Federated Identify, Credential, and Access Management Value Proposition Scenario: 2018 Austin Bombing Response

BACKGROUND

From March 2 to March 20, 2018, a man distributed multiple package bombs around the city of Austin, Texas, killing two people and injuring five more. Law enforcement personnel from many local, state, and federal agencies offered their support to the Austin Police Department (APD). The resulting criminal investigation involved crime scenes dispersed around the city and region and presented a massive coordination and information-sharing challenge for APD and its investigative partners. There was a need to share tips and suspicious activity reports generated by the public, victim and witness statements, and general situational awareness about the locations and activities of participating personnel. At the same time, the event spurred an ongoing sensitive criminal investigation, and many stakeholders did not need to know certain details of the case based on their roles and the laws and policies governing the sharing of investigative data.[1]

INFORMATION SHARING CHALLENGES

During the investigation, information sharing among APD and other agencies relied almost exclusively on manual processes such as email, phone calls, and in-person briefings. This made disseminating information slow and repetitive. In addition, the investigative response lacked a common platform to manage the flow of information and the assignment of tasks across participating agencies. Law enforcement personnel, who came to the Austin area from all over the United States to assist, did not have a centrally managed application or service through which to receive key information and briefings on the basics of the case. Rather than collaborating through a shared system or an interconnected (federated) collection of systems, each agency used its own "siloed" systems, applications, and databases during the investigation. This sometimes resulted in duplicated effort and wasted time, as participating teams could not easily distinguish when an investigative task had been completed, and could not quickly obtain new information as it was generated.

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

The information sharing challenges during the 2018 Austin bombing response highlight the potential benefits of integrated, interoperable platforms and applications for sharing information and assigning tasks among participating agencies. These benefits could include faster and more efficient apprehension of perpetrators, fewer casualties to civilians and first responders, and lower costs to the participating agencies. However, implementing and federating systems to facilitate more seamless investigative information sharing is a major challenge. Perhaps the biggest implementation barrier facing agencies is ensuring that approved external personnel with a verified "need to know" are provided the ability to quickly and easily authenticate internal systems and applications, while also respecting the laws, regulations, and other policy rules that define what data those users are permitted to access.

The process of vetting external personnel and onboarding them into local data-sharing systems is time consuming, expensive, and fraught with security and compliance risks, especially when local agency resources are already strained. A more promising approach is to leverage a technique known as

[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).

Federated Identity, Credential, and Access Management (ICAM). Under a Federated ICAM approach, external personnel can log into agencies' information-sharing systems and applications using their existing authentication credentials issued by their home agencies, and access to sensitive investigative data can be managed through trusted attributes provided by users' home agencies.

AUSTIN BOMBING RESPONSE VALUE PROPOSITION

- Information sharing transparency
- Information sharing will replace inefficient manual processes
- Minimize "siloed" systems, applications, and databases during the investigation
- Provide a common platform to manage the flow of information

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

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