CIO COUNCIL

ICAM
Identity, Credential,
& Access Management

Federal CIO Council
Information Security and Identity Management Committee

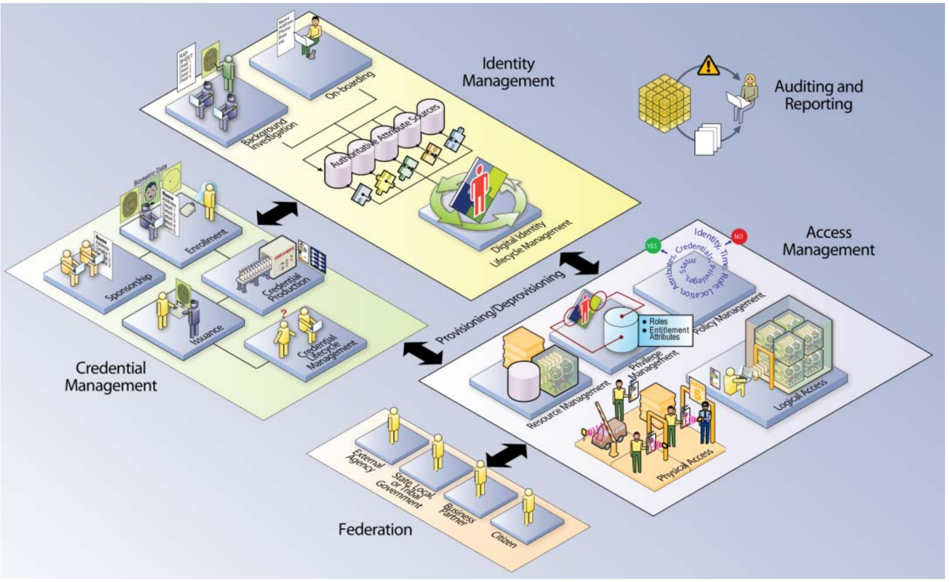
Identity, Credential, and Access Management

An information exchange For Information Security and Privacy Advisory Board

Deb Gallagher
General Services Administration
Office of Governmentwide Policy
Deborah.Gallagher@gsa.gov

ICAM

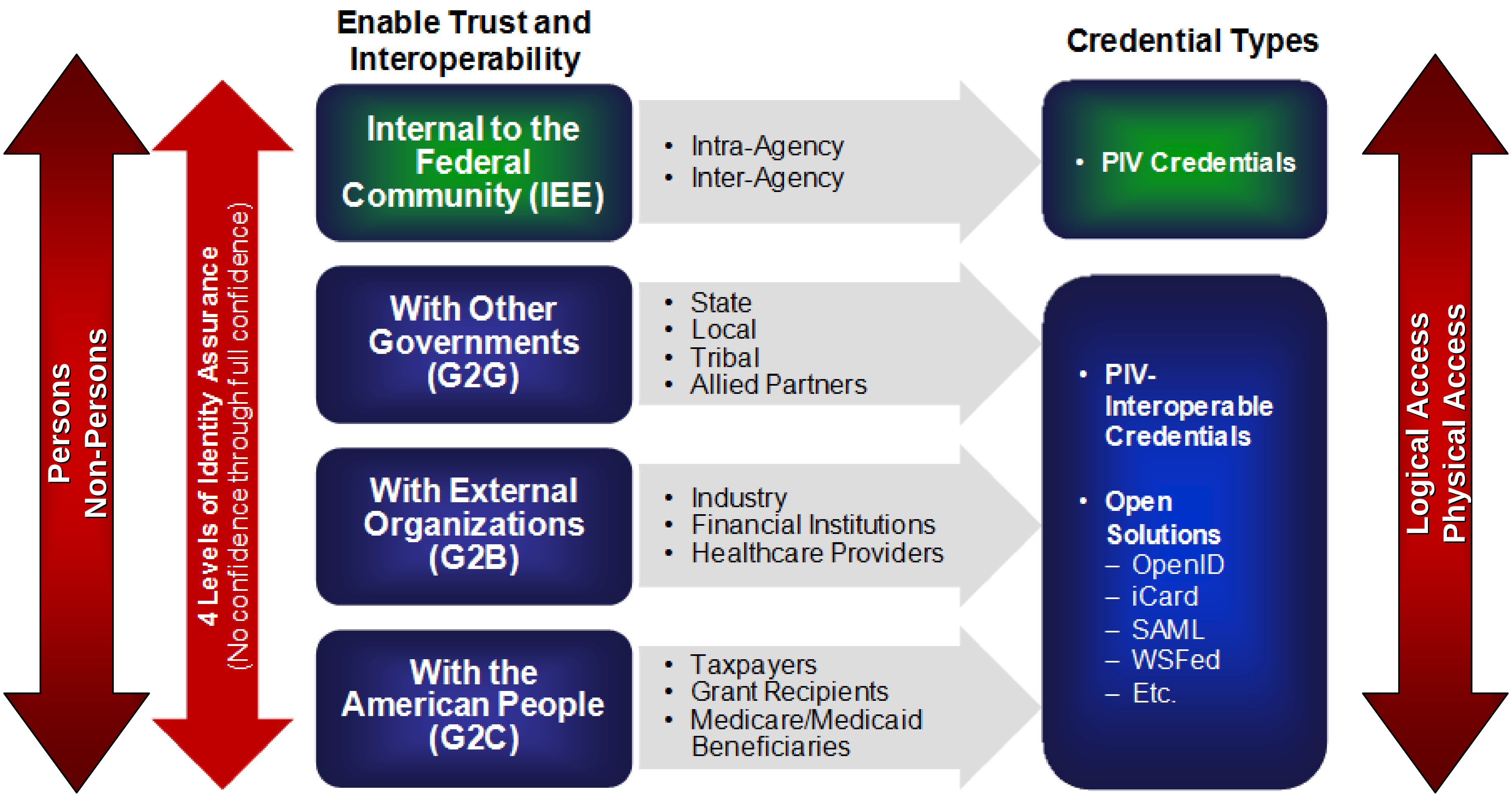
- ICAM represents the intersection of digital identities, credentials, and access control into one comprehensive approach.
- Consolidates 3 Programs:
  - Federal PKI
  - E-Authentication
  - HSPD-12
- Streamlines government-wide activities
- Minimizes duplication of effort
- Breaks down stovepipes
- Key enabler for National Strategy for Trusted Identities in Cyberspace



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

ICAM Scope



Persons

Non-Persons

4 Levels of Identity Assurance

(No confidence through full confidence)

Enable Trust and Interoperability

Internal to the Federal Community (IEE)

- Intra-Agency
- Inter-Agency

With Other Governments (G2G)

- State
- Local
- Tribal
- Allied Partners

With External Organizations (G2B)

- Industry
- Financial Institutions
- Healthcare Providers

With the American People (G2C)

- Taxpayers
- Grant Recipients
- Medicare/Medicaid Beneficiaries

Credential Types

- **PIV Credentials**

- **PIV-Interoperable Credentials**
- **Open Solutions**
  - OpenID
  - iCard
  - SAML
  - WSFed
  - Etc.

Logical Access

Physical Access

Federal ICAM Goals

- 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

The Federal ICAM Initiative provides cohesive governance for several programs that were previously governed and managed separately.

FICAM Roadmap Document v1.0

Chapter 1: Introduction. Provides background information on the ICAM Initiative and an overview of the purpose, scope, and structure of the document.

Chapter 2: Overview of Identity, Credential, and Access Management. Provides an overview of ICAM that includes a discussion of the business and regulatory reasons for agencies to implement ICAM initiatives within their organization.

PART A: ICAM Segment Architecture

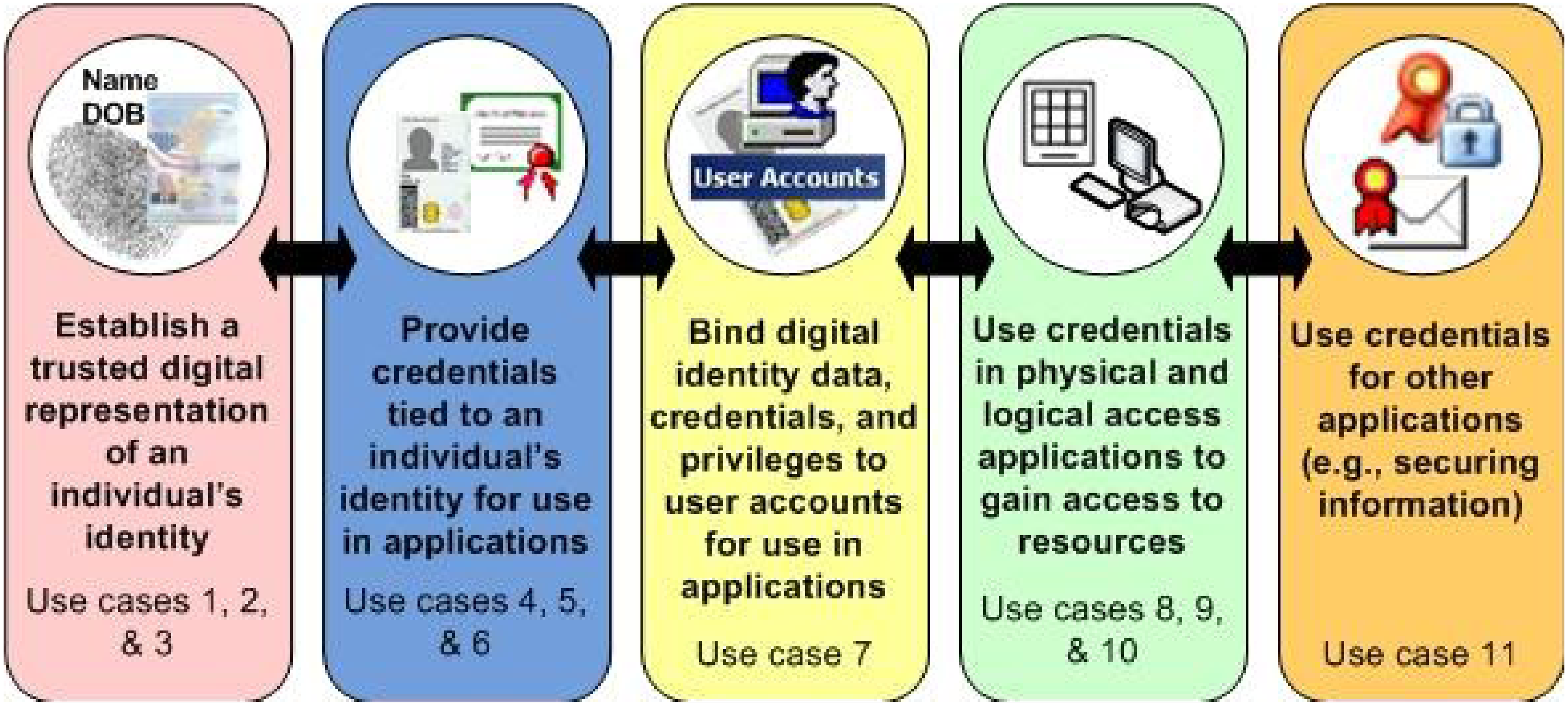
Chapter 3: ICAM Segment Architecture. Standards-based architecture that outlines a cohesive target state to ensure alignment, clarity, and interoperability across agencies.

Chapter 4: ICAM Use Cases. Illustrate the as-is and target states of high level ICAM functions and frame a gap analysis between the as-is and target states.

Chapter 5: Transition Roadmap and Milestones. Defines a series of logical steps or phases that enable the implementation of the target architecture.

The purpose of the Federal ICAM segment architecture is to provide federal agencies with a standards-based approach for implementing government-wide ICAM initiatives. The use of enterprise architecture techniques will help ensure alignment, clarity, and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the Federal Government.

Eleven Use Cases Covering:



Establish a trusted digital representation of an individual's identity

Use cases 1, 2, & 3

Provide credentials tied to an individual's identity for use in applications

Use cases 4, 5, & 6

Bind digital identity data, credentials, and privileges to user accounts for use in applications

Use case 7

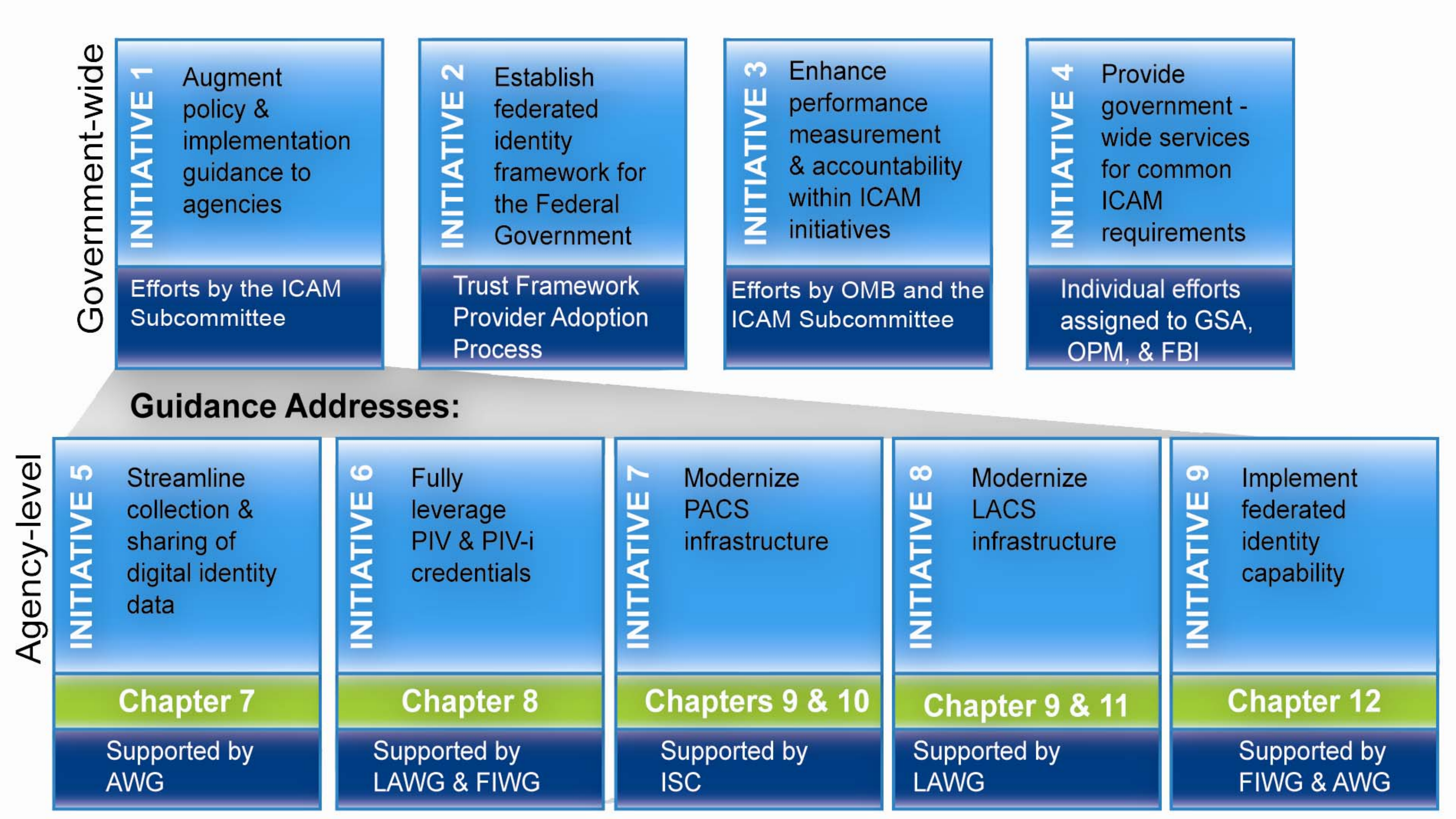
Use credentials in physical and logical access applications to gain access to resources

Use cases 8, 9, & 10

Use credentials for other applications (e.g., securing information)

Use case 11

Transition Roadmap Initiatives



Government-wide

INITIATIVE 1
Augment policy & implementation guidance to agencies
Efforts by the ICAM Subcommittee

INITIATIVE 2
Establish federated identity framework for the Federal Government
Trust Framework Provider Adoption Process

INITIATIVE 3
Enhance performance measurement & accountability within ICAM initiatives
Efforts by OMB and the ICAM Subcommittee

INITIATIVE 4
Provide government - wide services for common ICAM requirements
Individual efforts assigned to GSA, OPM, & FBI

Guidance Addresses:

Agency-level

INITIATIVE 5
Streamline collection & sharing of digital identity data
Chapter 7
Supported by AWG

INITIATIVE 6
Fully leverage PIV & PIV-i credentials
Chapter 8
Supported by LAWG & FIWG

INITIATIVE 7
Modernize PACS infrastructure
Chapters 9 & 10
Supported by ISC

INITIATIVE 8
Modernize LACS infrastructure
Chapter 9 & 11
Supported by LAWG

INITIATIVE 9
Implement federated identity capability
Chapter 12
Supported by FIWG & AWG

Part B Chapter Summary

PART B: Implementation Guidance

Chapter 6. ICAM Implementation Planning. Augments standard life cycle methodologies as they relate to specific planning considerations common across ICAM programs.

Chapter 7. Initiative 5: Streamline Collection and Sharing of Digital Identity Data. Provides guidance for agency activities required to eliminate redundancies in the collection and maintenance of identity data and mitigate the inefficiencies and security and privacy risks associated with current identity data management processes

Chapter 8. Initiative 6: Fully Leverage PIV and PIV-interoperable Credentials. Provides guidance for activities required to meet the intent of HSPD-12 for the usage of PIV credentials, make better use of cryptographic capabilities, and use of externally-issued PIV-interoperable credentials

Chapter 9. Access Control Convergence. Includes guidance topics that are applicable to both physical and logical access and will tie into PACS and LACS implementation chapters.

Chapter 10. Initiative 7: Modernize PACS Infrastructure. Provides guidance for agency activities required to update physical security processes and systems for routine access for PIV cardholders and visitor access for individuals with other acceptable credentials.

Chapter 11. Initiative 8: Modernize LACS Infrastructure. Provides guidance for upgrading logical access control systems to enable the PIV card and automate and streamline capabilities to increase efficiency and improve security.

Chapter 12. Initiative 9: Implement Federated Identity Capability. Provides guidance for agency activities to support streamlined service delivery to external consumers and reduce redundancy in ICAM programs by leveraging a government-wide federated identity framework

Phase 2 Workplan Progress

	Chapter 7 – Initiative 5: Streamline Collection and Sharing of Digital Identity Data	Chapter 8 – Initiative 6: Fully Leverage PIV and PIV-I Credentials	Chapter 12 – Initiative 9: Implement Federated Identity Capability	Appendix B – Glossary
Key Topics	• Enterprise digital identity • Identity life cycle process improvement • Reciprocity of background Investigations • Digital identity attribute exchange approaches	• PIV and PIV-I overview • Credential authentication • Lost/forgotten cards • Alternate biometrics • Encryption and digital signature • Key history management	• Federal trust frameworks • Scheme adoption certification process • Provisioning external users • Federated access using third party credentials	• Key ICAM terminology • Use case actor definitions • Service component definitions
Development Activities	✓ Request agency information on digital identity data management ✓ Collaborate with AWG and FIWG on content development ✓ Develop draft narrative ⌛ Conduct reviews and finalize draft	✓ Request Agency information on usage of PIV and PIV-I credentials ✓ Collaborate with RDT on content development ✓ Incorporate guidance from the CPWG ✓ Develop draft narrative ✓ Conduct reviews and finalize draft	✓ Request Agency information on implementation of federated identity capabilities ⌛ Collaborate with FIWG, COFG, and AWG on content development ⌛ Develop draft narrative • Conduct reviews and finalize draft	✓ Review existing glossaries and lexicons with terminology related to ICAM ✓ Collaborate with RDT Glossary Tiger Team on recommended definitions • Review and gain consensus on Glossary draft

● Not Started ⌛In Progress ✓Completed

Document Review Milestones

Date	Event
Friday, February 25, 2011*	Public Draft of Phase 1 chapters released
Friday, March 25, 2011	Initial Phase 2 Draft provided to RDT for two-week review period
Friday, April 8, 2011	RDT comments due on Initial Draft
Friday, April 22, 2011*	Complete ICAM Release Draft (incorporating RDT comments) provided to ICAM Community for 30-day review period
Friday, May 20, 2011	ICAM Community comments due on Release Draft
Friday, June 24, 2011*	Public Draft of Phase 2 chapters released

*Release dates subject to change based upon the volume and complexity of comments received during the comment periods.

ICAM Key Activities

- Federal PKI Activities
- PIV Interoperability: Defining the parameters for an “other government or industry smart card that emulates the PIV credential
  - FIPS 201 is limited to the Federal community
  - External interoperability/trust is achievable
- Trust Framework Providers and Scheme Adoption
  - Non-cryptographic solutions at lower levels of assurance
  - Industry self-regulation with government recognition
  - Working with Open Solutions to enable open government
- Backend Attribute Exchange

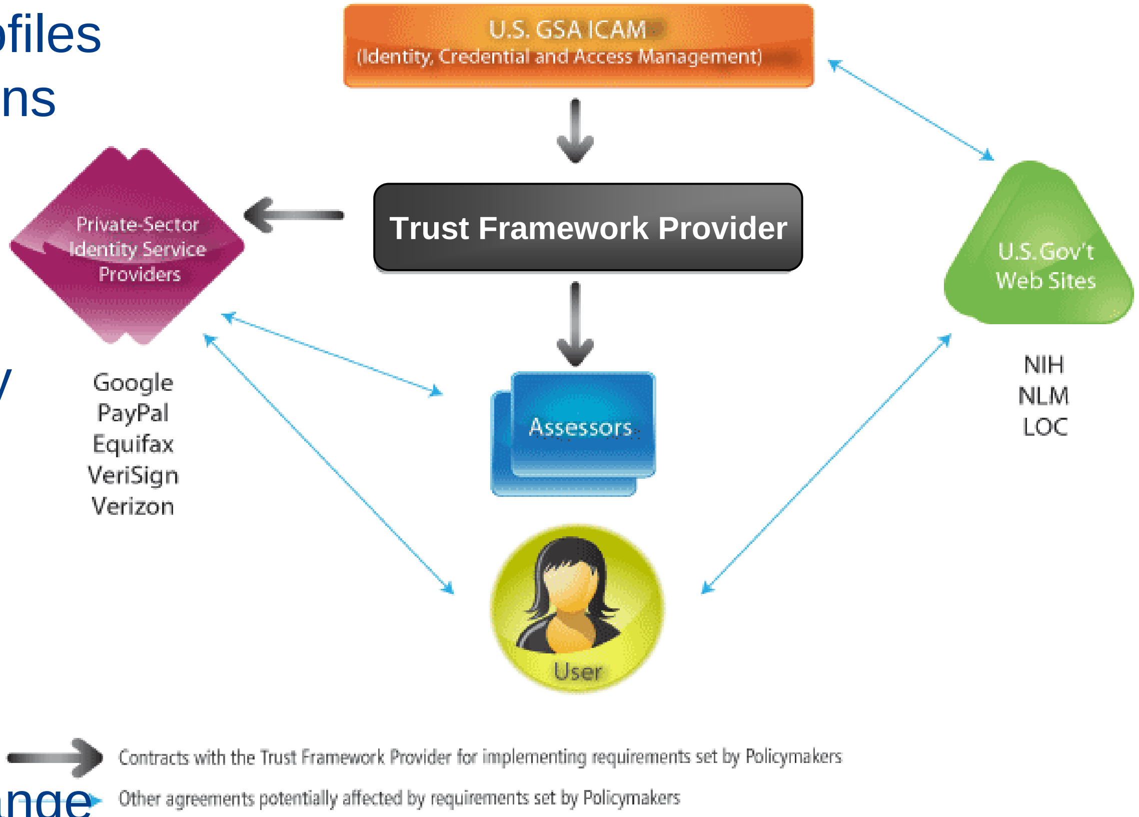
Current Status

- PIV-I requirements are now published in the Federal Bridge Certificate Policy
  - PIV-I Hardware and PIV-I Content Signing fall under the Medium Assurance level
  - PIV-I Card Authentication is a unique certificate policy within the FBCA CP
  - Find the revised FBCA policy at: http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf
- A set of mapping matrices are available for Entities with a *direct* cross certificate relationship with the FBCA at Medium Hardware.
- A set of PIV-I FAQs has been published to idmanagement.gov
- Federal PKI has collaborated to develop a test plan for PIV-I.
- Approved Certipath, Verisign and Verizon

Trust Frameworks: Open Solutions for Open Government

The ICAMSC:

- Establishes Federal Profiles for Open identity solutions
- Established Trust Framework Provider Requirements
- Worked the CIO Privacy Committee to establish Privacy Principles
- Reviews and Approves Trust Frameworks:
  - Kantara
  - Open Identity Exchange
  - InCommon (in progress)


U.S. GSA ICAM
(Identity, Credential and Access Management)
Trust Framework Provider
Private-Sector Identity Service Providers
Google
PayPal
Equifax
VeriSign
Verizon
U.S.Gov't Web Sites
NIH
NLM
LOC
Assessors
User
Contracts with the Trust Framework Provider for implementing requirements set by Policymakers
Other agreements potentially affected by requirements set by Policymakers

Graphic Courtesy of Open Identity Exchange

M-11-11

- *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*
- Each agency is to develop and issue an implementation policy, by March 31, 2011
  - The agency will require the use of the PIV credentials as the common means of authentication for access to:
    - Facilities
    - networks, and
    - information systems.

M-11-11

- Designate an agency lead official for ensuring the issuance of the agency's HSPD-12 implementation policy (Feb. 25)
- Develop and issue an implementation policy, by March 31
- Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.
- Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.

M-11-11

- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "*Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.*

- Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.5

- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov).

Questions
?