ICAM
Identity, Credential, & Access Management

Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

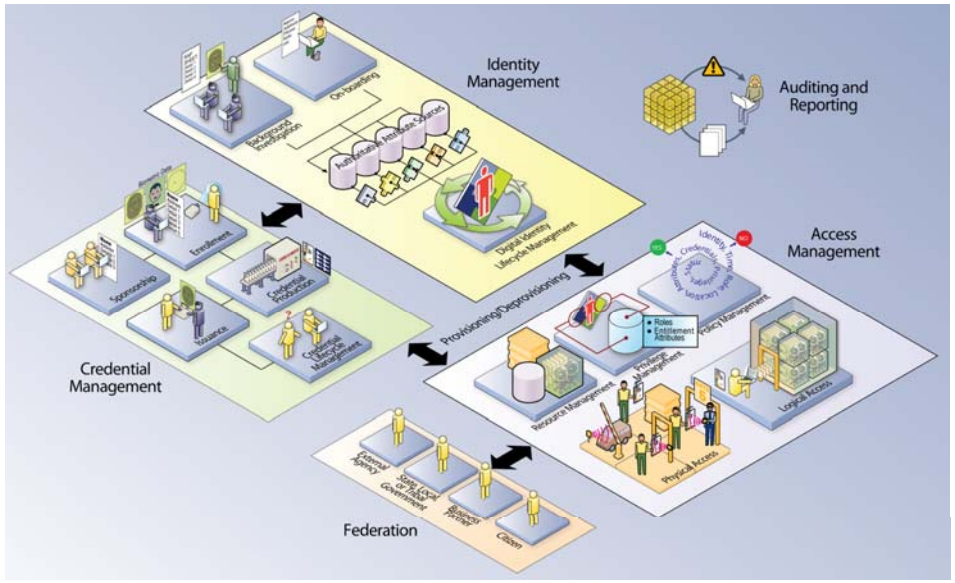
www.idmanagement.gov

The Future of Federal Identity Management

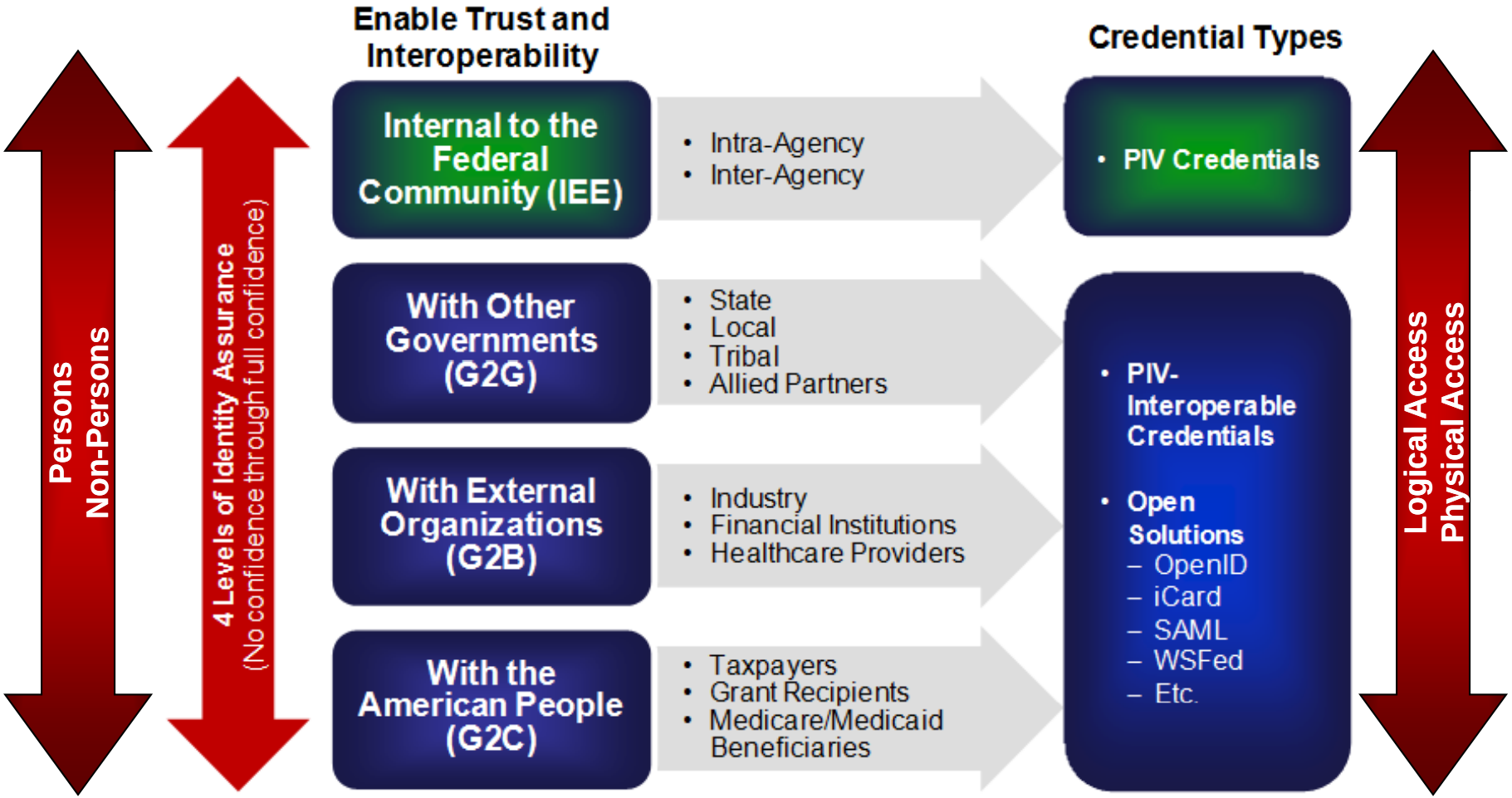
Judith Spencer
Agency Expert - IDM
Office of Governmentwide Policy
GSA
Judith.Spencer@GSA.Gov

What is ICAM?

- ICAM represents the intersection of digital identities, credentials, and access control into one comprehensive approach.
- Key ICAM Service Areas Include:
  - Digital Identity
  - Credentialing
  - Privilege Management
  - Authentication
  - Authorization & Access
  - Cryptography
  - Auditing and Reporting



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

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

Presidents Budget for FY 2010

Extract from Section 9.
LEVERAGING THE POWER OF TECHNOLOGY TO TRANSFORM THE FEDERAL GOVERNMENT

- To support this effort, the Federal Identity, Credential, and Access Management (ICAM) segment architecture provides Federal agencies with a consistent approach for managing the vetting and credentialing of individuals requiring access to Federal information systems and facilities

- 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.

FICAM Roadmap & Implementation Guidance Overview

- The Federal ICAM Roadmap outlines a strategic vision for identity, credential, and access management efforts within the Executive Branch of the Federal Government and how the Executive Branch of the Federal Government will interact with external organizations and individuals.

PART A: ICAM Segment Architecture (Phase 1 of the effort)

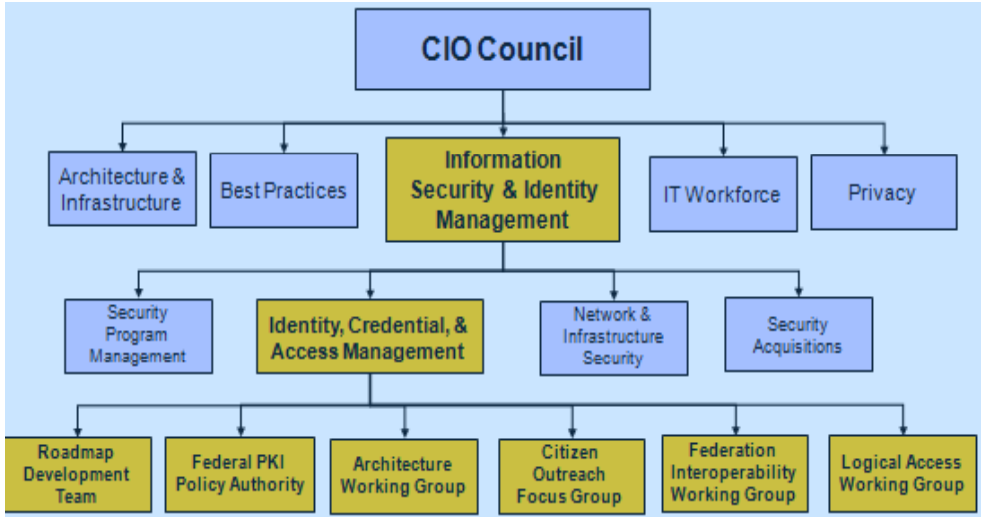
- **ICAM Segment Architecture.** Standards-based architecture that outlines a cohesive target state to ensure alignment, clarity, and interoperability across agency initiatives.
- **ICAM Use Cases.** Illustrate the as-is and target states of high level ICAM functions and frame a gap analysis between the as-is and target states.
- **Transition Roadmap and Milestones.** Defines a series of logical steps or phases that enable the implementation of the target architecture.

PART B: Implementation Guidance (Phase 2 of the effort)

- **ICAM Implementation Planning.** Augments standard life cycle methodologies as they relate to specific planning considerations common across ICAM programs.
- **Implementation Guidance.** Provides guidance to agencies on how to implement the transition roadmap initiatives identified in the segment architecture, including best practices and lessons learned.

FICAM Development Process

- The development process involves coordination and collaboration with Federal Agencies, industry partners, and cross-government working groups.
  - Interagency Security Committee (ISC)
  - Information Sharing Environment (ISE)
  - White House National Science and Technology Council (NSTC)
  - Committee for National Security Systems (CNSS)
  - Office of Management and Budget
  - National Institute of Standards and Technology (NIST)
  - Office of National Coordinator (ONC) for Health IT
  - Multiple agencies represented within the CIO council subcommittees and working groups



- The Roadmap team identified the key outputs of the Federal Segment Architecture Methodology (FSAM) needed for an ICAM segment architecture and coordinated these groups to develop workable approaches to enable cross-government solutions.

Components of the ICAM Segment Architecture

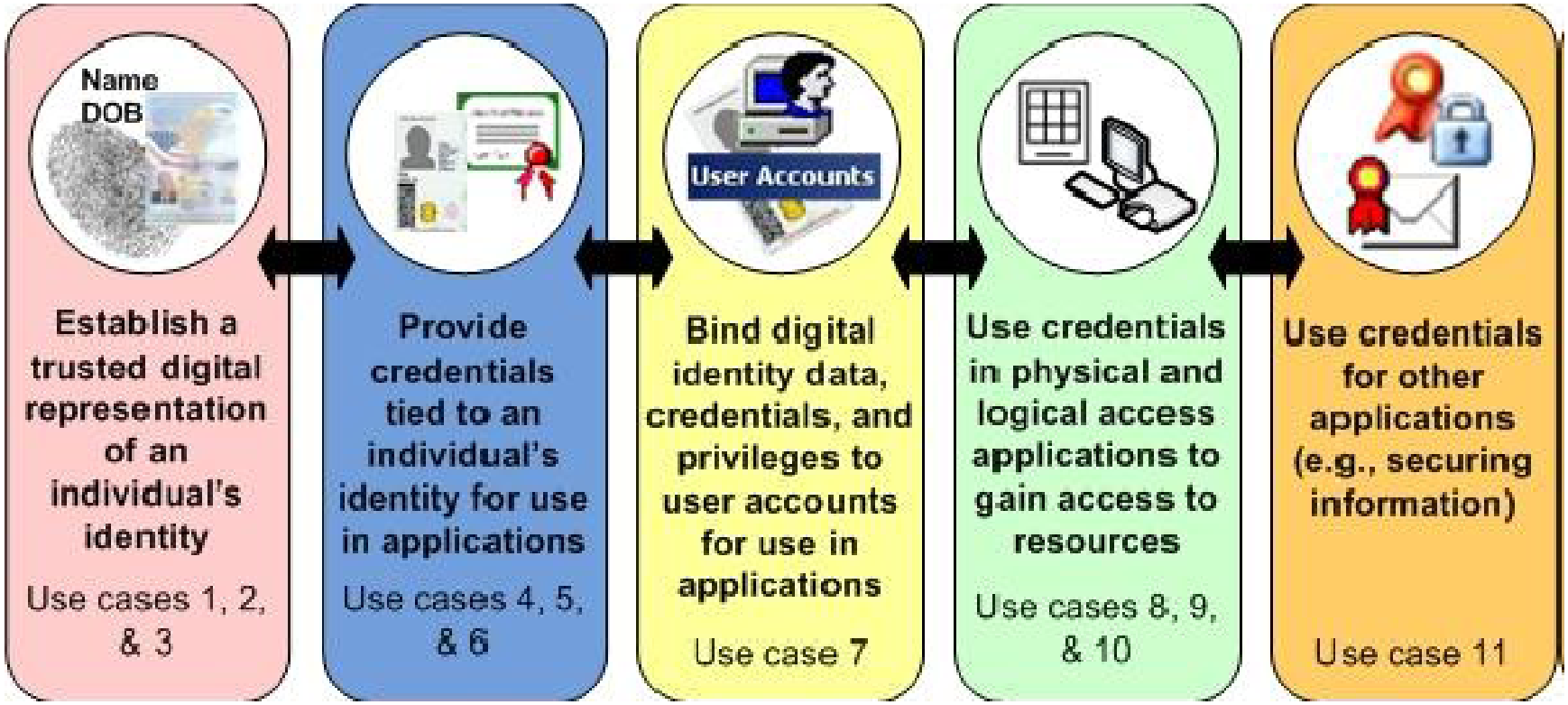
Performance Architecture	• Outlines strategic vision for ICAM • Includes 32 performance metrics, 4 of which will be tracked on data.gov
Business Architecture	• 11 use cases representing high level government-wide ICAM functions • Supports IEE, G2G, G2B, and G2C scenarios
Data Architecture	• Details data sources and elements supporting each use case • Illustrates the flow of information within the use cases
Service Architecture	• Defines service types and components specific to ICAM • Supports the Federal Enterprise Architecture Service Reference Model
Technical Architecture	• Comprise the high level vision of the technical architecture • Target state moves towards shared agency and federal infrastructures

ICAM Goals and Objectives

The Federal ICAM Roadmap addresses unclassified federal identity, credential, and access management programs and demonstrates the importance of implementing the ICAM segment architecture in support five overarching strategic goals and their related objectives.

Goal 1: Comply with Federal Laws Relevant to ICAM	Goal 2: Facilitate E-Government by Streamlining Access to Services	Goal 3: Improve Security Posture across the Federal Enterprise	Goal 4: Enable Trust and Interoperability	Goal 5: Reduce Costs and Increase Efficiency
• Align and Coordinate Federal Policies and key initiatives impacting ICAM Implementation • Establish and Enforce Accountability for ICAM implementation to Governance Bodies	• Expand Secure Electronic Access to Government Data and Systems • Promote Public Confidence through Transparent ICAM Practices	• Support Cybersecurity Programs • Integrate Electronic Verification Procedures with PACS • Drive the Use of a Risk-based Framework for Access Control • Improve Electronic Audit Capabilities	• Support ISE Committees of Interest • Align Processes with External Partners • Establish and Maintain Trust Relationships • Leverage Standards and COTS for ICAM Services	• Reduce Administrative Burden Associated with Performing ICAM Tasks • Align Existing and Reduce Redundant ICAM Programs • Increase Interoperability and Reuse of ICAM Programs and Systems

Eleven Use Cases Covering:



On-Going Activities

- PIV Interoperability: Defining the parameters for an 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
- Federal PIV deployment exceeds 60%
  - LACS deployment beginning
  - PACS demonstration system operational

Summary

- ICAM is foundational to information sharing and collaboration
- Federal CIO Council ICAM activities are key to strong identity and access management
- We must move forward together if we are to be successful
- Progress depends on public-private partnering
- Our work is just beginning
- Keep pace with ICAM: www.idmanagement.gov

12