Interagency Advisory Board

Meeting Agenda, April 1, 2010

1. **Opening Remarks** *(Tim Baldridge, NASA)*
2. **SCA/IAB Joint Events Rationale***(Randy Vanderhoof, SCA)*
3. **ICAM Roadmap: Requirements & Status** *(Judy Spencer, GSA)*
4. **The Growing Use of SAFE-BioPharma Digital Identities** *(Mollie Shields-Uehling)*
5. **National Strategy for Secure Online Transactions** *(Tom Lockwood, DHS)*
6. **The Impact of PIV and PIV-I on Microsoft Products***(John Biccum)*
7. **Panel Discussion: The Impact & Importance of PIV-I** *(Led by Bob Gilson, DMDC)*
8. **Closing Remarks** *(Tim Baldridge, NASA)*

IAB
April 1, 2010

Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

in and with

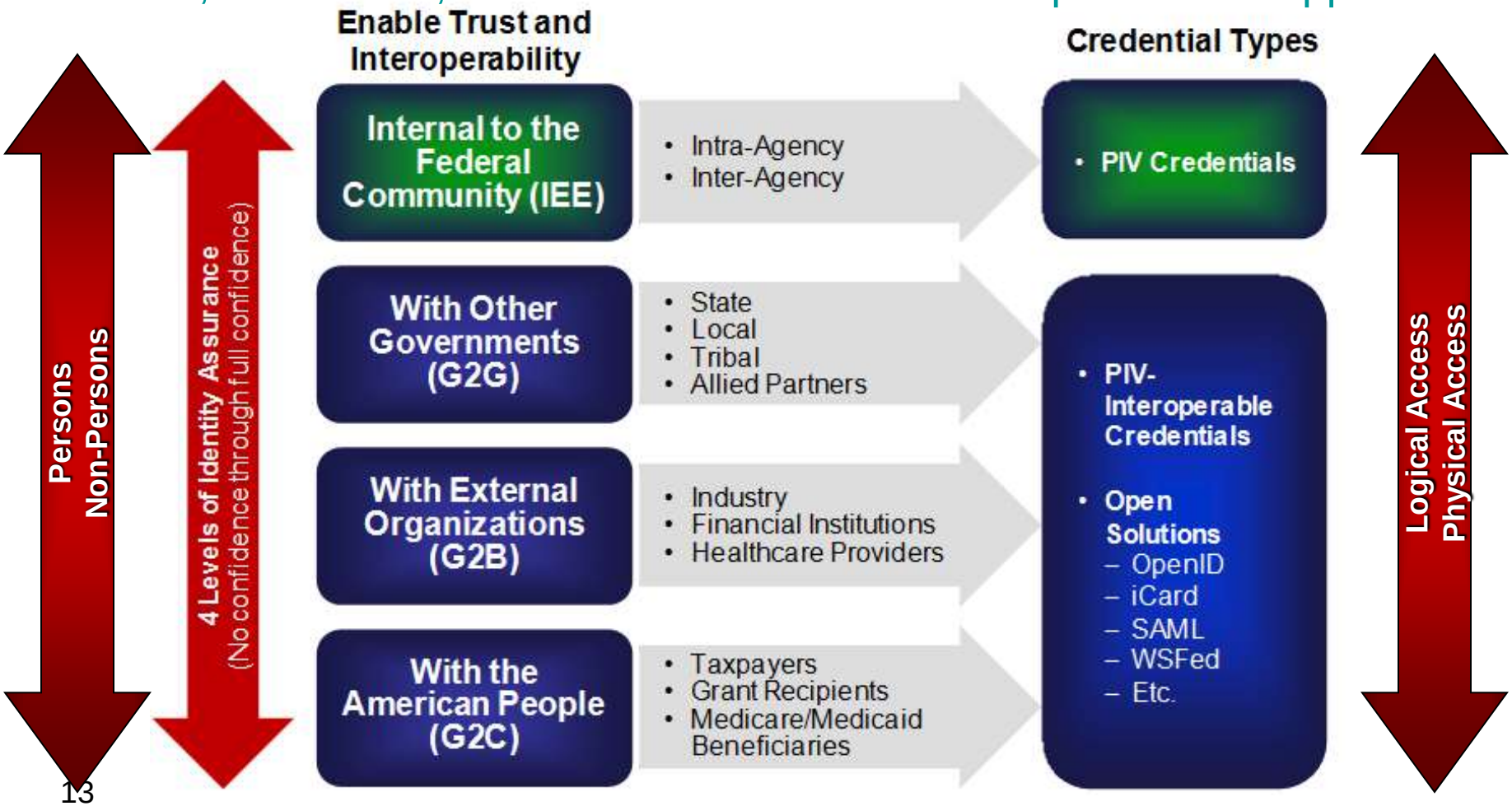
The Federal Government

Paul D. Grant
Special Assistant,
Federated Identity Management and External Partnering
Office of the CIO
DoD
Paul.Grant@OSD.Mil

Co-Chair, ICAM Subcommittee

http://www.IdManagement.Gov

ICAM Scope: ICAM represents the intersection of digital identities, credentials, and access control in one comprehensive approach

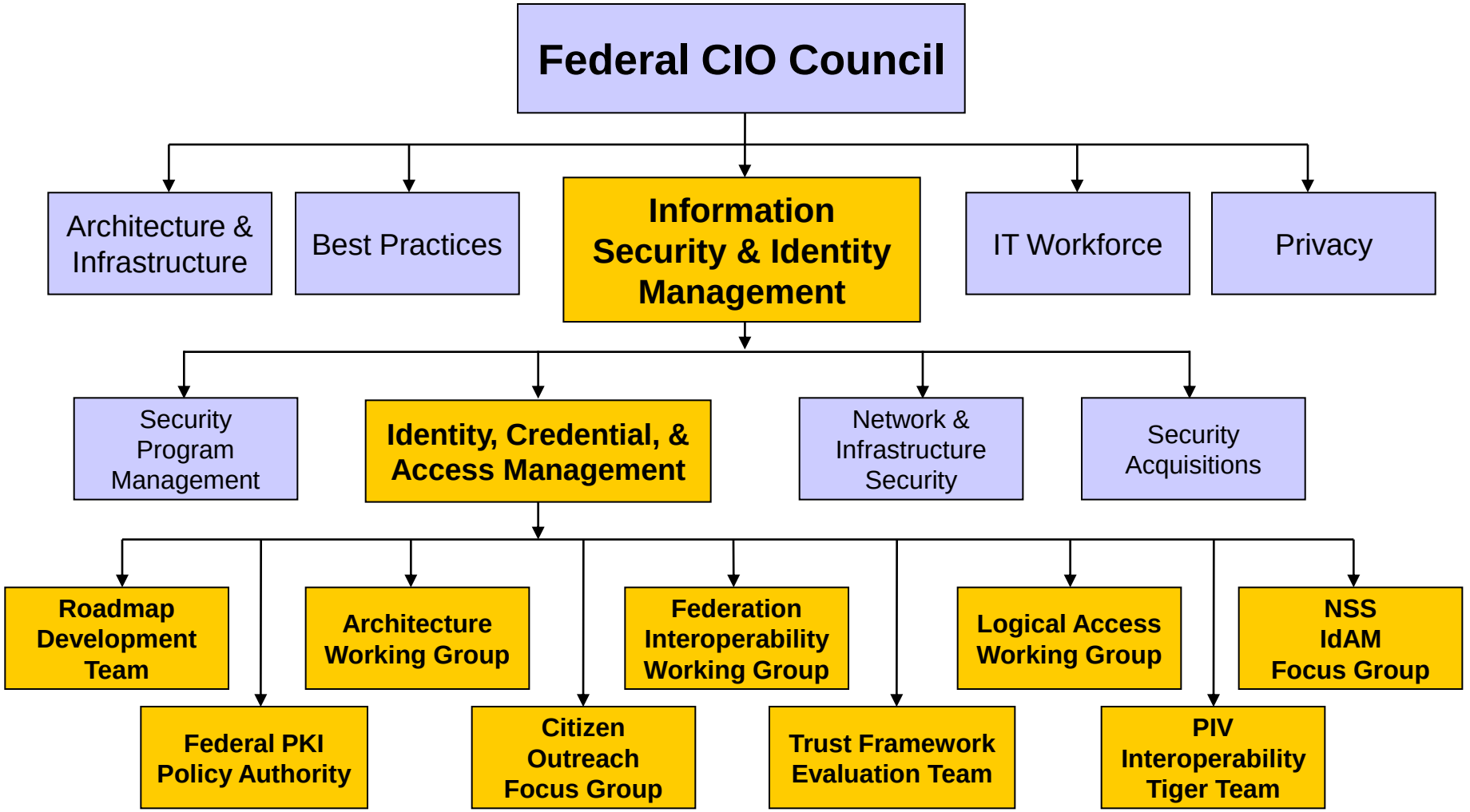


ICAM Drivers

- Increasing Cybersecurity threats
  - There is no National, International, Industry “standard” approach to individual identity on the network. (*CyberSecurity Policy Review*)
  - Security weaknesses found across agencies included the areas of user identification and authentication, encryption of sensitive data, logging and auditing, and physical access (*GAO-09-701T*)
- Need for improved physical security
- Lag in providing government services electronically
- Vulnerability of Personally Identifiable Information (PII)
- Lack of interoperability
  - “The ICAM segment architecture will serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions.” (President’s FY2010 Budget)
- High costs for duplicative processes and data management

14

Committee Structure



ICAM Alliances: Interagency Security Committee, IC IdAM, NASCIO, & More

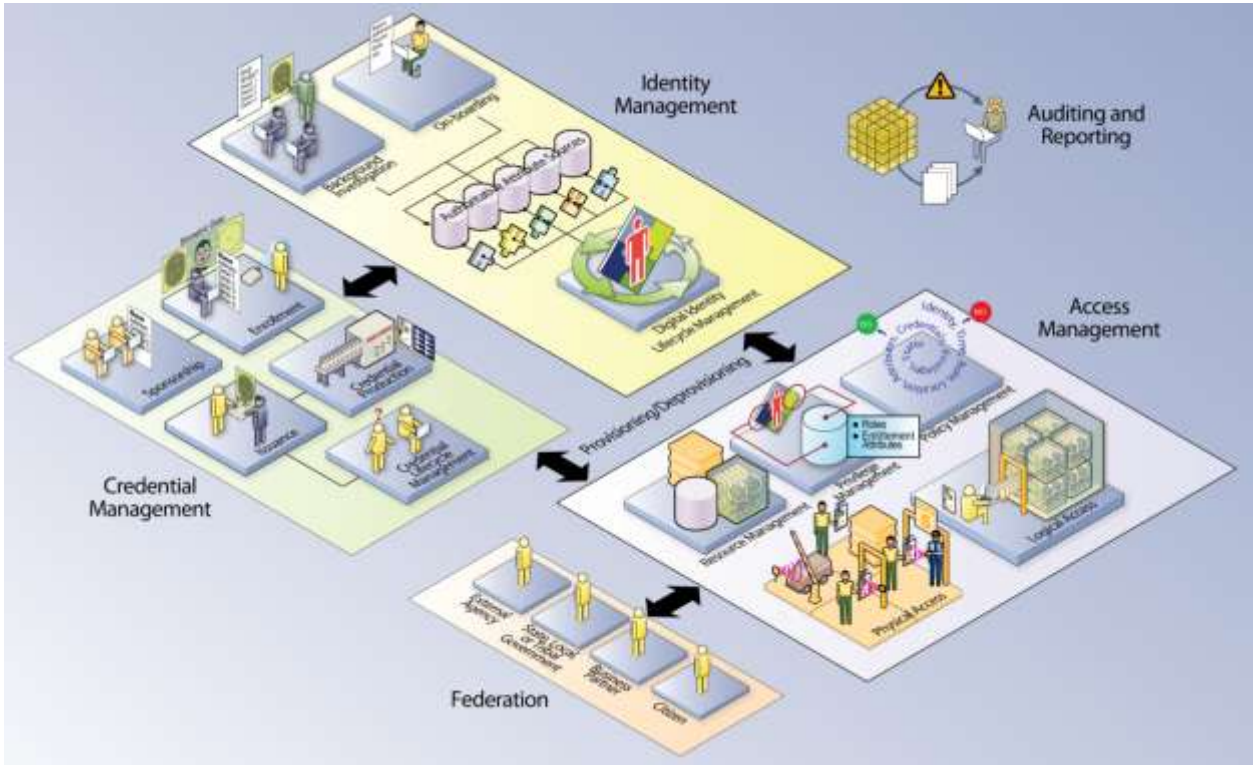
Identity Assurance Levels (IAL)

M-04-04:E-Authentication Guidance for Federal Agencies

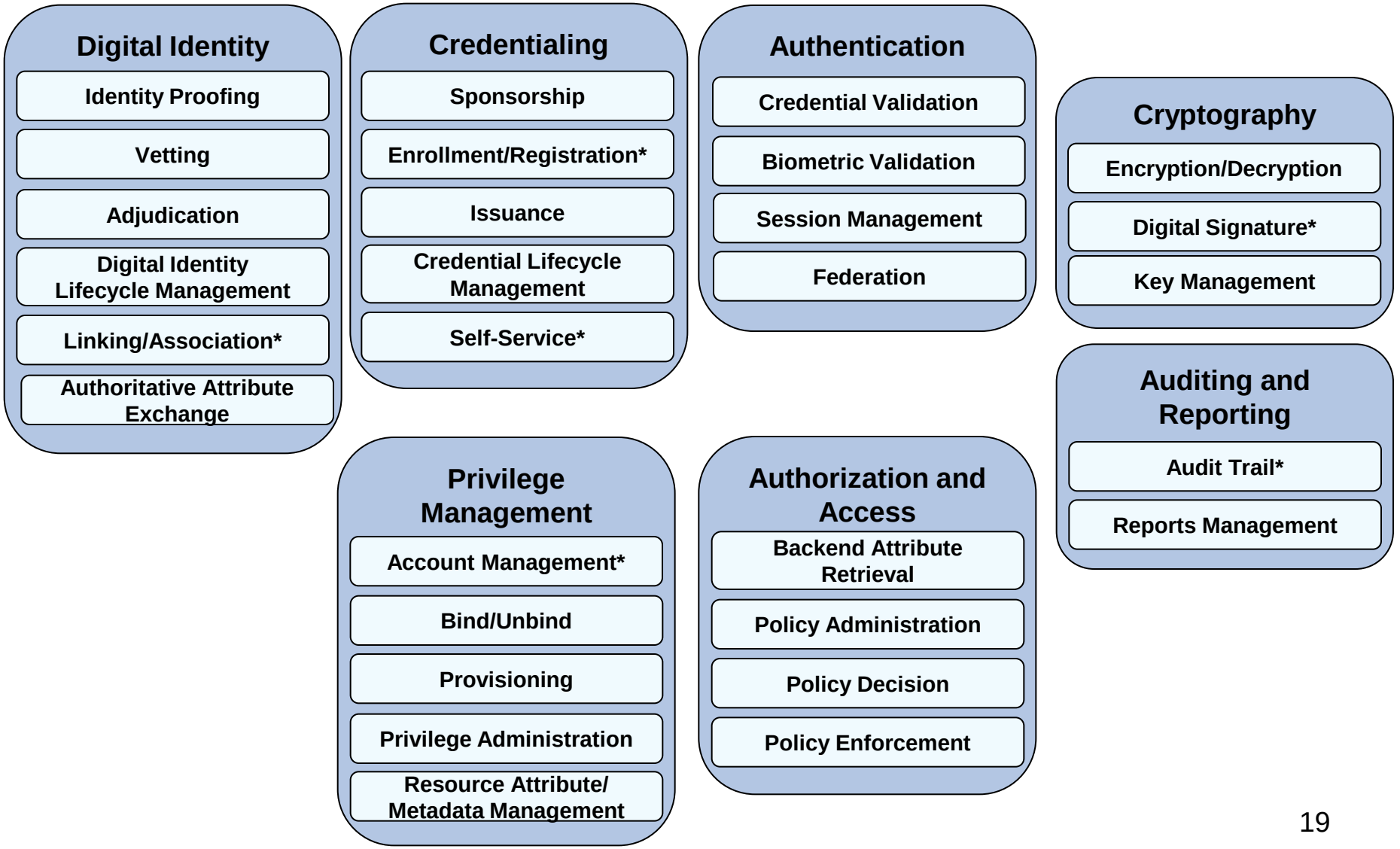
OMB Guidance establishes 4 authentication assurance levels

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	**Some confidence in asserted identity**	**High confidence in asserted identity**	**Very high confidence in asserted identity**
Self-assertion minimum standards	On-line instant qualification, out-of-band follow-up	On-line out-of-band verification for qualification Cryptographic Solution	In person proofing Record a biometric Cryptographic solution Hardware Token

- **Key ICAM Service Areas Include:**
  - **Digital Identity**
  - **Credentialing**
  - **Authentication**
  - **Authorization & Access**
    - **Privilege Management**
    - **Cryptography**
    - **Digital Signature**
    - **Auditing and Reporting**



Services Framework



Personal Identity Verification - Interoperable (PIV-I) Cards for Non-Federal Issuers

Basis for PIV Card Trust

- Well-defined standards
- A compliance regimen that ensures parties adhere to the well-defined standards
- Relying Party verification that allows relying parties to verify compliance when trusting and
- Secure components inherent to the PIV Card

Situation

- PIV Cards, by definition, are issued only to/by the Federal Government
- Organizations external to the U.S. Federal government have expressed a desire to establish identity credentials that are interoperable with the Federal PIV card.
- They want a card that is:
  - Technically compatible / interoperable with the PIV system
  - Capable of Trust in the Federal environment

Top 5 for ICAMSC for 2010

(as of 22 January)

1. PIV-I "Certification"	**-Publishing PIV-I FAQ** **-Making changes to the FBCA policy to accommodate PIV-I** **-Validation of Non-Federal Issuers of PIV-I cards**
2. Publish Roadmap and Implementation Guidance (Part B)	**-Developing Implementation Guidance to assist agencies with transition activities** **-Publishing the guidance as Part B of the Roadmap**
3. Trust Frameworks	**-Establish process for Evaluation of TFP (at Assurance Levels 1&2)** **-Expand Number and Variety of TFP and NFI**
4. PACS Modernization	**-Work with ISC on Physical Access Requirements** **-Enable PACS for all access controlled Federal buildings** **-All PACS standardized to accept PIV/PIV-I cards** **-Develop common visitor access management processes** **-Establish rules for Attribute exchange (inter-organizational)**
5. LACS Modernization	**-Implement smart card/PKI-based access control for all network logon** **-Enable all applications that serve the Federal community to accept PIV-based access credentials.** **-Establish Inter-Enterprise Peer Services (e.g. attribute exchange)**

Summary & Conclusions

- **Strong Identity and Access Management Are Foundational to Secure Information Sharing, Collaboration and Cybersecurity**

- **Shared Guidance is Improving: Much Room for More Improvement**
  - **Clear, Concise, Consistent, Credible**
  - **For Ourselves and Our Mission Partners**

- **Federal Identity, Credential, and Access Management (ICAM) is providing this consistent approach (with your help)**

- **Mission Partners are Fielding Strong Identity Credentials as well as Creating Federations for Sharing & Collaboration**

- **Progress Depends on Public-Private Partnering**
  - **Domestically and**
  - **Internationally**