Federal Chief Information Officer Council
Federal Chief Information Security Officer Council
Identity, Credential, and Access Management Subcommittee Charter

Developed June 2018

Updated September 2023

Name

Identity, Credential, and Access Management Subcommittee - ICAMSC

Authority

The ICAMSC is established under the Federal Chief Information Security Officer Council. It is one element of an interagency support structure established to achieve information resource management and security objectives delineated in statute and executive policy, including but not limited to:

1. E-Government Act of 2002 (Public Law 107–347) on December 17, 2002.
2. Homeland Security Presidential Objective 12 - Policies for a Common Identification Standard for Federal Employees and Contractors on August 27, 2004.
3. Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure on May 11, 2017.
4. OMB Circular A-130 - Managing Information as a Strategic Asset on July 28, 2016.
5. OMB Memo 19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management on May 21, 2019.
6. Credential Executive Agent Memorandum on Credentialing Standards Procedures for Issuing PIV Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for PIV Credentials on December 15, 2020.
7. Executive Order 14028 - Executive Order on Improving the Nation's Cybersecurity on May 12, 2021.
8. OMB Memo 22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles on January 26, 2022.

Purpose

The Federal CISO Council ICAM Subcommittee is the principal interagency forum to improve the enterprise-wide approach to workforce ICAM governance, architecture, modernization, security, acquisition, and performance. Workforce ICAM is defined as an agency issued and managed digital identity used to help the agency deliver its mission.

Vision

The ICAMSC aspires to be the catalyst in enabling federal agencies to meet its mission and deliver federal services that are convenient and secure. Reduce friction in using digital identities across the federal government. Continuously enhance workforce digital identity practices and processes across the federal government.

Objectives and Functions

The ICAMSC shall be the principal interagency forum for topics related to identity, credential, and access management of enterprise and mission application. These two communities are split between the federal workforce (agency staff and contractors) and partner identities. In support of this role, the ICAMSC is responsible for performing the following objectives and functions:

1. **Governance Coordination**
    a. Establish and maintain a link between the ICAMSC and agencies' governance structures for effective interagency coordination.
    b. Obtain, aggregate, and assess common risks (e.g., mission, strategic, reputation, security) to coordinate an appropriate response (e.g., policy recommendations, services, frameworks, etc.).
    c. Consult with the Office of Management and Budget Office of the Federal CIO (OFCIO), NIST and CISA to consider both government-wide and agency priorities to establish Federal ICAM strategies and roadmaps.
    d. As necessary, the ICAMSC provides performance reports to update the community on government wide ICAM advancements.
2. **Policy Development Support & Recommendations**
    a. Recommend new ICAM policies or update existing ones. These recommendations are to be presented to the Chief Information Security Officer Council (CISOC), the Chief Information Officers Council (CIOC), and the OFCIO for consideration for policy action. All policy recommendations should reflect priorities of agency executives.
3. **Facilitating Communications and Information Sharing**
    a. Share lessons learned, ideas, best practices, and innovative approaches.
    b. Solicit perspectives affecting ICAM from other councils, as well as industry, academia, and other Federal, tribal, and state and local governments and provide outreach.
4. Technical Guidance, Requirements, and Best Practices.
    a. Support the development and use of ICAM performance measures.
    b. Develop and maintain standardized business requirements for use in agency acquisitions and operations.
    c. Advance and promulgate a cohesive Identity landscape that include components of architecture, terminology, infrastructure, conformance, recognition, and acquisition.

Subcommittee Leadership and Responsibilities

The ICAM Subcommittee shall be led by three chairs and validated on an annual basis.

- A lead chairperson is named by the General Services Administration Office of Government-wide Policy Associate Administrator from the GSA OGP Identity Assurance and Trusted Access Division. This chair is primarily responsible for ICAM governance, as well as working with agencies to evolve the federal identity landscape which includes components such as architecture, technical specifications, conformance, and useability.
- A vice chairperson is named by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency Cybersecurity Division Executive Assistant Director. This chair is primarily responsible for aggregating and assessing risks and threats affecting ICAM systems and assuring alignment within the ICAM landscape, strategy, and methodologies.
- A voted chair is selected by the ICAM subcommittee to serve two consecutive, one-year terms, but may serve multiple terms beyond two years. This chair is responsible for assuring effectiveness of ICAM processes through leading benchmarking, evaluations, and reviews.

The Subcommittee leadership shall be responsible for:

- Promoting ICAM Subcommittee activities and status within the Federal IT and Security community.
- Convene the ICAM Subcommittee on a regular basis and preside over Subcommittee meetings.
- Act as an advocate and elevate issues to the appropriate levels on behalf of the ICAM Community.
- Participate as leaders in the broader Federal IT Community to help foster cross-agency collaboration and shared solutions above and beyond the agency silos.
- Manage subcommittee operations and structure.
- Serve as the final decision-making body.
- Oversee and assign work of the subcommittee.

Membership

The ICAMSC member is a federal employee, GS-13 or above, and the agency designated ICAM representative for the integrated agency-wide ICAM office, team, or governance structure identified in OMB M-19-17. The Agency CISO shall designate a primary and secondary ICAMSC member. Each primary member may also identify a secondary representative if not identified by the Agency CISO. The membership is confirmed on an annual basis by the Agency CISO or through the Federal CISO Council. The ICAM Subcommittee shall be composed of the following voting member agencies.

- The Agency ICAM Lead from each agency described under section 901(b) of Title 31 of the U.S. Code.
- The ICAM Agency Lead for the Department of the Army, Department of the Navy, and the Department of the Air Force.
- Two Small Agency Council representatives.
- One representative for the legislative and judicial branch.

Member Responsibilities

The members of the ICAM Subcommittee shall:

- Attend the regularly scheduled meetings called by ICAM leadership.
- Review and consider initiatives presented at Subcommittee meetings and be an active participant in the discussions.
- Provide recommendations and/or cast a vote regarding the presented initiatives and participate in prioritization of presented initiatives.
- Bring to the Subcommittee's attention initiatives and issues that might have an impact on the overall Federal IT community.
- Participate in implementation of Subcommittee's priority initiatives or projects.
- Participate as a leader of the broader ICAM community to help foster cross-agency collaboration and shared solutions above and beyond agency silos.

Ex Officio Members

Ex Officio members represent a shared, governmentwide workforce identity function in either shared services, requirement or standard development, identity policy development, or coordination. Each Ex Officio member will identify one primary and secondary representative to attend and participate. Additionally, any federal agency CISO can appoint their ICAM lead to join the ICAMSC. They do not have voting rights.

- Office of Management and Budget Office of the Federal Chief Information Officer
- Department of Homeland Security Continuous Diagnostic and Monitoring
- Department of Homeland Security Quality Service Management Office
- General Services Administration Federal Acquisition Service
- Office of Personnel Management Suitability and Credentialing Executive Agent
- National Institute of Standards and Technology
- National Archives and Records Administration
- Governmentwide workforce identity shared services
- Co-Chairs of any ICAM Subcommittee chartered sub-groups.
- At least one state and local government representative.
- Others designated by vote of the ICAM Subcommittee leadership or appointed by an Agency CISO.

Structure and Procedures

The ICAMSC is responsible for the following items.

- Set subcommittee priorities.
- Aligning FICAM work products.

- Establish working groups, tiger teams, task forces, and other temporary bodies as necessary to consider items that are of concern to the subcommittee and to carry out implementation of Federal ICAM initiatives or projects.

The ICAMSC meets every month and is open to any ICAMSC member. Only federal employees may regularly attend the ICAMSC meetings.

Subcommittee Support

The General Services Administration Office of Government Policy shall provide administrative, archival of all minutes and documents, and other subcommittee support. The secretariat staff is led by the GSA OGP Identity Assurance and Trusted Access Division Director and shall provide strategic guidance, coordinate subcommittee activities, including setting priorities, promoting collaboration, and managing the subcommittee budget.

Working Groups

The ICAMSC has the authority to establish working groups, or other bodies as necessary, to support its mission, purpose, and functions. Groups are co-chaired by an agency ICAM lead, or by other individuals as the subcommittee may designate, at least one of whom shall be a federal employee. Membership may include a broader set of agency implementers and direct support contractors. The ICAMSC may establish working groups as standing or ad hoc. The ICAMSC leadership may disband the groups at their discretion. Participants have the following responsibilities:

- Actively participate and represent home agency priorities and experience.
- Coordinate reviews of work products with stakeholders across their agency.
- Contribute content and ideas and drive progress towards timelines.
- Communicate, coordinate, and align policy and implementation best practices.

Standing working groups include:

- Federal PKI Policy Authority - Manage the PKI trust framework for digital certificates in support of HSPD-12 and digital signature interoperability.
- Digital Identity Community of Practice – Designed for any federal employee or contractor practitioners who want to learn more about ICAM as well as recommend initatives to the ICAMSC.

Voting

When votes are taken, each member of the Subcommittee will get one vote, including the two representatives for small agencies, who will have one vote each. Votes will be held on official matters with the lead chair as the tie-breaking vote. There is no minimum requirement to establish a quorum at a meeting. The number of members required for a quorum will be the number of members at a meeting. Ex-officio members are invited to contribute their expertise to projects and work groups, but do not have a vote.

Amendments and Effective Date

This charter may be amended upon the request and approval of the ICAMSC leadership and coordinated with the CISO Council and OMB. This charter is effective as of the date signed and remains so until modified or rescinded.

Signatures

The undersigned is a CISO Council representative authorizing this charter.

DocuSigned by:
Steven M Hernandez
E77E1AC4A3B84DE...

CISO Council Representative
Name / Date 10/11/2023

The undersigned accept the responsibilities of an ICAMSC leadership position.

DocuSigned by:
Kenneth Myers
3CCF9722230043F...

GSA OGP Chair 9/8/2023
Name / Date

DocuSigned by:
Ross Foard
DC65DAC2E155488...

DHS CISA Chair 9/11/2023
Name / Date

DocuSigned by:
Ramon Burks
F0B282A880594BA...

Voted Chair 10/11/2023
Name / Date