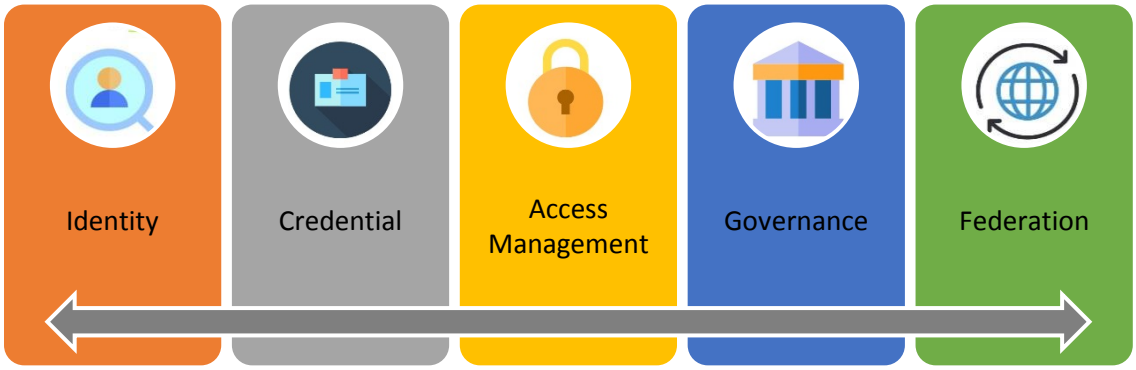
Reference Materials for Identity, Credential, and Access Management (ICAM) for Public Safety



During emergency response operations the ability for public safety personnel to make the best possible decisions, as well protect themselves and the public; requires getting the right information to the appropriate emergency response personnel in a timely manner, however, the lack of a nationwide information strategy is a significant barrier for federal, state, local, and tribal public safety agencies. Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.

The following resources provide information on core principles and critical components related to ICAM, the Trustmark Framework, and other federal and government sponsored ICAM initiatives.

Introduction to ICAM

Information Sharing Environment (ISE) Introduction to ICAM Principles – ISE Fact Sheet on ICAM principles and terms.

ICAM, "An Information Exchange for Information Security and Privacy Advisory Board" – PowerPoint presentation from the Federal CIO Council explaining the basics of ICAM.

Nationwide ICAM Initiatives

Federal Identity, Credential, and Access Management (FICAM) – Created in 2008, FICAM coordinates the US Federal agencies on execution of the related policy, standards, implementation guidance, and information technology architectures.

- List of FICAM's "Adopted Trust Framework Providers" – the Trust Framework Solutions (TFS) program assesses the Trust Frameworks of commercial and non-profit organizations to

determine if the polices, processes and technologies are comparable to the US Federal Standards for identity assurance, authentication assurance and privacy protections.
- FICAM Framework and Overview
- FICAM Roadmap and Implementation Guidance

Global Federated Identity and Privilege Management (GFIPM) Program – Initiated in 2005, the GFIPM program is part of the Global Justice Information Sharing Initiative. GFIPM seeks to develop secure, scalable, and cost-effective technologies for information sharing within the law enforcement and criminal justice communities.

Identity and Access Management (IdAM) – The Department of Defense (DoD) envisions IdAM as the combination of technical systems, policies and processes that create, define, and govern the utilization and safeguarding of identity information, as well as managing the relationship between an entity and the resources to which access is needed. The vision of IdAM is to allow person and non-person entities to securely access all authorized DoD resources, anywhere, at any time.

National Identity Exchange Federation (NIEF) – NIEF is a collection of federal agencies that share sensitive law enforcement information. NIEF leverages existing GFIPM work products and also serves as a source of real-world feedback to drive the development of new GFIPM work products.
- Policies for NIEF Trustmarks - NIEF offers a wide range of trustmarks to its members and other agencies that wish to participate in the emerging Trustmark ecosystem.

National Information Exchange Model (NIEM) – NIEM establishes a common vocabulary of reusable, and repeatable data terms, definitions, and processes to facilitate machine-readable information exchanges between communities of interest (COI).

State Identity, Credential, and Access Management (SICAM) – The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.
- California Department of Public Safety: Identity, Credential, and Access Management (ICAM) Roadmap and Implementation Guide – Outlines California's strategic vision for state-based identity, credential, and access management efforts. The California SICAM architecture enables the state and its partners to share and audit identification, authentication, and authorization across enterprise boundaries.

Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (TFOPA) – The Federal Communications Commission (FCC) established TFOPA to analyze the current structure and architecture of the nation's PSAPs facilities; and to determine if additional consolidations of PSAP facilities and architecture would enhance the efficiency of public safety communications, performance, and operations functionality.
- TFOPA Working Group 1: Optimal Cybersecurity Approach for PSAPs (December 2015) – Details the intersection between the nationwide cybersecurity initiative and implementing a nationwide federated ICAM solution. Both are needed to ensure secure and interoperable information sharing throughout the public safety community.
- TFOPA Adopted Final Report (January 2016) – Includes a high-level overview of ICAM goals and objectives as well as references federal implementation model (IFICAM). The Report emphasizes

the need to educate the public safety community on identity control and access management at all levels of interface.

FirstNet – FirstNet, through the Public Safety Advisory Committee (PSAC), established a Task Team in February 2016 to review ICAM. ICAM is a critical enabler for facilitating mutual aid and assisting first responders in accessing necessary data to effectively perform their duties. FirstNet's goals for this task team are to understand some of the issues that public safety agencies experience today due to the lack of an inter-operational ICAM solution; document initial governance rules for ICAM use in public safety; establish a framework for onboarding agencies into the use of federated identity; and examine potential working ICAM solutions. Further, as FirstNet begins to explore ICAM-enabling technologies to undercover potential risks or roadblocks, we want to ensure that we incorporate the PSAC recommendations into these efforts.

- Interview with Harlin McEwen on key findings from the PSAC's report to FirstNet about the implementation of ICAM.
- FirstNet Early Builders Blog details lessons learned from five public safety Long Term Evolution (LTE) network projects.

ICAM Program Offices and Coordination Programs

National Institute of Science and Technology NIST, Trusted Identities Group (TIG) – The TIG is focused on achieving an environment in which individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. NIST has published cybersecurity standards (NIST 800 series), released a Cybersecurity Framework, and administers The National Strategy for Trusted Identities in Cyberspace (NSTIC)

- National Strategy for Trusted Identities in Cyberspace (NSTIC) – Administered through NIST, NSTIC charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions.

Program Manager for the Information Sharing Environment (PM-ISE) – The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the Office of the PM-ISE and granted it the authority to plan, oversee, and manage the Information Sharing Environment. PM-ISE is located within the Office of the Director of National Intelligence, Partner Engagement office.

- 2014 National ICAM Strategy Summit: After Action Report – The 2014 ICAM National Strategy Summit: After Action Report provides foundational information on ICAM, identifies key ICAM principles and recommended actions for public safety.

Standards Coordinating Council

The Standards Coordinating Council provides oversight in the world of standards-based information sharing and safeguarding, locating and assessing efforts by disparate organizations and identifying how they fit into the information sharing standards landscape.

ICAM Pilots and Proof of Concept Projects

GTRI NSTIC Trustmark Framework Pilot – GTRI maintains a website with general information, technical specifications, and artifacts for the Trustmark Framework.

- ISE Article – An ISE story on the NIEF Trustmark Pilot for Federated ICAM and its goals.
- ISE Blog Post – Blog post on the Trustmark Framework and its inclusion as a FICAM Trust Framework Provider.

NSTIC Pilots: Catalyzing the Identity Ecosystem (NISTIR 8054) – Summaries and outcomes of NSTIC pilots, including the Trustmark Framework.

Visit the SAFECOM website to learn more about the ICAM Working Group, ICAM, and the Trustmark Framework: https://www.dhs.gov/safecom/icam-resources