DHS Science and Technology Directorate
Identity, Credential, & Access Management (ICAM) Acquisition and Implementation Guidance

First Responders Need to Share Information, Validate Users and Maintain Records

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Project Responder 5 Report identified key capabilities necessary to help first responders be more effective in their mission. Findings included the need to securely share information, validate responders from other organizations and securely maintain records.

These challenges only increase as responders rely on more data from more sources of information. There is a critical need for responders to securely validate users and share information. Identity, Credential, & Access Management (ICAM) principles can mitigate these challenges.

What is ICAM?

ICAM is a framework of policies built into an organization's IT infrastructure that allows system owners to have assurance that the right person is accessing the right information at the right time for the right reason. ICAM policies fall into four management categories:

Identity – A set of characteristics that describe a person.

Credential – Evidence of a person's identity linked to a record within an organization.

Access – Authorization of only permitted users to interact with certain information within a system.

Federation – The ability for one organization to accept another organization's credentials based on reciprocal trust.

An organization implements ICAM policies under these four management categories to achieve secure and scalable information sharing, user access and validation and records maintenance within its system.

What is ICAM's Impact?

ICAM is adaptable to first responder needs at all levels of government. It enables first responders to focus on their essential mission functions by bringing security, scalability and interoperability through embedded policies within their systems.

Risk Assessment

A responder organization must first determine what type of information is in its system, the risk associated with that information and what level of protection it requires. Once known, ICAM polices are built to secure an organization's information.

Identity, Verification, Access

Responder organizations must stringently verify the identities of its personnel (i.e., perform background checks). Identities are then tied to credentials (e.g., an ATM) card). For added security, a second factor is added to that credential, such as a PIN. Multifactor authentication includes "something you know" (PIN), "something you have" (ATM card) or "something you are" (fingerprint).

Then, organizations link characteristics of the individuals to their credential and create policies to determine when certain individuals can obtain access to that information. Attribute-based access control (ABAC) is an approach that empowers streamlined access to data by automatically applying an organization's policies for protecting data based on the requesting individual's characteristics. Finally, a trust federation, or collection of policies agreed to by multiple organizations, allows information sharing across jurisdictions by all users within the federation.

ICAM Acquisition and Implementation Materials

The Public Safety Communications ICAM Working Group has developed ICAM Acquisition and Implementation Guidance. The documents will be released in summer 2018:

- **ICAM Executive Primer** – a high-level overview for executive leadership of key concepts and real-world scenarios of ICAM principles.
- **ICAM Acquisition Guidance** – an overview for Program Managers of what to look for while acquiring ICAM products, and advice to Solutions Architects about lessons learned from the implementation of ICAM-enabled systems with multifactor authentication.
- **ICAM Implementation Guides** – step-by-step guides integrating various combinations of commercially available products to create ICAM-enabled systems, which allow system engineers to properly install and configure ICAM solutions to enhance the organization's security with multifactor authentication.

These knowledge products will be made available to S&T's first responder stakeholders and partners at all levels of government to enhance secure, scalable and interoperable information sharing, user validation and records maintenance.

To learn more about ICAM within the first responder community, contact first.responder@hq.dhs.gov.

2018-06-06