Federated Identity, Credential, and Access Management Value Proposition Scenario: School Active Shooter Response

BACKGROUND

According to the Federal Bureau of Investigation, 277 active shooter incidents occurred in the United States from 2000 to 2018, of which 57 (21 percent) occurred in educational environments.[1] In response to this unfortunate reality, many schools now maintain Action Response Plans (ARPs) that can provide key information to help first responders coordinate an effective and rapid response to shooting incidents. ARPs include floor plans, daily schedules, access codes, exit diagrams, contact information, and other images and documents that can aid the responders. ARPs can help first responders respond to shooting incidents more rapidly and more effectively, resulting in fewer injuries and deaths — but only if the data can be shared with those who need it, when they need it.

INFORMATION SHARING CHALLENGES

During an active shooter response, every second matters, and wasted time and confusion among first responders can result in lives lost. First responders at the scene need to coordinate with each other and with additional off-site resources such as dispatchers and Real Time Crime Centers (RTCCs) that provide real-time intelligence, analysis, and other logistical support. But gathering and disseminating ARP data and other critical data securely and quickly is a challenge. An ARP for the school may not exist, and if it does, it may be out of date, available only in hardcopy format, or stored in a secure electronic location that is not accessible to all of the responding agencies. Additionally, other important data such as criminal records or criminal intelligence data about the suspected shooter may exist, but is stored in systems that are accessible only by personnel with special certifications (e.g., 28 CFR Part 23 training), and not readily available to those who need it on site. As a result, on-scene responders and logistical support staff today often resort to slow and inefficient methods of data sharing, such as email or in-person exchanges, for situational awareness. This may result in delay, confusion, and suboptimal decisions that too often lead to wasted time and unnecessary casualties.

POTENTIAL FOR FEDERATED IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

Better information sharing solutions and capabilities would lead to better outcomes for school shooting responses. An ideal solution would allow any person with proper credentials and authorization — whether an on-scene first responder, RTCC intelligence analyst, school official, or other approved user — to not only view ARP data and other related data during an incident, but to also create and update the aspects of the ARP that require changes over time (schedules, access codes, etc.) in advance of an incident. This would lead to more accurate data, maintained in a timely fashion by those who can best maintain it, and accessible by those who need it when they need it. A system or application that provides these capabilities to schools and first responders can result in lifesaving and cost saving benefits.

[1] *Quick Look: 277 Active Shooter Incidents in the United States From 2000 to 2018*. Federal Bureau of Investigation. https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics (accessed July 1, 2020).

However, creating a system to collect, maintain, and share this data among a large group of people is challenging. Managing users and access levels can be complex and costly, especially since authorized users can come from many different types of organizations. Users must be properly vetted and attested in order for the system and data to be trusted. The data needs to be accessible, but also secured in a way that is trusted. The data needs to be accessible, but also secure. Federated ICAM enables many types of data sharing systems and applications that span multiple agencies and communities. Under a Federated ICAM approach, authorized users are issued credentials and provided with attributes by their home agencies or organizations. These credentials and attributes allow the user to log into information sharing systems and applications and access shared data.

ACTIVE SHOOTER VALUE PROPOSITION

- Facilitate viewing and sharing of Action Items
- Enable access to criminal records or criminal intelligence data
- Improve coordination with off-site resources such as dispatchers and Real Time Crime Centers (RTCCs)
- Create and update aspects of Action Response Plans in advance of an incident

SAFECOM AND THE NATIONAL COUNCIL OF STATEWIDE INTEROPERABILITY COORDINATORS

SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) recognize the vast potential of Federated ICAM to improve public safety information sharing, and they also recognize the lack of clear Federated ICAM implementation guidance available to public safety agencies today. In response, they are developing a new framework of Federated ICAM implementation tools and guidance that will enable public safety agencies to reap the tremendous potential benefits that Federated ICAM can provide.

Five major components of a successful ICAM program.

TRUSTMARK FRAMEWORK

The proposed solution SAFECOM and NCSWIC are developing is based on an emerging technology called "trustmarks." Trustmarks will enable agencies to quickly and easily discover and define the policy requirements for their information sharing use cases in a transparent, standard way. Trustmarks also will enable agencies to quickly and cost-effectively demonstrate that their personnel and applications comply with those requirements. This framework can be integrated into existing information sharing applications and future applications quickly and cost-effectively. When it is available, this framework will provide a clear and cost-effective path for agencies to develop trusted information sharing relationships and implement trusted information sharing systems that will lead to more effective mission outcomes across the entire public safety community.

VISION FOR TRUSTMARKS

- Standardize policy requirements
- Information sharing transparency
- Cost-effective solution
- Leverage existing identity credentials
- Ease of integration