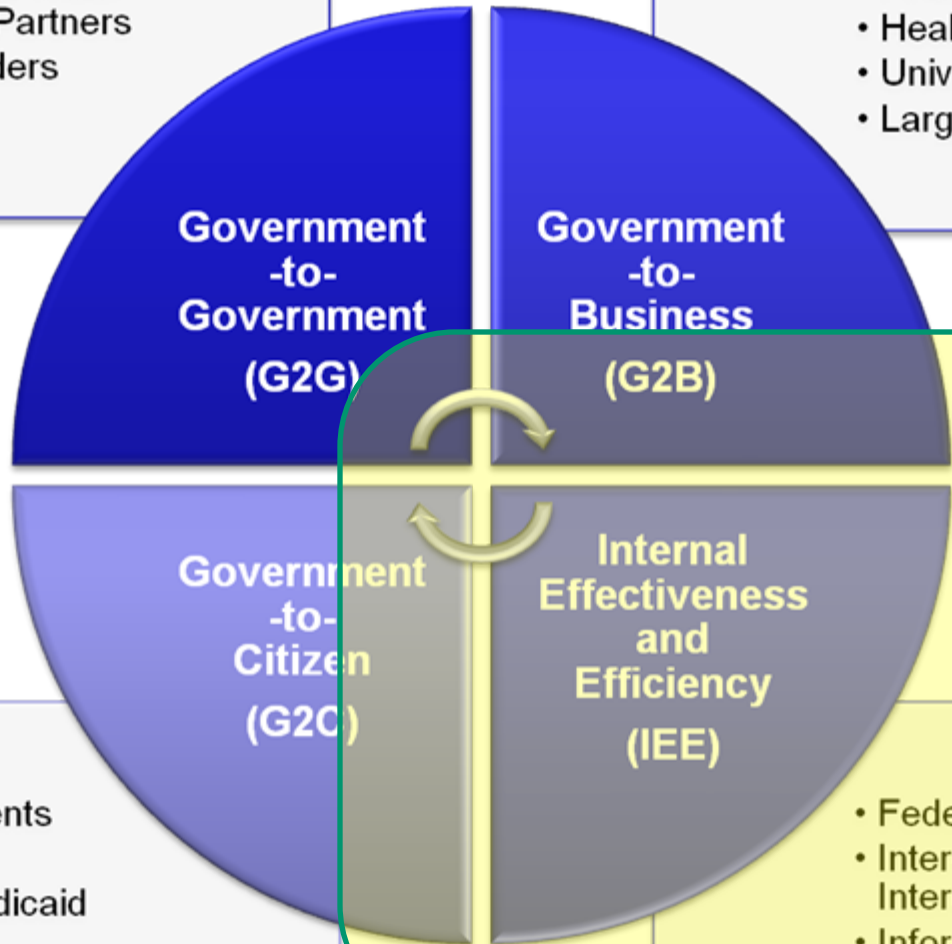


Identity, Credential, and Access Management

Applicability

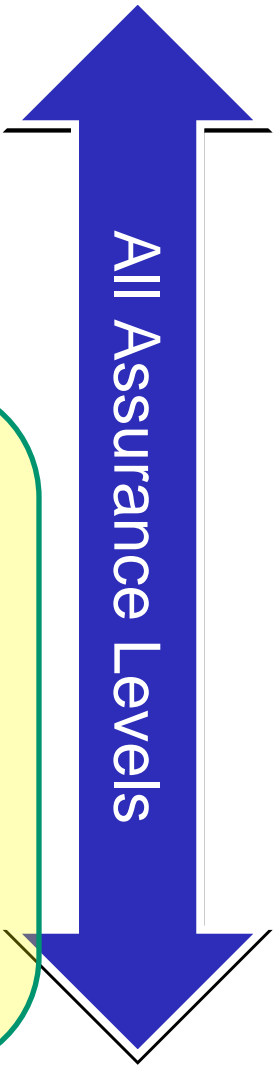
- State, Local, & Tribal Government Partners
- First Responders

- Financial Institutions
- Healthcare Providers
- University Partners
- Large Integrators



- Grant Recipients
- Taxpayers
- Medicare/Medicaid Beneficiaries

- Federal Agencies
- Inter-agency Interoperability
- Information Sharing





FIWG Purpose

- Promote federation pilots
 - Intra-Federal
 - External parties
 - Levels of Assurance 2 – 4
- Identify roadblocks to federation
- Address roadblocks



Roadblocks Identified

- Identifiers/Linkage
- PIV Enablement
- Trusted Certificate Authorities
- Federation Agreements



Identifiers/Linkage

- How do you uniquely identify federated users?
- How do you link identity data you have with your federated partner?
- Partnered with HR LOB to define:
 - Common identity profile for use in Fed-to-Fed space
 - Identifier(s) that can be relied upon to uniquely identify a person
 - Identifier(s) that can be used to link existing identities in two systems to enable PIV and SAML authentication



PIV Enablement

- Two basic methods
- Registration
 - User is invited to remotely present PIV card
 - Linkage is made between Identity/account and PIV card
- Backend Attribute Exchange
 - Federation partners exchange data to enable linkage
 - For existing applications that already exchange identity information, adding key PIV attributes to the existing exchange is simple to implement



PIV Enablement and SAML/Single Sign-on

- Is it acceptable to use a SAML assertion of PIV authentication?
 - Yes, depending on your risk assessment
- OASIS standard developed for asserting PIV
- SAML assertions still must be signed and encrypted
 - See Trusted Certificate Authorities



Trusted Certificate Authorities

- Need a Trust Anchor, similar to FBCA, to allow for SAML exchanges
 - Signed, encrypted assertions for BAE and authentication exchange
- eGov Certificate Authority (eGCA) can meet this need
 - Re-vamping eGov eAuth documents to allow issuance of eGCA certs for BAE and federated authentication
 - Federal Agencies will be able to self-certify to receive certs
 - Other partners will certify through the Trust Provider Framework



Federation Agreements

- Developing a standard federation agreement that can be used multi-laterally
 - Owner of the agreement establishes the parameters for federation
 - Other parties sign on
- In general, the use of bi-lateral agreements should be avoided
 - Difficult to maintain agreement standards
 - Doesn't support attribute aggregation



Attribute Aggregation

- Collect multiple attributes from different sources in order to make authorization decisions
- Example:
 - NASA asserts that I am a NASA employee
 - DHS asserts that I am authorized to access a disaster site
 - Anne Arundel County asserts that I am a certified Emergency Medical Technician
 - Bank of America asserts that I am the owner of the smartcard credential they issued
- Goal is to collect attributes from the authoritative source
 - The certifier/issuer is the authoritative source



Identity, Credential, and Access Management

Presenter

Corinne Irwin

Project Executive, Authentication & Authorization

National Aeronautics and Space Administration (NASA)

Corinne.S.Irwin@nasa.gov

202-358-0653