Introductions

ICAM Refresh/Overview of Fundamentals

ICAMSC Update

ICAM Current State

What’s Next for ICAM
Deb Gallagher: General Services Administration

Paul Grant: Department of Defense

Leo Scanlon: National Archives and Records Administration
Government-wide ICAM Update Panel Discussion
ICAM Forms the Foundation of Business Operations

Identity Management
- Protect personally identifiable information
- Securely share attributes
- Implement PIV for employees & contractors
- Leverage PKI
- Leverage trusted externally-issued credentials (e.g., PIV-I)

Access Management
- Manage users & accounts
- Access federal facilities
- Access IT Resources
- Federate access for external users
- Leverage PKI

Credential Management

Agency Employees & Contractors
Customers
Business Partners
ICAM processes and solutions are central to the ability to manage systems and resources, streamline day-to-day business activities, and enable trusted interaction with authorized individuals.
Government-wide ICAM Update Panel Discussion
ICAM and HSPD-12 are Fundamental to…

Cybersecurity

Know who is on your networks, control access, and monitor activity

- Security Breaches
- Insider Threat
- Phishing
- Unintended Disclosure and Loss of PII
- Malicious Devices, Applications, and Code

Business Process Improvement

Streamline and automate user and resource management within and across agencies

- Paperless Processes
- Interoperability with Many Communities
- Asset Management
- Extended and Shared Trust Nationally
- Maximize ROI
Government-wide ICAM Update and Panel Discussion
Identity, Credential and Access Management Subcommittee Priorities

Federal CIO Council
  + Information Security and Identity Management Committee (ISIMC)
    - Federal PKI Policy Authority (FPKIPA)
      - Technical Working Group (TWG)
      - PKI Shared Service Provider Working Group (SSP WG)
    - Identity, Credential, and Access Management Subcommittee (ICAMSC)
      - Joint CNSS Identity & Access Management (CNSS IdAM WG)
      - Identity Federations Coordination (IFC) Working Group – Joint with Information Sharing & Interagency Policy Committee (ISA IPC)
      - Modernized Physical Access Working Group (MPAWG) - Joint with Interagency Security Committee (ISC)

Color Key of Organizational Bodies
- Council
- Committee
- Subcommittee or Authority
- Working Group Support
- Tiger Team Support
- Short-term Standing

NPE Credential Tiger Team
Privileged User Management Tiger Team
Access Management Policy Framework Tiger Team
Access Control and Attribute Governance Tiger Team
Currently, the ICAMSC has four tiger team supporting the priority items in alignment with the direction from the Federal CIO Council

<table>
<thead>
<tr>
<th>Priority Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management Policy Framework</td>
<td>This framework will be based on an analysis of current agency practices, policies and requirements, and will provide implementation guidance for creating and managing authorization at the enterprise level.</td>
</tr>
<tr>
<td>Privileged User Instruction</td>
<td>Provides federal agencies with guidance on the implementation and monitoring of privileged user management in alignment with the priorities of the ICAMSC and ISIMC and in coordination with related efforts already underway in other federal communities (e.g., Intelligence Community, working groups).</td>
</tr>
<tr>
<td>NPE Decision Document</td>
<td>Document the decision of how non-person entity (NPE) credentials will be implemented in the Executive Branch (two phases)</td>
</tr>
<tr>
<td>Attribute Implementation Instruction</td>
<td>This instruction document will address life cycle management of attributes and include a registry of the available/approved attributes (developed as a coordinating work item with federation activities).</td>
</tr>
</tbody>
</table>
In order to meet the breadth of ICAM agency needs, the ICAMSC has been focusing on the following items in parallel:

<table>
<thead>
<tr>
<th>Groups</th>
<th>Activities/Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Technology Tiger Team (MTTT)</td>
<td>• Mobile Pilot Solution Case Studies</td>
</tr>
<tr>
<td>FIPS 201/FICAM Testing Team</td>
<td>• Ensuring that product categories and FICAM-approved products are available to agencies to meet implementation needs</td>
</tr>
<tr>
<td>Management Working Group (CNSS IdAM WG)</td>
<td></td>
</tr>
<tr>
<td>Identity Federations Coordination Working Group (IFC WG)</td>
<td>• <em>Priority Objective #4 (PO#4) Implementation Plan</em></td>
</tr>
<tr>
<td>Access Control and Attribute Governance Working Group (ACAG</td>
<td>• Trusted Framework Solutions suite of documents</td>
</tr>
<tr>
<td>WG)</td>
<td></td>
</tr>
</tbody>
</table>
Government-wide ICAM Update and Panel Discussion
Current State of PIV Issuance

![Bar chart showing the current state of PIV issuance across various agencies](chart.png)

- **DHS**: 70% Issued and Required, 11% Issued but Not Required
- **DOD**: 89% Issued and Required, 0% Issued but Not Required
- **HUD**: 100% Issued and Required, 0% Issued but Not Required
- **NRC**: 100% Issued and Required, 0% Issued but Not Required
- **NSF**: 100% Issued and Required, 0% Issued but Not Required
- **SSA**: 99% Issued and Required, 1% Issued but Not Required
- **State**: 11% Issued and Required, 89% Issued but Not Required
- **EDU**: 24% Issued and Required, 76% Issued but Not Required
- **EPA**: 98% Issued and Required, 2% Issued but Not Required
- **DOT**: 90% Issued and Required, 10% Issued but Not Required
- **VA**: 97% Issued and Required, 3% Issued but Not Required
- **DOI**: 93% Issued and Required, 7% Issued but Not Required
- **HHS**: 84% Issued and Required, 16% Issued but Not Required
- **Treasury**: 92% Issued and Required, 8% Issued but Not Required
- **OPM**: 73% Issued and Required, 27% Issued but Not Required
- **NASA**: 56% Issued and Required, 44% Issued but Not Required
- **DOC**: 75% Issued and Required, 25% Issued but Not Required
- **DOE**: 80% Issued and Required, 20% Issued but Not Required
- **GSA**: 69% Issued and Required, 31% Issued but Not Required
- **USDA**: 69% Issued and Required, 31% Issued but Not Required
- **DOJ**: 44% Issued and Required, 56% Issued but Not Required
- **USAID**: 59% Issued and Required, 41% Issued but Not Required
- **SBA**: 49% Issued and Required, 51% Issued but Not Required
Washington Metropolitan Area Transit Authority (WMATA) New Electronic Payments Program (NEPP) Vision:
- Enhance customer experience
- Improve fare system reliability
- Reduce the cost of processing transactions

The Program Scope includes the following:
- New central data system; hardware and software
- New gates, ticket vending machines
- New contactless smart card readers on bus and parking
- Updated website and customer interfaces
Leveraging ICAM processes and solutions provides:

- Foundational support for cybersecurity by protecting access to Federal Government resources
- Foundational for business process improvement
- Potential for future value-added applications of the PIV (e.g., transit benefits, payment)
Align  Collaborate  Enable