Identity, Credential, and Access Management

Wireless Mobility in Law Enforcement, Justice, and Public Safety

National Strategy Summit

October 8–9, 2014 • Washington, DC

Recommended Principles and Actions Report

January 2015

Table of Contents

Acknowledgements

In the explosion of technology supporting public mobility and ubiquitous connectivity, law enforcement, justice, and public safety agencies have been left behind: great difficulty still exists in making the connection to the last mile . . . the police officer, deputy sheriff, firefighter, and paramedic in a vehicle or in the field. These professionals—our colleagues—need immediate access to critical information from the wide variety of systems technology available (particularly portable computers, tablets, and smartphones) to make the best possible decisions and protect themselves and the public. Hand in hand with access challenges is the imperative to ensure robust internal controls on security, including factoring in today's "Bring Your Own Device" (BYOD) environment.

Resolution of these access and security issues has been a long-standing challenge and high-priority need. With support from the Program Manager for the Information Sharing Environment, the U.S. Department of Homeland Security, and the International Association of Chiefs of Police, a planning committee was formed to advance the nation's wireless mobility capabilities through a collaborative event.

In early October 2014, we convened justice and public safety leaders and communications subject-matter experts from across the associated communities at the National Strategy Summit ("Summit") on Identity, Credential, and Access Management (ICAM)—Developing a National Strategy for Wireless Mobility in Law Enforcement, Justice, and Public Safety. Each invitee was chosen not only to represent a specific organization, sector, or constituency, but also based on his or her individual skillset and professional background, with an eye toward carefully balancing viewpoints and equities at the Summit table. (See *Appendix C* for the Summit roster.)

As Planning Committee cochairs, we want to express our sincere appreciation to members of this impressive team for their efforts throughout the Summit process: from digesting the preparatory materials; to vigorous on-site engagement and exchanges of viewpoints and experiences; to thoughtfully revising and significantly strengthening this document. The following *Recommended Principles and Actions Report* is a direct reflection of the participants' willingness to capitalize on the Summit opportunity, partnering, and contributing a wide range of expertise toward a common goal and greater good.

We also want to thank the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Department of Justice, for hosting the Summit in Washington, DC.

Fundamental to the October discussions was the understanding that successful development of and cross-disciplinary support for a national ICAM approach is essential to widespread adoption of wireless mobility in the law enforcement, fire service, emergency medical service, and justice communities, and is ultimately fundamental to the safety of our colleagues and communities. We believe the Summit results and recommendations are a significant next step towards these goals.

ICAM Summit Planning Committee Cochairs

Mr. Kshemendra Paul, Program Manager for the Information Sharing Environment

Mr. Daniel Cotter, Director, Office for Interoperability and Compatibility, U.S. Department of Homeland Security

Chief Harlin R. McEwen, Chairman, Communications and Technology Committee, International Association of Chiefs of Police

Background

The First Responder Network Authority (FirstNet) is an independent authority within the National Telecommunications and Information Administration, established by Public Law 112-96 on February 22, 2012. FirstNet is charged with implementing a single Nationwide Public Safety Broadband Network (NPSBN), a wireless broadband data-sharing network primarily for public safety personnel. The FirstNet NPSBN will be different from current commercial wireless networks, as it is dedicated to public safety.

With the implementation of the FirstNet NPSBN comes an opportunity for law enforcement and public safety entities to take advantage of a more reliable network. With this opportunity comes the challenge of protecting the integrity and security of the network and the privacy and confidentiality of the data that is accessed. This network will enable public safety agencies nationwide to exchange information across jurisdictional and disciplinary boundaries, from virtually any location, using a wide variety of mobile devices. Achieving this mission will require FirstNet to develop strategies, standards, and conventions in many areas, in order to ensure interoperability, security, and efficient operation of the network.

One such area addresses the registration, verification, authentication, and authorization of a public safety official or other approved individual to have proper access to the NPSBN, both initially and on an ongoing basis as officials' roles, agency associations, levels of training and certification, and employment status change over time. This area of concern is commonly called Identity, Credential, and Access Management (ICAM).

On October 8-9, 2014, 60 public safety and ICAM subject matter experts[1] convened at the Bureau of Alcohol, Tobacco, Firearms and Explosives headquarters in Washington, DC for the ICAM National Strategy Summit.[2] The objective of the Summit was to gain a consensus around principles and actions that will inform a strategy for identifying and managing authorized users of the FirstNet NPSBN.

While the Summit focused primarily on an ICAM strategy for FirstNet, there was recognition that the principles underlying this strategy—and, in fact, the strategy itself—should be leveraged by other initiatives needing to secure access to resources by understanding the identity and characteristics of the users needing to access those resources. [3]

The Summit was co-sponsored by the Program Manager, Information Sharing Environment (PM-ISE), the Department of Homeland Security, Science & Technology Directorate, and the International Association of Chiefs of Police (IACP). Both FirstNet and PM-ISE have a

[1] Please see Appendix C for the ICAM National Strategy Summit attendee roster.
[2] Please see Appendices B and D for the ICAM National Strategy Summit overview document and agenda, respectively.
[3] Please see Appendix E for the range of uses cases provided to attendees in advance of the meeting, establishing a context for on-site Summit discussions.

shared lineage, being born out of the 9/11 Commission Report, and a shared mission of facilitating responsible information sharing. Many of the activities described in the White House's 2012 *National Strategy for Information Sharing and Safeguarding* (NSISS), which also traces its origin to the 9/11 Commission Report, apply to these responsible information sharing efforts and provide a useful framework for developing these recommendations.

Summit participants were acutely aware of the nature of FirstNet as a network, not as a provider of services that may be made available over the network, yet recognized the potential of FirstNet being a new national network upon which identity management could be constructed in such a way as to provide a model for existing or other networks that may serve the public safety needs for information sharing and safeguarding. Summit participants also recognized the cross-cutting and broad-based nature of the conversation – that there are existing mature identity, credential, and access management trust frameworks and standards that FirstNet should leverage.

During the Summit, FirstNet staff gave a presentation about its requirements and identified foreseen ICAM challenges that the group should take into consideration. Participants then heard from several ongoing ICAM programs to understand lessons-learned, proven practices, and potential areas of reuse from these initiatives. These program presentations[4] included the National Strategy for Trusted Identities in Cyberspace (NSTIC); Federal Identity, Credential, and Access Management (FICAM); State Identity, Credential, and Access Management (SICAM); Personal Identity Verification-Interoperability (PIV-I); First Responder Authentication Credential (FRAC); the Trustmark Initiative; National Identity Exchange Federation (NIEF) and Global Federated Identity and Privilege Management (GFIPM).

Document Purpose

This document recommends principles and actions for developing an ICAM strategy that will focus on registering, verifying and authorizing network users. While this strategy focuses on FirstNet, the principles and actions are relevant to any initiative that needs to identify and authorize users for access to secure resources. The recommendations presented here are based in many ways on the priority objectives of the National Strategy for Information Sharing and Safeguarding, and represent those principles that must guide any collection of public safety information technology serving national needs.

The recommended principles and actions are the result of much discussion, consideration and, ultimately, consensus of the ICAM National Strategy Summit participants.

[4] For additional information on the program presentations, please see Appendix F for associated briefing sheets.

Recommended Principles

I. Federated ICAM Strategy

Many potential FirstNet users are already part of an identity and credential management initiative, in which an authority has verified their identity and issued a credential that provides access to a set of protected resources. For most users, credential issuance occurs at the local agency as part of employment and in order to provide access to information technology systems and resources, such as records management, dispatch, and email. In addition, the Regional Information Sharing Systems (RISS) and the Federal Bureau of Investigation (FBI) have historically vetted the identity of and issued credentials to users of their law enforcement services.

A *federated ICAM strategy* for FirstNet would leverage these existing identity and credential management investments, where FirstNet would recognize the existing credentials to be used to authorize access to FirstNet and resources on the network for a significant segment of the user community. In a federated ICAM strategy, FirstNet would focus on its core mission—providing a reliable and interoperable nationwide wireless network—and delegate to (and trust) identity and credential providers for the identification and authentication of users. Federated ICAM also reduces cost and duplication by enabling **shared services**.

The strategy would encompass[5]:

- Identity proofing of network users—the process of verifying a user's identity
- Attribute provisioning—including in the identity information about the user necessary to determine access to the network and resources, such as job role/duties, level of training or certification, type of agency, etc.
- Credentialing—the process of issuing a secure representation of the user's identity.
- Attribute Exchange and Verification Service-the process of transmitting user's entitlements, authorizations, and other attributes and/or verifying user's attributes while preserving the user's privacy.[6]

A federated ICAM strategy rests on a foundation of trust—specifically, that FirstNet is able to rely on the identity proofing, attribute provisioning, and credentialing and authentication conducted by others. Accomplishing this will require the adherence of credential providers to credentialing policies and standards that FirstNet adopts. Many of the other principles and actions described in the remainder of this document are intended to guide the establishment of these policies and standards, so that in the end a federated ICAM approach is both achievable and effective.

---

[5] Please see Appendices A and G for a terminology list and *Introduction to ICAM Principles* brochure, respectively, providing definitions and an overview of key ICAM terms used in this document.

[6] The Backend Attribute Exchange SAML 2.0 profile was accepted by FICAM for government-wide adoption. An XACML-based verification profile pilot is under development providing an attribute verification service without the disclosure of attributes.

One important lesson learned from the presentations at the Summit was that ICAM efforts in both state governments and the federal government are converging on consistent, interoperable trust frameworks, (defined in Appendix A) through the FICAM and SICAM efforts, and within the scope of the NSTIC. This convergence will undoubtedly assist in the development of policies and standards for credentialing of FirstNet users.

Examples of Federated ICAM that FirstNet can look to for lessons learned are the National Interoperability Exchange Federation (NIEF) and the initiative implemented under the Information Sharing and Access Interagency Policy Committee (ISA IPC). This initiative consists of four core Sensitive But Unclassified (SBU) networks: DHS's HSIN, FBI's LEEP/LEO, DoJ's grant-funded and State-owned RISSNet, and the Intelligence Community's Intelink. This initiative implements a "No Wrong Door" strategy and, includes Federal, State, and Local partners, and spans the Criminal Justice, Homeland Security, and Intelligence mission areas.

II. Modularization and Layering of Policies

A federated ICAM strategy for FirstNet, in which FirstNet leverages existing identity proofing and credentialing processes, implies that the credentials used to authenticate users for access to FirstNet will also be used for other purposes. For example, a law enforcement officer may gain access to FirstNet through use of his/her existing RISS credential, or a firefighter or paramedic may gain access to FirstNet through use of his/her agency's internal credentialing process; however, these officials will also use these same credentials for other purposes, such as access to RISS applications or local records systems.

It is likely that these existing credentials will have unique properties with regard to security, privacy, interoperability, attributes, trust, etc. since they will have been issued under disparate and pre-exiting trust frameworks and business requirements.

FirstNet will need to specify (adopt) a baseline set of policies, standards, operating procedures, aka a trust framework, which defines its ICAM requirements.

The reusability of credentials will be most successful if the policies and standards governing their issuance and maintenance are *modular*. If policies and requirements are stated as sets of self-contained "components" or "modules", then FirstNet stakeholder communities—and the credential providers that support them—will be able to "mix and match" to satisfy their unique requirements, as well as satisfy the FirstNet requirements that they all share by virtue of participation in FirstNet.

This will leave identity providers and credential issuers the latitude to implement whatever additional credential features their stakeholder communities and markets may desire.

Modularization of policies will also support a *layered* approach, in which the same credential can support basic access to FirstNet, as well as more specific (and generally more stringent) access to applications, services, and data on the network.

On the first day of the Summit, participants heard from the NSTIC Trustmark Pilot initiative, which is developing the notion of "trustmarks" to support this kind of modular, layered approach to ICAM. Trustmarks can provide standardized, and in many cases machine-readable, representations of policy modules that can be certified by any certification authority.

III. Favor Decentralized Credentialing with Delegation

During presentations of existing ICAM initiatives, Summit participants heard about the decentralized and delegated approach to credential management that several organizations have implemented at the national and state levels. Specifically, the National Crime Information Center (NCIC) system maintains physical connections and originating agency identifiers to federal and state designated criminal justice agencies; however, the process of issuance and maintenance of user credentials is delegated to officials in state and local law enforcement agencies. The FBI's National Data Exchange (N-DEx) program maintains a user credential directory but also delegates the process of issuance and maintenance of user credentials to state and local law enforcement agencies. The Regional Information Sharing Systems (RISS) manage user credentials across the nation in much the same way. Similarly, participants heard from the Texas Department of Public Safety (DPS), which manages thousands of user credentials statewide via a similar approach.

These initiatives have demonstrated that there are technology efficiencies to providing identity as a service at the state or even national level, but still maintaining local control over the issuance and maintenance of credentials. This local control is important, because it is at the local level that changes in users' circumstances and characteristics, which impact the issuance and revocation of credentials, are known best, and thus can be reflected accurately and in a timely fashion. The initiatives have also developed auditing processes to ensure that the delegated issuance and maintenance of user credentials adheres to applicable policies and standards.

These initiatives have also demonstrated, through their participation in the National Identity Exchange Federation (NIEF) as a trusted framework, that the credentials they issue can be federated, and thus reused for controlling access to a wide range of protected resources. Thus users credentialed by one NIEF partner can use their credentials to access their own agency's resources, as well as resources offered by other NIEF parties at the state, regional, or national level. Because of a well-defined, transparent, and trusted set of federation policies, practices, and interoperability profiles allowing local agencies to issue and manage credentials locally, resource providers gain a level of comfort in trusting the accuracy of the credential, as well as the security offered by the federation trust framework.

This decentralized, delegated approach to credential management can benefit FirstNet in two ways. FirstNet should consider leveraging these existing credential providers as part of its ICAM strategy. In addition, FirstNet should consider a decentralized, delegated approach for management of credentials in segments of the FirstNet stakeholder community outside of law enforcement. In particular, such an approach may address the needs of smaller agencies that lack the resources to provision a credential management solution. Such agencies may be able to participate in existing initiatives, such as RISS, or there may be a need to establish a new credentialing process for them; identifying these strategies will be an important role for the FirstNet governance process.

IV. Importance of Standards

A federated ICAM strategy for FirstNet, in which FirstNet encourages decentralization and delegation of credentialing, will require a certain level of consistency in order allow for affordable interoperability. Standards will enable this consistency while encouraging competition, market choice, and innovation. Standards do not necessarily have to be a product of a formal standards development organization, but could instead be the result of an ICAM stakeholder community consensus or community-accepted practices for addressing specific problems.

FirstNet is likely to require standards in a number of areas in order to ensure proper access control across the network, regardless of the agency issuing a user's credential. Technical interoperability standards (or profiling an existing set of standards) will ensure that credentials are represented and asserted in a uniform manner. Similarly, FirstNet will need to adopt a standard way of asserting specific details or attributes about users that will inform access control decisions, such as name, agency, employment position, and certifications.

FirstNet will need to identify baseline security standards to confirm that details made available about users are not accessible to untrusted sources nor can they be manipulated. FirstNet will also need to adopt a standard approach for representing FirstNet policies and confirming an agency's conformance to those policies.

Adopting **interoperable standards**, both in the realm of user identity and credential information as well as of **data tagging**, is critical to enabling ICAM. A robust, interoperable ICAM solution will allow users to **discover and gain access** to information automatically, reducing both the time required and the associated costs to manually adjudicate every access request.

A number of ICAM-related standards currently exist in the commercial identity ecosystem, some of which were presented at the Summit. It is strongly suggested that FirstNet examine these existing standards and consider adopting one or more before developing new standards. The Summit heard from one such example, the Global Federated Identity and Privilege Management (GFIPM) initiative.

V. Leverage What Exists

It's very likely that existing ICAM initiatives have faced several of the decisions and implementation considerations that FirstNet will encounter. A federated ICAM strategy for FirstNet should take advantage of applicable successes achieved by other ICAM initiatives. On the first day of the Summit, participants heard from the following ICAM initiatives that likely offer valuable reuse opportunities to FirstNet.

The Federal Identity, Credential, and Access Management (FICAM) initiative has established a trust framework and trust framework providers which support multiple levels of identity assurance (LOA) as way to measure the strength of the organization's identity proofing process, as well the strength of the issued credential to withstand common types of attacks. These levels of assurance are intended to enable confidence in both the identity claimed by the credential as well in the credential itself, especially in federated ICAM environments, like that proposed for FirstNet. The State Identity, Credential, and Access Management (SICAM) initiative introduces the benefits of FICAM at the State level.

The use of technologies and capabilities that are aligned with FICAM and the LOA-construct will greatly improve interoperability with Federal services that are made available via FirstNet. For instance, if the Federal Emergency Management Agency (FEMA) makes a service available on FirstNet, the ability to access that service may be dependent on the user having a FICAM-approved credential. This does not mandate the "use" of FICAM; it simply notes that a FICAM-approved capability may provide the users of FirstNet with additional capabilities.

The Trustmark initiative, one of several pilot efforts sponsored by the National Strategy for Trusted Identities in Cyberspace (NSTIC) office, is very likely to support the modular and layered policy approach to ICAM recommended as a principle earlier in this report. Trustmarks will provide standardized, and in many cases machine-readable, representations of policy modules that can be certified by any certification authority.

The National Identity Exchange Federation (NIEF) is a componentized trustmark-based trust framework with a partnership of Federal, State and Local agencies that trust one another for the purpose of exchanging secure credentials to gain access to secure resources. The NIEF framework has policies and procedures for important ICAM aspects including security, identity proofing, auditing, privacy, attributes, certificates, and legal agreements that are aligned and conformant with FICAM and GFIPM standards for enabling technical trust and interoperability. Under a DHS Science and Technology grant, NIEF is deploying a capability that will enable Personal Identity Verification-Interoperability (PIV-I) credential use with trusted resources such as RISS.

PIV-I cards are identification cards issued by select non-Federal agencies as the result of an identity proofing process that meets federal guidelines for verifying the identity

of individuals. These cards are designed to be easily authenticated, both visually and electronically. The First Responder Authentication Credential (FRAC) is a PIV-I solution that enables interoperability between local, state, and federal levels. Even if PIV-I or FRAC cards don't play a direct role in the FirstNet ICAM strategy, it is likely that policies or processes that result in issuance of these cards could be of use to FirstNet in establishing its ICAM strategy.

In the spirit of leveraging what exists, the federated ICAM strategy for FirstNet should encourage reuse of existing credentialing processes. It's likely that many potential FirstNet users are already part of an identity and credential management initiative, in which an authority has verified their identity and issued a credential that provides access to a set of protected resources. The strategy should allow agencies to follow current credentialing processes for enabling user access to the network. A user should then be able to provide credentials once to access the network and should not be required to provide credentials again to access resources on the network (unless, of course, the user remains inactive for some period of time or if other policies exist that would force re-authentication).

VI. Implementation Feasibility

A federated ICAM strategy for FirstNet should establish a vision and direction that is within the technical, financial and governance means of the FirstNet program.

Many of the other principles identified at the Summit will help to achieve implementation feasibility. A federated strategy, in and of itself, removes a major potential implementation burden from FirstNet, by leveraging credentialing processes and infrastructure that already exist. Adopting open standards and aligning with ongoing ICAM efforts at the Federal and state levels will reduce (if not eliminate) "one off" or FirstNet-specific technologies and strategies that require large investments to design and implement. Standards, too, improve vendor-neutrality and increase market choice and implementation options.

Still, in adhering to the principles outlined here, the FirstNet community should keep implementation feasibility in mind. As FirstNet designs and implements the device issuance process—to include user identification and vetting through existing credentialing processes—it will be important to consider the impact on the inherently limited resources of both the FirstNet staff and customer agencies.

The strategy should encourage use of commercially available devices rather than require FirstNet specific technologies or solutions. Not only will this help keep the initial implementation costs low, but it will minimize ongoing maintenance and troubleshooting costs for the FirstNet program as users will be able to resort to device vendors for troubleshooting device issues.

VII. Ease of Use for Practitioners

A federated ICAM strategy for FirstNet should not raise undue barriers between authorized users and access to the network when they need it. The strategy should take into consideration real world requirements and likely scenarios where users will require access to the network. For instance, individuals will often access the network in high-stress situations with difficult environmental conditions, such as protective clothing or other equipment. The FirstNet strategy will need to focus on achieving access control without making it unduly difficult for users to gain access, especially in these types of situations.

In adopting an overall ICAM strategy, FirstNet should identify credentialing requirements that result in the necessary level of security and credential trust, but do so in a manner that allows for greatest flexibility and ease of use for users. A federated strategy supports this notion, by allowing credential providers to satisfy FirstNet's stated requirements, but compete on efficiency and cost, with users being incentivized to obtain their credentials from the most cost-effective providers.

VIII. Affordability and Sustainability

A federated ICAM strategy for FirstNet should not introduce requirements that lead to unreasonable expenses for FirstNet users and should encourage reuse of existing investments wherever possible. A FirstNet strategy should allow for use of commercially-available devices that include FirstNet public safety spectrum band 14, offered by a number of vendors, for accessing the network. The choice of an ICAM approach for FirstNet should support the widest range of possible devices and technologies.

The strategy should consider the expense of rigorous credentialing requirements and should allow for multiple levels of credential assurance. This will empower agencies to determine what level of credentialing they will invest in, understanding that achieving higher-levels of assurance is likely more expensive but will result in a credential with a high level of confidence.

Encouraging market competition will be important in keeping ICAM-related costs down and will give users options in choosing which devices to use on the network. To do this, the strategy should require use of open standards for implementing ICAM as opposed to a vendor-specific or a proprietary approach to ICAM. This will also assist with future-proofing the FirstNet ICAM strategy. A strategy that is focused on use of open standards is much more likely to adapt to future technologies and requirements than a strategy that is tied to a specific technology or vendor solution.

The federated ICAM strategy for FirstNet should also support the overall FirstNet plan for sustainability.

IX. Scalability and Agility

Summit participants recognized that the FirstNet user community, as well as the capabilities available on the network and the kinds of devices supported, will continue to grow after the initial implementation. Along with this growth will be an ongoing evolution of the public safety business environment in which FirstNet will operate, and therefore a continual change in the requirements placed on the network.

This reality will compel FirstNet to keep scalability and agility (planning for change) in mind in all aspects of network design, including planning for ICAM. As FirstNet plans for and implements a strategy for an initial community of users and resource providers, it will be important for that strategy to evolve as new applications, use cases, and user communities join the network in the future.

The other principles identified during the Summit, and outlined here, will support scalability and agility. For instance, a modular and layered policy approach will allow the addition of new policy layers in the future, to accommodate new requirements, without disrupting the support for existing resources and users. A federated ICAM approach naturally supports scalability and agility by separating the provisioning of resources and applications from the credentialing of users, thus allowing new user communities to join in an incremental fashion over time.

X. Importance of Governance

Successful implementation of the principles identified at the Summit, and outlined in this report, will result in some specific responsibilities for the FirstNet governance structure.

Of perhaps the greatest initial importance, FirstNet will need to identify the specific policy requirements for network access and—in alignment with these principles—express those policy requirements as modules and layers. Since these policies will define the levels of assurance required by credentials used to access the network, FirstNet will need to identify processes and mechanisms for vetting credential providers in order to verify conformance with the policies.

The FirstNet governance process will also need to adopt standards for credentials, including the means of representing user characteristics, and definitions of those characteristics. The governance process will need to identify potential technical standards, vet those against requirements, and then establish the necessary standards to ensure technical interoperability in the transmission and exchange of credentials where necessary. The existing ICAM initiatives that presented at the Summit can provide a wealth of assistance and input on these issues, but it will ultimately be up to FirstNet to establish its own standards, while ensuring that ongoing Federal and state ICAM initiatives have already paved a path here, and for FirstNet to be interoperable with existing approaches, coordination and leveraging of what already exists will be important.

Summit participants stressed that stakeholder community involvement and engagement in establishing policies and standards for FirstNet will be essential. This is especially true for FirstNet's ICAM strategy. The FirstNet governance structure is well-positioned to provide stakeholder community engagement in development and implementation of the ICAM approach.

Recommended Actions and Next Steps

I. Adopt Principles and Factor into Implementation

FirstNet should formally adopt the recommended principles specified in the previous section of this document and appropriately factor these into the upcoming FirstNet request-for-proposal (RFP).

II. Determine Role of ICAM Summit Participants

FirstNet should determine what role the ICAM summit participants will play in the future of FirstNet and its ICAM strategy and how to fund continued participation if FirstNet deems necessary their continued participation.

III. Develop a Roadmap

FirstNet should develop and publish a roadmap that consists of projected timelines and milestones for rolling out the ICAM strategy. The purpose of this roadmap should be to give the FirstNet audience a sense of how the ICAM approach will affect them and will give a sense of when users need to be prepared to react.

This roadmap should be developed with Summit participants or with other avenues to include appropriate stakeholder input, and should firmly anchor within the larger federated Identity, Credential, and Access Management Ecosystem.

IV. Articulate FirstNet Access Requirements

FirstNet should clearly define and document the requirements for gaining authority to utilize the FirstNet network. These requirements should describe exactly who should be authorized to access the network and what information must be made available about each authorized user to determine the levels of access and priority. FirstNet should move to formalize conformance with these requirements in the form of interoperable componentization represented by policy modules; FirstNet should prefer these representations to be machine-readable where possible.

V. Test Candidate Solutions

Until the FirstNet network is operational, FirstNet should test and confirm candidate ICAM solutions in existing ICAM environments. FirstNet has established an Early Builder Working Group consisting of five entities (Texas, Adams County, Colorado, New Mexico, New Jersey and Los Angeles RICS) that will be establishing ICAM initiatives in furtherance of their activity with a FirstNet early builder spectrum

agreement; however, FirstNet should explore all options. This approach will allow FirstNet to make progress in implementing components of the ICAM strategy before the network is fully operational.

VI. Federal Service Providers to Modularize their Security Policies

Federal service provider partners, such as FBI CJIS, should modularize and componentize their security policies (using a technology such as Trustmarks). (The FBI CJIS Security policy is owned by the community of criminal justice users and is vetted by that community's representation through the FBI CJIS Advisory Policy Board [APB] process.) This will allow the FirstNet federated identity providers to map their policies as shown in the earlier sections and identify any differences or gaps that would prevent users from securely gaining the access they require.

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix A

Terminology

Appendix A—Terminology

The following are definitions of key ICAM terms used throughout the document.

Attribute	A quality or characteristic inherent in or ascribed to someone or something
Identity	The set of **attributes** that describe an individual in a given context
Credential	Authoritative evidence of an individual's claimed **identity**
Trust Framework	A trust framework is developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific process and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. Different trust frameworks can exist within the Identity Ecosystem, and sets of participants can tailor trust frameworks to meet their particular needs. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline standards established by the Identity Ecosystem Framework.

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix B

National Strategy Summit:
Identity, Credential, and Access Management (ICAM)—
Developing a National Strategy for Wireless Mobility in Law Enforcement, Justice, and Public Safety

Revised 09/07/14

National Strategy Summit

Identity, Credential, and Access Management (ICAM)—
Developing a National Strategy for
Wireless Mobility in Law Enforcement, Justice, and Public Safety

Washington, DC—October 8–9, 2014

PURPOSE

- Development of a comprehensive strategy for a national standardized approach to identity, credential, and access management (ICAM) is critical to the success of widespread adoption of wireless mobility in the law enforcement, fire service, emergency medical service, and justice communities.

- Development of a clear and widely supported definition of requirements that are acceptable to local, tribal, state, and federal entities; a reasoned and evolutionary road map to identity management that balances existing technologies and capabilities with a long-term road map of functionality; solutions acceptable to law enforcement, fire service, emergency medical service, justice entities, legislative bodies, and data repository operators, including the FBI; and a strategic plan for resolving the issues remaining, as well as agreement on the steps toward implementation.

NATIONWIDE OPPORTUNITY

In the explosion of technology supporting the general mobility of the public for ubiquitous connectivity, law enforcement, justice, and public safety agencies have been left behind. In spite of the successes in improving information sharing, great difficulty still exists in making the connection to the last mile—primarily the officer, deputy sheriff, firefighter, and paramedic in a vehicle or in the field. These men and women need immediate access to the information that will enable them to make better decisions and protect themselves and the public. Today, they need access to information from the wide variety of systems technology available, particularly portable computers, tablets, and smartphones.

Law enforcement, justice, and public safety agencies struggle with the challenge of utilizing mobile access while ensuring robust internal controls on security, satisfying data repository operator rules (such as FBI CJIS) for accessibility, and managing threats to network security.

Law enforcement agencies are increasingly looking to mobile technologies to enhance the efficiency and effectiveness of officers in the field, but few national standards or best practices presently exist to foster and support secure, enterprisewide access for law enforcement, justice and public safety. The rapidly expanding adoption of smartphones,

tablets, and other mobile devices makes it necessary for law enforcement, justice, and public safety agencies to develop and implement policies to enable personnel to easily access appropriate critical information, even when utilizing their own mobile devices, commonly referred to as "bring your own device" (BYOD).

To add additional complexity to the issue, the First Responder Network Authority (FirstNet), an independent authority within the National Telecommunications and Information Administration, established by Public Law 112-96 on February 22, 2012, is working toward development and implementation of a single Nationwide Public Safety Broadband Network (NPSBN), a wireless broadband data sharing network for first responders. The network will be a welcome addition and will permit the development of creative new solutions, but without standards of practice and functional interoperability beyond the equipment level, the optimal result will not be realized. In the years necessary to implement the FirstNet NPSBN, there will be enormous value and opportunity if we can "unlock" data in a secure and standard way. A cohesive national strategy is needed for implementation of information sharing across jurisdictional boundaries using mobile devices. For a nationwide cross-domain network such as the NPSBN, a federated identity and credentialing approach is likely the most practical, since it will improve security and user convenience while avoiding the expense and governance issues that come with a national, centralized credential directory.

Today, a number of identity, credential and access management programs are in use, but no nationwide identity management approach or strategy has been universally accepted or implemented by all local, tribal, state, and federal entities that provides a pathway for members of public safety agencies to have trusted access to critical information at either their desktops or on mobile devices. Law enforcement, justice, and public safety entities need access to this information on a regular basis from mobile devices, and the methods to access information need to be low-cost, simple, and standardized. A comprehensive national strategy for the widespread adoption of mobility in law enforcement, justice, and public safety is needed now. Such a strategy would include the development of a clear and widely supported definition of requirements; a reasoned set of solutions that are acceptable to legislative bodies and data repository operators, including the FBI; and a strategic plan for resolving the issues remaining, as well as agreement on the steps toward implementation.

The solution needs to provide information sharing interoperability among all participating local, tribal, state, and federal users of the NPSBN.

National Strategy Summit

The starting point with all such projects where national consensus is required is to develop a strategy to achieve such consensus. A group of approximately 50 subject-matter experts will meet to learn about existing ICAM programs and develop a strategy for moving forward. The group will include representatives from major justice and public safety organizations and representatives from key nonprofit organizations engaged in information sharing.

The group, composed of people who are knowledgeable about this issue, will be tasked with developing next steps to solving the problem. The group will take into account the benefits that could be derived by embracing programs such as the National Strategy for Trusted Identities in Cyberspace (NSTIC); Federal Identity, Credential, and Access Management (FICAM); State Identity, Credential, and Access Management (SICAM); Personal Identity Certification-Interoperability (PIV-I); First Responder Authentication Credential (FRAC); the Trustmark Initiative; National Identity Exchange Federation (NIEF), Global Federated Identity and Privilege Management (GFIPM); and the National Information Exchange Model (NIEM).

The objective of the Summit is to gain a consensus strategy that will result in identifying and managing authorized users of the FirstNet Nationwide Public Safety Broadband (wireless) Network (NPSBN). To reach this objective, participants will consider possible solutions and lessons learned by current Identity, Credential, and Access Management (ICAM) programs.

The NPSBN being planned by FirstNet will be different from current commercial wireless networks, and access will be restricted to authorized users only. With the implementation of the FirstNet NPSBN comes an opportunity for law enforcement and public safety entities to take advantage of a more reliable network while protecting the integrity and security of the network.

A process must be in place to register, verify identity, and authorize a public safety representative or other approved individual to have access as a user of the network. There is also a need for a process for ongoing management of users to determine their continuing eligibility to be authorized users of the network.

It is envisioned that, at a minimum, potential NPSBN users will be required to complete a FirstNet application process. This process will result in the verification and establishment of a user **identity** and the issuance of a **credential** to **access** the network. Identity also may be verified by membership in another FirstNet trusted system such as FBI LEEP or RISS.

The Summit will focus on various options currently being used by established ICAM programs and will develop recommendations for consideration by FirstNet.

The focus of the Summit is not to develop a process to authorize devices to be operated on the network or to gain access to applications or services using the network. It is recognized that mobile devices (smartphones, mobile terminals, and laptops) will need to be authorized by FirstNet and that devices using the network will need to be registered, issued, or owned by an authorized network user. These issues will be addressed in other forums.

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix C

Attendee Roster

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Summit Participants

Mr. Ali Afrashteh
Chief Technology Officer
First Responder Network Authority (FirstNet)
Washington, DC
Representing: FirstNet

Mr. Steven Ambrosini
Executive Director
IJIS Institute
Ashburn, VA
Representing: IJIS Institute

Mr. Glenn Archer III
Deputy Director
National Fusion Center Association
Representing:
National Fusion Center Association

Mr. Jeff Bratcher
Deputy Chief Technology Officer
First Responder Network Authority (FirstNet)
Washington, DC
Representing: FirstNet

Mr. Scott Came
Executive Director
SEARCH, The National Consortium for
Justice Information and Statistics
Sacramento, CA
Representing: SEARCH,
The National Consortium for
Justice Information and Statistics

Ms. Maria Cardiellos
Program Manager
New Jersey Information Sharing Environment
Newark, NJ
Representing:
New Jersey Identity Management Program

Thomas Clarke, Ph.D.
Vice President
Research and Technology
National Center for State Courts
Williamsburg, VA
Representing:
National Center for State Courts

Ms. Cynthia Cole
Chief Executive Officer
Cynergyze Consulting, Inc.
Chicago, IL
Representing:
Interconnectivity Infrastructure Group

Mr. Daniel Cotter
Director
Information Applications Division
Science and Technology Directorate
U.S. Department of Homeland Security
Washington, DC
Representing:
Science and Technology Directorate,
U.S. Department of Homeland Security

Mr. Todd Early
Deputy Assistant Director
Law Enforcement Support Division and Statewide Communications Interoperability Coordinator
Public Safety Communications Service
Texas Department of Public Safety
Austin, TX 78752
Representing: Law Enforcement Support Division and Statewide Communications Interoperability, Texas Department of Public Safety

Commander Scott Edson
Los Angeles County Sheriff's Department
Immediate Past Chair, Law Enforcement Information Management Section
International Association of Chiefs of Police
Los Angeles, CA
Representing: Law Enforcement Information Management Section, International Association of Chiefs of Police

Ms. Deborah Gallagher
Director
Identity Management
U.S. General Services Administration
Washington, DC
Representing: Federal Identity, Credentialing, and Access Management

Mr. Jeremy Grant
Senior Executive Advisor
National Strategy for Trusted Identities in Cyberspace
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, DC
Representing: National Strategy for Trusted Identities in Cyberspace

Mr. Paul Grassi
Senior Standards and Technology Advisor
National Strategy for Trusted Identities in Cyberspace
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, DC
Representing: National Strategy for Trusted Identities in Cyberspace

Mr. Michael Haas
Senior Law Enforcement Advisor and Special Assistant
Office of the Chief Information Officer
U.S. Department of Justice
Washington, DC
Representing: Office of the Chief Information Officer, U.S. Department of Justice

Admiral Ronald Hewitt (Retired)
Director
Office of Emergency Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC
Representing: National Protection and Programs Directorate, U.S. Department of Homeland Security

Ms. Karyn Higa-Smith
Research and Development Program Manager
Homeland Security Advanced Research Projects Agency
Cyber Security Division
Science and Technology Directorate
U.S. Department of Homeland Security
Washington, DC
Representing: Personal Identity Verification—Interoperability/ First Responder Authentication Credential

Mr. Ashwini Jarral
Director of Operations
IJIS Institute
Ashburn, VA
Representing: IJIS Institute

Mr. Michael Lesko
Deputy Assistant Director
Crime Records
Texas Department of Public Safety
Austin, TX
Representing: Federal Bureau of Investigation– Criminal Justice Information Services Division Advisory Policy Board Identification Services Subcommittee

Ms. Marsha MacBride
Senior Counsel to the Assistant Secretary
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC
Representing: National Telecommunications and Information Administration

Chief William McCammon (Retired)
Executive Director, East Bay Regional Communications System Authority
Vice Chair, FirstNet Public Safety Advisory Committee
Dublin, CA
Representing: Fire Service

Mr. Thomas McCarty
Director
Identity, Credential, and Access Management Program Management Office
Office of the Chief Information Officer
U.S. Department of Homeland Security
Representing:
Office of the Chief Information Officer, U.S. Department of Homeland Security

Mr. Matthew McDonald
National Coordinator
Regional Information Sharing Systems
Philadelphia, PA
Representing:
Regional Information Sharing Systems

Chief Harlin McEwen (Retired)
Chair, Communications and Technology Committee
International Association of Chiefs of Police
Chair, FirstNet Public Safety Advisory Committee
Ithaca, NY
Representing:
FirstNet Public Safety Advisory Committee

The Honorable Michael Milstead
Sheriff
Minnehaha County Sheriff's Office
Sioux Falls, SD
Representing:
National Sheriffs' Association

Mr. Maury Mitchell
Director, Alabama Criminal Justice Information Center
Chair, CONNECT Consortium Board
Montgomery, AL
Representing: CONNECT Consortium

Mr. Tom Moran
Executive Director
All Hazards Consortium
Frederick, MD
Representing: All Hazards Consortium

Mr. Kshemendra Paul
Program Manager
Office of the Program Manager, Information Sharing Environment
Office of the Director of National Intelligence
Washington, DC
Representing:
Office of the Program Manager, Information Sharing Environment

Mr. Bill Phillips
Information Security Officer
Nlets—The International Justice and Public Safety Network
Phoenix, AZ
Representing: Nlets—The International Justice and Public Safety Network

Mr. Chris Pickering
Homeland Security Coordinator
State of Missouri
Jefferson City, MO
Representing: National Governors Association

Mr. David Roberts
Senior Program Manager
Technology Center
International Association of Chiefs of Police
Alexandria, VA
Representing: Technology Center, International Association of Chiefs of Police

Mr. Douglas Robinson
Executive Director
National Association of
State Chief Information Officers
Lexington, KY
Representing:
National Association of
State Chief Information Officers

Mr. John Ruegg
Director
Information Systems Advisory Body at
Los Angeles County
Chair, Global Federated Identity and
Privilege Management Delivery Task Team
Los Angeles, CA
Representing: Global Federated Identity and
Privilege Management Delivery Task Team

Admiral David Simpson (Retired)
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC
Representing:
Federal Communications Commission

Mr. Tom Sorley
Deputy Director, City of Houston
Vice Chair, FirstNet Public Safety Advisory
Committee
Houston, TX
Representing: U.S. Conference of Mayors

Mr. R. Scott Trent
Designated Federal Officer
Criminal Justice Information Services Division
Federal Bureau of Investigation
Clarksburg, WV
Representing: Federal Bureau of
Investigation–Criminal Justice Information
Services Division

Mr. John Wandelt
Research Fellow and Division Chief
Information Exchange and Architecture Division
Georgia Tech Research Institute
Executive Director, National Identity Exchange
Federation
Atlanta, GA
Representing: National Identity Exchange
Federation

Mr. Joseph Wassel
Director
Public Safety Communications
Office of the Secretary of Defense
U.S. Department of Defense
Washington, DC
Representing: U.S. Department of Defense

Chief Charles Werner
Fire Department Chief, City of Charlottesville
Chair, National Information Sharing Consortium
Charlottesville, VA
Representing:
National Information Sharing Consortium

Mr. Carl Wicklund
Executive Director
American Probation and Parole Association
Lexington, KY
Representing:
American Probation and Parole Association

Mr. Craig Wilson
Deputy Director, Operations Division
Officer-in-Charge, MW Continuity Readiness
Center
National Continuity Programs
Federal Emergency Management Agency
U.S. Department of Homeland Security
Washington, DC
Representing: Personal Identity
Verification—Interoperability/
First Responder Authentication Credential

Mr. Paul Wormeli
Executive Director Emeritus
IJIS Institute
Ashburn, VA
Representing: IJIS Institute

ATF ICAM Summit Hosts

Director B. Todd Jones
Bureau of Alcohol, Tobacco, Firearms
and Explosives
U.S. Department of Justice
Washington, DC

Mr. James Burch, II
Assistant Director
Public and Governmental Affairs
Bureau of Alcohol, Tobacco, Firearms
and Explosives
U.S. Department of Justice
Washington, DC

Observers

Mr. Doug Babics, PMP
Acting Program Manager
Identity Management Services
Office of the Chief Information Officer
U.S. Department of Justice
Washington, DC

Mr. Randy Bachman
Cybersecurity Engineer
Cybersecurity and Communications Reliability
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC

Mr. Mark Golaszewski
Senior Manager, Applications
Consultant to FirstNet
FirstNet Technical Headquarters
Boulder, CO

Mr. Michael Howell
Deputy Program Manager
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National Intelligence
Washington, DC

Mr. Brian Hurley
Attorney Advisor
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC

Mr. Kent Kettell
Lead Engineer
Enterprise Services Division
Information Technology Services Office
Office of the Chief Information Officer
U.S. Department of Homeland Security
Washington, DC

Mr. Gabriel Martinez
Senior Electronics and Computer Engineer
Architecture and Advanced Technologies
Office of Emergency Communications
U.S. Department of Homeland Security
Washington, DC

Mr. Vincent Sritapan
Chief Information Security Officer
Science and Technology Directorate
U.S. Department of Homeland Security
Washington, DC

Staff

Mr. Josh Freedman
Director
National Security Staff Engineering
Office of Information and Technology
U.S. Customs and Border Protection
U.S. Department of Homeland Security
Washington, DC

Mr. Rick Gregory
Institute for Intergovernmental Research (IIR)
Tallahassee, FL

Ms. Donna Lindquist
Institute for Intergovernmental Research
Washington, DC

Mr. Andrew Owen
Director
Information Sharing Programs
SEARCH, The National Consortium for Justice
Information and Statistics
Sacramento, CA

Ms. Terri Pate
Institute for Intergovernmental Research
Tallahassee, FL

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix D

Agenda

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Agenda—Page One

October 8, 2014

8:30 a.m. **Day 1—Summit Convenes**

8:30 a.m. – 9:00 a.m. **Welcome and Introductory Remarks**

Welcome to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Headquarters
Mr. B. Todd Jones, Director, ATF

Introductory Remarks
Mr. Kshemendra Paul, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence

Chief Harlin McEwen (Retired), Chairman, Communications and Technology Committee, International Association of Chiefs of Police

Mr. Daniel Cotter, Director, Office for Interoperability and Compatibility, Science and Technology (S&T) Directorate, U.S. Department of Homeland Security (DHS)

9:00 a.m. – 9:15 a.m. **Goal of the Summit**
Mr. Scott Came, Executive Director, SEARCH—The National Consortium for Justice Information and Statistics

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Agenda—Page Two

9:15 a.m. – 9:45 a.m.	**Briefing: First Responder Network Authority (FirstNet)— Nationwide Public Safety Broadband Network** *Mr. Ali Afrashteh, Chief Technology Officer (CTO) FirstNet* CTO Afrashteh will brief attendees on this new challenge and opportunity for Identity and Access Management (IdAM) efforts.
9:45 a.m. – 10:15 a.m.	**Briefing: National Strategy for Trusted Identities in Cyberspace (NSTIC)—National Perspective** *Mr. Jeremy Grant, Senior Executive Advisor for Identity Management, National Institute of Standards and Technology*
10:15 a.m. – 10:30 a.m.	***Break (on your own)***
10:30 a.m. – 11:00 a.m.	**Briefing: Federal Identity, Credential, and Access Management (FICAM)— Federal Perspective** *Ms. Deborah Gallagher, Director, Identity Assurance and Trusted Access Division, General Services Administration*
11:00 a.m. – 11:30 a.m.	**Briefing: Personal Identity Verification-Interoperable (PIV-I)— First Responder Authentication Credential (FRAC) Perspective** *Mr. Craig Wilson, Senior Consultant and Program Manager, Federal Emergency Management Agency, DHS* *Ms. Karyn Higa-Smith, Research and Development Program Manager, S&T Directorate, DHS*
11:30 a.m. – 12:00 Noon	**Briefing: State Identity and Credential Access Management (SICAM)—State Chief Information Officers' Perspective** *Mr. Douglas Robinson, Executive Director, National Association of State Chief Information Officers*

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Agenda—Page Three

12:00 Noon – 1:15 p.m.	***Lunch (on your own)***
1:15 p.m. – 2:00 p.m.	**Briefings: Trustmark Initiative and the National Identity Exchange Federation (NIEF)** *Mr. John Wandelt, Division Chief, Georgia Tech Research Institute and NIEF Director*
2:00 p.m. – 2:30 p.m.	**Facilitated Discussion: Short-Term and Long-Term ICAM Strategies** *Mr. Came, Facilitator*
2:30 a.m. – 2:45 a.m.	***Break (on your own)***
2:45 p.m. – 5:00 p.m.	**Facilitated Discussion *(continued)*: Short-Term and Long-Term ICAM Strategies** *Mr. Came, Facilitator*
5:00 p.m.	**Day 1—Evening Recess**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Agenda—Page Four

October 9, 2014

8:30 a.m.	**Day 2—Summit Reconvenes**
8:30 a.m. – 8:45 a.m.	**Facilitated Discussion: Review of Day 1 Discussions, Setting the Stage for Day 2** *Mr. Came, Facilitator*
8:45 a.m. – 10:00 a.m.	***Facilitated Discussion (continued from previous day): Short-Term and Long-Term ICAM Strategies*** *Mr. Came, Facilitator*
10:00 a.m. – 10:15 a.m.	***Break (on your own)***
10:15 a.m. – 11:15 a.m.	**Facilitated Discussion: Agreement on Next Steps and Way Ahead** *Mr. Came, Facilitator*
11:15 a.m. – 11:30 a.m.	**Closing Remarks** *Program Manager Paul* *Chief McEwen*
11:30 a.m.	**Summit Adjournment**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix E

Use Cases

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Use Case 1

FirstNet Scenario: **A series of homicides in Baltimore are linked with a series in Newark, New Jersey, and a Newark police officer is sent to Baltimore to collaborate. The two detectives responding to the scene of a homicide check in using their FirstNet credentials, logging their presence, and notifying supervisors. They then use their FirstNet mobile devices to access photos from their respective previous cases' digital case files directly from the scene. The Baltimore detective is able to grant the visiting Newark detective access to her case files to facilitate collaboration, with FirstNet automatically enforcing access control policies such as 28 CFR Part 23 training.**

Before FirstNet, law enforcement personnel often had to return to their offices or use vehicle-based mobile data terminals to access case information. This prevented them from leveraging case information while looking at the scene of a crime and often introduced significant delays. By enabling an officer to leverage the NPSBN, a FirstNet mobile device brings this information out of the office and out of the vehicle.

Role of ICAM: **A robust FirstNet ICAM implementation allows the police department's digital case file system to ensure that only authorized individuals have access to case file information.**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Use Case 2

FirstNet Scenario: **A Basic Life Support (BLS) unit and paramedic Smith are dispatched to the scene of a possible drug overdose. During initial assessment of the nonresponsive patient, a pill container with several pills in it is found nearby. Using his FirstNet mobile device, the responder sends a digital photograph of the pill and container, along with the patient's status and other relevant information, directly to the hospital's emergency department (ED) computer system. The ED system notifies the paramedic that the patient has an identified renal impairment, resulting in different instructions for treatment during transport to the hospital.**

Before FirstNet, the responder would have had to read the label on the pill container to the county 9-1-1 dispatcher, who would then relay it to the hospital. By allowing the responder to simply send a digital photograph directly to the hospital, FirstNet enables the responder to focus more time and attention on the patient. Because the responder can directly receive treatment instructions from the hospital using the patient's medical records, the responder can provide appropriate treatment.

Role of ICAM: **Access to a patient's health information is strictly controlled under HIPAA. FirstNet's ICAM solution enables the hospital's medical records system not only to know who is requesting access to the patient's medical records, but to retrieve attributes about the requestor (in this case, that he is a trained, certified paramedic) as well as about the context of the request (in this case, that the paramedic is providing emergency care to the patient). FirstNet's ICAM solution allows all of this information to be quickly and automatically retrieved.**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Use Case 3

FirstNet Scenario: **A routine burglary alarm is received at 10:30 p.m. at the Chester County, Pennsylvania, 9-1-1 center from Stewart's, a local jewelry store. With the massive growth of privately owned Internet-accessible security cameras, the Chester County, Pennsylvania, Emergency Services Department has entered into a voluntary agreement with Stewart's to allow county 9-1-1 center staff secure access to remotely view their video cameras in the event of an alarm. The county staff member connects to Stewart's video system, authenticating use of the store's trusted FirstNet credential, and provides valuable real-time intelligence to the responding units.**

Role of ICAM: **A private business such as Stewart's would want to ensure that only authorized users can view the video feed from their security camera systems. Simply using a username and a password would not provide the level of accountability required, and the password would make an excellent target for a would-be criminal. The FirstNet credential is significantly stronger than a simple username and password, providing for greater accountability (in that each is assigned to a specific 9-1-1 center staff member, rather than a shared group password) and greater security (in that the FirstNet credential is more than a single "something you know").**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Use Case 4

FirstNet Scenario: **A tourist bus with 50 passengers is involved in a severe accident on Interstate 95 in rural Virginia. Local first-response capacity is overwhelmed, and the county 9-1-1 operator requests assistance from surrounding counties. Arriving paramedics from non-local facilities use their FirstNet mobile devices to gain access to local hospital emergency departments, allowing them to transmit vital patient information to the hospitals even though they do not have a routine association with those facilities (that is, they are not "anticipated" precredentialed users at those hospitals).**

Role of ICAM: **The FirstNet credential allows a hospital to securely accept information from a non-local first responder, despite the lack of a preestablished relationship. The hospital is able, first, to authenticate the responder, ensuring that the responder is who he or she claims to be (as vouched for by FirstNet) and second, to retrieve the appropriate attributes about the responder (that he or she is a trained and certified paramedic), all automatically and electronically.**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

Use Case 5

FirstNet Scenario: **In the aftermath of a large hurricane landfall in Florida, an incident commander (IC) authorizes the deployment of a FirstNet National Public Safety Broadband Network (NPSBN) compatible unmanned aerial vehicle (UAV) supplied by FEMA to survey the damage, identify the hardest-hit areas, and allocate rescue resources accordingly. The video from the same UAV is used by the Florida Highway Patrol (FHP), serving as interagency dispatchers as a result of the disaster, to route responders around blocked/destroyed roads. The FirstNet-compatible credentials held by the IC and the FHP dispatchers grant each access to the FEMA UAV, allowing both types of users to view the video but allowing only the IC to control the vehicle.**

Before FirstNet, UAV information downlink required expensive microwave, line-of-sight, or satellite downlink equipment, significantly limiting the number and diversity of users. A UAV integrated with the FirstNet NPSBN significantly reduces the cost and complexity of utilizing UAVs, allowing considerably more users to view the UAV's video, and possibly command the UAV, with their handheld FirstNet devices.

When an UAV is allowed to communicate with commodity devices rather than with expensive and specialized equipment, the risk of unauthorized individuals either eavesdropping on the video or hijacking control of the UAV increases. Further, more responders may be authorized to view the video than are authorized to control the UAV.

Role of ICAM: **A robust FirstNet ICAM implementation allows appropriate credentials issued by the FHP to be trusted and accepted by the FEMA UAV system, eliminating the need for responders to obtain separate credentials for each agency or system they work with. Additionally, the FirstNet ICAM implementation allows the FEMA UAV system to make access control decisions for any FirstNet identity, regardless of which entity issued its credential, based on standards and trust.**

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix F

Briefing Sheets

Identity, Credential, and Access Management (ICAM)

Wireless Mobility in Law Enforcement, Justice, and Public Safety

National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8-9, 2014

- **Program Name:** **Federal Identity Credential and Access Management (FICAM)**

- **Program Description and Business Case**
  - **Program description and maturity: FICAM is a compilation of the architecture (both "as is" and "to be") use cases and best practices for the identity, credential, and access management initiative for the federal government. The complete name is the *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance* (December 2011).**

  - **Who manages the program? Explain program governance. The Identity, Credential, and Access Management Subcommittee (ICAMSC) chartered under the Information Security and Identity Management Committee (ISIMC) of the Federal CIO Council manages the program. It is governed by the Federal CIO Council.**

  - **Relationship to other ICAM programs? FICAM provides the desired state and the implementation guidance for ICAM activities. There are specific milestones and activities identified with the responsible organization.**

  - **How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety?" The FICAM is a living document that addresses identity management concerns for the beginning agency as well as emerging needs of the federal government. As wireless and mobile technology uses become more prevalent, the FICAM will evolve to address those needs.**

- **Planned next steps, increasing adoption and implementation, and future activities. The next version of the FICAM is being reviewed now with the intent to add mobile, new NIST guidelines/standards and needs of ICAM in the federal space.**

- **Program Users**
  - **Constituency served–Federal Executive Branch Agencies**
  - **Current state of implementation–Varied**
  - **Program scope and stakeholders–Federal, Commercial, State, Local, and Tribal**

- **Online Program Resources**
  http://www.Identitymanagement.gov

- **Program Point(s) of Contact**
  Deb Gallagher
  Deborah.Gallagher@gsa.gov
  Director, Identity Assurance and Trusted Access Division
  Office of Governmentwide Policy
  GSA
  (202) 219-1627

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

- **Program Name:** First Responder Network Authority (FirstNet)

- **Program Description and Business Case**
  - Program description and maturity
    - The Middle Class Tax Relief and Job Creation Act of 2012 created FirstNet as an independent authority within the Department of Commerce, National Telecommunications and Information Administration (NTIA), to provide emergency responders with the first nationwide public safety broadband network. The FirstNet Board was appointed in August 2012, the Public Safet Advisory Committee (PSAC) was established in February 2013, and hiring of staff and stakeholder outreach began in early 2013. The main headquarters offices and technical headquarters office were established in 2014 in Reston, Virginia, and Boulder, Colorado. Initial state consultation meetings commenced in July 2014.

  - Who manages the program? Explain program governance.
    - The General Manager runs FirstNet's daily operations. In addition, there is a 15-member board. Representatives include the Secretary of Homeland Security, the Attorney General of the United States, and the Director of the Office of Management and Budget as permanent members. The remaining members are selected by the Secretary of Commerce and have public safety, technical, network, and/or financial expertise. FirstNet also leverages its PSAC, a 40-member committee representing all disciplines of public safety as well as state, territorial, tribal, and local governments that provide advice on matters involving shared intergovernmental responsibilities or administration.

  - Relationship to other ICAM programs?
    - ICAM will be a critical component in the design and implementation of the FirstNet network. The FirstNet network's relationship to other ICAM programs is still to be determined.

  - How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety?"
    - FirstNet will provide priority and preemption to ensure that public safety always has access to the broadband network during emergency and nonemergency periods. The integration of real-time data and applications

into emergency response will improve incident management effectiveness and the safety of citizens and public safety personnel.

- Planned next steps, increasing adoption and implementation, and future activities
  - FirstNet just released a Request for Information for Comprehensive Network Solutions, which incorporates a draft Statement of Objectives to seek input from interested parties regarding approaches to, and objectives for, establishing a nationwide interoperable public safety broadband network. FirstNet intends to release a draft Comprehensive Network Request for Proposal by early 2015. On September 24, 2014, a public notice will be released in the Federal Register to request comments on certain preliminary interpretations of FirstNet's enabling legislation. Both the RFI and public notice have a 30-day comment period.

- **Program Users**
  - Constituency served: All federal, state, local, and tribal public safety personnel.
  - Current state of implementation: Ongoing outreach to public safety and federal, state, local, and tribal stakeholders; conducting initial state consultation meetings; developing a comprehensive network acquisition strategy.
  - Program scope and stakeholders: Development of a nationwide public safety broadband network for federal, state, local, and tribal public safety stakeholders.

- **Online Program Resources**

  Web Site: http://www.firstnet.gov
  Twitter: @FirstNetGov
  YouTube: https://www.youtube.com/user/FirstNetGov
  Flickr: https://www.flickr.com/photos/firstnetgov

- **Program Point(s) of Contact**

  Ali Afrashteh
  Chief Technical Officer
  FirstNet
  Telephone: (202) 422-2420
  E-Mail: ali.afrashteh@firstnet.gov

  Jeff Bratcher
  Deputy Chief Technical Officer
  FirstNet
  Telephone: (202) 740-3491
  E-Mail: jeff.bratcher@firstnet.gov

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

- **Program Name: Global Federated Identity and Privilege Management (GFIPM)**

- **Program Description and Business Case**

The Global Federated Identity and Privilege Management (GFIPM) initiative was developed through a collaborative effort of the Global Justice Information Sharing Initiative (Global) membership, the U.S. Department of Justice's Bureau of Justice Assistance (BJA), and the U.S. Department of Homeland Security (DHS). This document provides an executive overview of the GFIPM concept. It also discusses the GFIPM value proposition and provides additional resources for those interested in learning more.

Background and the Business Case for GFIPM

Ensuring that the right people, and only the right people, have access to the right information is a daunting task for the justice community, for several reasons.

1. Justice information users are represented at all levels of government and are provisioned in many systems. Because of fragmented funding for justice and public safety systems, local, state, tribal, and federal government agencies have invested (and reinvested) in security solutions that are largely noninteroperable and that fail to take into account the changing needs of the justice community.

2. Traditionally, the end user in the justice information exchange transaction has had to manage different credentials, passwords, tokens, and secondary factors on a system-by-system basis. This administrative effort—which includes juggling the access requests and expirations for different system credentials and passwords—limits the time that law enforcement officers and others have available to prevent and solve crimes and engage in other substantive work.

3. There is no single data source for justice users. The creation of a central user store is impractical, not cost-effective, and difficult to maintain because of high personnel turnover in the justice arena and the distributed nature of justice and public safety systems. Also, many legacy justice systems require the use of private networks, which are often costly and burdened with administrative

processes and lag time. In turn, justice users are burdened with additional overhead for obtaining access to disparate systems.

To help solve these problems and enable cost-effective, cross-jurisdiction information sharing within the justice community, the Global Justice Information Sharing Initiative has developed the GFIPM suite of products.

The conceptual foundation of the GFIPM project is the idea of secure, interoperable, cost-effective Federated Identity and Privilege Management (FIPM). FIPM is an extension of the more common concept of federated identity management, which allows for the separation of user identities from the systems and applications in which those identities are used. Within an identity federation, identity provider (IDPs) manage user identities and service providers (SPs) manage applications and other resources. Federated identity management provides valuable benefits for information sharing, including greater usability because of identity reuse, as well as improved privacy and security. The FIPM concept seeks to extend traditional federated identity management by addressing the issue of authorization—or privilege management—within systems and applications in a federated environment. Each system or application in an identity federation typically has its own set of business requirements and access control policies. FIPM provides a cost-effective framework that allows these systems to be made available to federated users while still respecting their native requirements.

The GFIPM concept has been designed and implemented based on a well-grounded understanding of the needs of real-world law enforcement information sharing systems. GFIPM development began with a bottom-up analysis of the usage and access requirements of several prototypical information sharing systems at the state, local, and tribal law enforcement levels. The process also included extensive community involvement and feedback, similar to the process used in the development of the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM). The end result is that GFIPM not only meets the needs of a large class of its target systems (state and local law enforcement information sharing applications), but also has achieved a broad level of acceptance within its target community.

The GFIPM concept recognizes and seeks to facilitate interoperability and scalability at all critical levels of an identity federation, including governance, policy and business rules, technology standards, implementation and onboarding of participants, and ongoing operations such as change management and user support. At the governance level, GFIPM is consensus-based, with all participating agencies represented in an identity federation governance structure. The core governance philosophy is to provide enough structure to enable the establishment of basic trust agreements and memoranda of understanding between participants, but also to respect the desire of participating agencies to remain autonomous and retain full control over their information resources. At the levels of policy and technology standards, GFIPM specifies a small set of well-defined requirements to provide a baseline for identity interoperability while still giving participants a high degree of latitude in terms of local policy and implementation. In addition to the basic

interoperability requirements, GFIPM provides documentation, tools, and other facilities to encourage rapid, low-cost, and independent participant onboarding in parallel with each other. GFIPM includes very little centralized infrastructure and has no mandatory centralized services within the critical path of information sharing transactions, so there is no single point of failure or bottleneck in the federation from a technical standpoint. This philosophy also carries over into the area of day-to-day operations management, since GFIPM seeks to reuse and leverage existing operations and user support infrastructure as much as possible. In every dimension, GFIPM's goal is to facilitate an interoperable identity solution that maximizes scalability by minimizing centralization and embracing the distributed, disparate nature of a federation.

By using GFIPM technology, organizations can realize two major benefits. First, they can provide more data to their existing user bases. Second, they can make their existing data more widely available to users in other organizations. GFIPM provides the requisite technology and policy infrastructure to permit these information sharing transactions to occur in a manner that is secure and also compliant with laws and other policy-level requirements.

In addition to benefitting organizations, GFIPM can provide valuable benefits to end users in the form of reduced complexity, increased convenience, and increased privacy when they access data sources. These benefits to users are the result of GFIPM single sign-on (SSO) technology, plus a well-defined taxonomy of information attributes about users. Their use results in fewer security forms to fill out, fewer passwords and other security credentials to manage, and tighter control over the personal information about users that is often required by data providers.

- **Program Users**

  - Constituency served; Program scope and stakeholders (local, tribal, state, federal?) GFIPM work products are used within multiple identity federations, by agencies at the federal, state, and local levels. This section contains a partial list of communities that leverage GFIPM.

    1. **National Identity Exchange Federation**
       The National Identity Exchange Federation (NIEF) is a collection of agencies in the United States that have come together to share sensitive law enforcement information. NIEF was created in 2008 as a direct outgrowth of the GFIPM program and maintains a close, symbiotic relationship with GFIPM, as it leverages existing GFIPM work products and also serves as a source of real-world feedback to drive the development of new GFIPM work products. Additional information about NIEF is available at https://nief.gfipm.net/ or by contacting Mr. John Wandelt, NIEF Executive Director, at john.wandelt@gtri.gatech.edu.

    2. **FBI CJIS Law Enforcement Enterprise Portal (LEEP)**
       LEEP is a federated identity management system developed by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS)

Division. The goal of LEEP is to provide access to resources beneficial to the law enforcement, intelligence, and emergency management communities via its Federation Portal page. LEEP was built based on GFIPM technical specifications but uses a "trusted broker" model rather than a fully distributed federation model. LEEP is connected to NIEF as both an identity provider and a service provider. For more information about LEEP, please contact the FBI CJIS Division's Law Enforcement Online Operations Unit at leoportal@leo.gov.

3. **CONNECT Consortium**
   The CONNECT Consortium is a group of U.S. states dedicated to working closely together to better solve specific information sharing challenges facin the criminal justice community. CONNECT provides a meaningful way for members to work together, pool limited resources, coordinate the creation and deployment of standards-based information sharing tools, and promote the sharing of information across jurisdictional borders to better solve and prevent crimes in their home communities. Additional information about the CONNECT Consortium is available at http://www.connectconsortium.org/ or by contacting Mr. Maury Mitchell, CONNECT Consortium Director, at maury.mitchell@alacop.gov.

- Current state of implementation
  After nearly ten years of development, the GFIPM concept has matured into a full suite of solutions, from interagency governance and policy guidance to technical specifications and sample implementations.

- **Online Program Resources**

To learn more about the GFIPM program, please see the following resources.

OJP GFIPM Portal—http://it.ojp.gov/gfipm
Operated by the U.S. Department of Justice (DOJ) Office of Justice Programming (OJP), the OJP GFIPM Portal contains basic background information about the GFIPM program, as well as all formal publications (technical specifications, nonnormative policy guidance, and white papers) developed through the GFIPM program.

GFIPM.net—http://gfipm.net/
GFIPM.net provides additional information about the GFIPM program and GFIPM concept.

GFIPM Implementation Portal—https://impl.gfipm.net/
The GFIPM Implementation Portal contains a GFIPM Implementer Wiki with community-contributed articles about implementing information sharing solutions based on GFIPM standards. It also hosts a GFIPM Implementer Mailing List.
GFIPM Reference Federation—http://ref.gfipm.net/

Operated by the Georgia Tech Research Institute (GTRI), the GFIPM Reference Federation is a collection of online systems that serve as an interoperability test bed for the GFIPM implementer community.

- **Program Point(s) of Contact**

Mr. John Ruegg
Los Angeles County Information Systems Advisory Body
jruegg@isab.lacounty.gov

Mr. James Dyche
Pennsylvania Justice Network
jdyche@state.pa.us

Mr. John Wandelt
GTRI GFIPM
Project Director
John.wandelt@gtri.gatech.edu

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

- **Program Name:** National Association of State Chief Information Officers (NASCIO) State Identity Credential and Access Management (SICAM) Guidance and Roadmap

- **Program Description and Business Case**

  - **Program description and maturity:**

    - The NASCIO SICAM Guidance and Roadmap provides goals and architectural direction for a statewide (enterprise) identity management framework. SICAM was developed by the NASCIO State Digital Identity Working Group. The group was initially chartered in 2010 and is composed of both NASCIO state government and corporate members. SICAM version 1 was released in 2012.
    - NASCIO issued a call to action as a follow-up to release of SICAM v1 to enable states to pursue an enterprise-wide approach to digital identity management.

  - **Purpose of the working group:**

    - The State Digital Identity Work Group will provide a consensus-based forum that enables State Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Enterprise Architects, and line-of-business stakeholders to collaborate on developing recommendations on federated identity management initiatives. This working group intends to provide a framework for the key guidelines for program management and collaboration. The charter seeks to develop solutions for a sustainable and supportable model for use in identity, credentialing, and access efforts.

- **Goals and objectives:**

  - Promote the use of an enterprise architecture governance structure.
  - Distinguish appropriate capabilities for identifying, authenticating, and authorizing individuals with appropriate access to resources.
  - Enable trust and interoperability.
  - Improve security and privacy.
  - Facilitate e-government use by facilitating secure access to services and transactions.
  - Increase efficiencies and reduce costs.
  - Facilitate efficiency and security of commercial transactions.
  - Seek to find ways to expand convenience of services while improving security and privacy.
  - Investigate the short- and long-term sustainability of a state digital identity program.

- **Who manages the program?**

  - NASCIO manages the program and the State Digital Identity Working Group.

- **Relationship to other ICAM programs?**

  - Endorses the FICAM roadmap and the PIV-I/FRAC TTWG and draws heavily on other national standards, federal guidance, and the digital identity management architecture work of the states.

- **How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety"?**

  - Goals and architectural approach are in support of FICAM, GFIPM, and the concepts of an identity ecosystem.
  - Goals support the concept of interoperability across government lines of business.
  - The scope of SICAM is an all-encompassing approach regardless of end-user devices.
    - *. . . smartphones, tablets, laptops, and the numerous other devices that now connect us to resources , including ever increasing services and products which previously required in-person presence . . .*

- **Planned next steps, increasing adoption and implementation, and future activities:**

  - The State NASCIO Digital Identity Working Group meets monthly via conference call and has been rechartered through October 31, 2014.
  - Primary future activity is to develop a SICAM version 2 guidance document that includes additional considerations state governments must address, including:

- Strategies for promoting enterprise IAM adoption.
- Concept of trustmarks.
- Other elements to be identified and vetted by the NASCIO State Digital Identity Working Group.

- **Program Users**

  - Constituency served: Primary target is state CIOs and state government entities.
  - Current state of implementation: SICAM v1.
  - Program scope and stakeholders: local, tribal, state, federal?

    - State Chief Information Officers (CIO), state Chief Information Security Officers (CISO), state Enterprise Architects (EA), and other state ICAM implementers at all stages of program planning, design, and implementation; however, the roadmap also may be used as a resource for systems integrators, end users, other entities, and commercial business partners seeking interoperability or compatibility through state programs.

- **Online Program Resources**

  - NASCIO State Digital Identity Working Group page: http://www.nascio.org/committees/digitalID/
  - The State Identity Credential and Access Management Guidance and Roadmap (SICAM), September 2012 http://www.nascio.org/publications/documents/SICAM.pdf
  - NASCIO Call-to-Action: The Necessity for Maturing Identity and Access Management in State Government, November 2012 http://www.nascio.org/publications/documents/NASCIO-Call-to-Action-The-Necessity-for-Maturing-Identity-and-Access-Management-in-State-Government.pdf

- **Program Point(s) of Contact**

Eric Sweden, MSIH MBA
Program Director, Enterprise Architecture and Governance
National Association of State Chief Information Officers (NASCIO)
201 East Main Street, Suite 1405, Lexington, KY 40507 USA
(859) 514-9189 | esweden@nascio.org | www.nascio.org

Identity, Credential, and Access Management (ICAM)

Wireless Mobility in Law Enforcement, Justice, and Public Safety

National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8-9, 2014

- **Program Name: National Identity Exchange Federation (NIEF)**

- **Program Description and Business Case**
  - **Program description and maturity:**
    NIEF is a collection of law enforcement agencies and other organizations in the United States that have come together to share sensitive law enforcement information. NIEF has developed a federated identity trust framework that supports the secure exchange of user identities and attributes in support of secure information exchange between agencies.

    Federation is a fundamental concept in NIEF. The federation provides an agreed-upon framework for allowing agencies to directly provide services for trusted users whom they do not directly manage. NIEF benefits include:

    - **User convenience**
    - **Interoperability**
    - **Cost-effectiveness**
    - **Privacy**
    - **Security**
    - **Scalability**
    - **Compliance**
    - **Technical assistance**
    - **Strategic roadmap**
    - **Trusted framework**

  - **Who manages the program? Explain program governance.**
    Created in 2008 as a direct outgrowth of the Global Federated Identity and Privilege Management (GFIPM) program, the NIEF Center was established by the Georgia Tech Applied Research Corporation, a tax-exempt entity under Section 501(c)(3) of the Internal Revenue Code, and a supporting organization of the Georgia Institute of Technology under Section 509(a)(3)

of the Code. NIEF still maintains a close symbiotic relationship with the GFIPM program by leveraging GFIPM work products and also serving as a source of real-world feedback to drive the development of new GFIPM work products.

- **Relationship to other ICAM programs; How NIEF fits into an overall strategy for "wireless mobility in law enforcement, justice, and public safety"; Planned next steps, increasing adoption and implementation, and future activities.**

  In addition to full alignment with GFIPM, NIEF is fully committed to participation and alignment with many broader nationwide identity initiatives, including the following:

  1. **Federal Identity, Credentialing, and Access Management (FICAM)—NIEF is aligning with FICAM by seeking adoption as a FICAM Trust Framework Provider (TFP), which will enable NIEF to certify its Identity Provider Organizations (IDPOs) for technical and policy-level interoperability with federal government services offered through the FICAM program and the Federal Cloud Credential Exchange (FCCX).**

  2. **State Identity, Credentialing, and Access Management (SICAM)—NIEF is working closely with the National Association for State Chief Information Officers (NASCIO) to help develop a vision for cost-effective and scalable implementation of the SICAM initiative that NASCIO originally introduced in its 2012 SICAM Guidance and Roadmap white paper (see http://www.nascio.org/publications/documents/SICAM.pdf).**

  3. **Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) High-Assurance Identities—NIEF is working with the Department of Homeland Security Science and Technology Directorate (DHS S&T) and the Johns Hopkins University Applied Physics Lab (JHUAPL) to pilot a gateway that will enable all PIV and PIV-I cardholders to gain logical access to NIEF resources, subject to applicable access controls.**

  4. **The Backend Attribute Exchange (BAE) Suite of Standards—In conjunction with its work with DHS S&T and JHUAPL, NIEF has developed a standard profile of the BAE Query-Response Profile and prototyped an implementation of the profile to enable Attribute Provider Organizations (APOs) to offer supplementary attributes to other NIEF member organizations.**

  5. **The National Strategy for Trusted Identities in Cyberspace (NSTIC)—In an effort to help develop cost-effective and scalable solutions to the "interfederation" trust and interoperability problem that exists**

throughout the federated identity community today, NIEF and its membership are participating in the Georgia Tech Research Institute (GTRI) NSTIC Trustmark Pilot Project, funded by the NSTIC program through the National Institute of Standards and Technology (NIST).

These programs are collectively shaping the national identity and trust ecosystem. By aligning with them and participating actively in them, NIEF is positioning itself as a premier national operational federation for enabling wide-scale trusted information exchange among agencies at the state, local, tribal, and territorial (SLTT) levels, as well as information exchange between SLTT agencies and federal agencies. Also, since many SLTT agencies and implementers do not have the resources to track how these broad-based programs could impact them, participation in NIEF enables them to leverage their resources to ensure that their efforts align with new technologies, frameworks, and strategies that may arise at the national level.

- **Program Users**
  - **Constituency served; Current state of implementation; Program scope and stakeholders (local, tribal, state, federal?).**

    While the GFIPM suite of products was originally developed for the U.S. justice and law enforcement community, NIEF's use of GFIPM products is agnostic to the business information being shared among its participants, which makes NIEF ideal for adoption among most or all government agencies. NIEF lowers the barriers to entry and cost of adoption for wide-scale information sharing among agencies at the federal, state, local, territorial, and tribal levels, as well as their information sharing business partners.

    The following organizations are currently members of NIEF:

    1. **Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division**
    2. **Regional Information Sharing Systems (RISS)**
    3. **U.S. Department of Homeland Security Information Network (HSIN)**
    4. **Criminal Information Sharing Alliance (CISA)**
    5. **Pennsylvania Justice Network (JNET)**
    6. **Los Angeles County Sheriff's Department (LASD)**
    7. **Institute for Intergovernmental Research (IIR)**
    8. **Tennessee Bureau of Investigation (TBI) and Tennessee Methamphetamine and Pharmaceutical Task Force (TMPTF)**
    9. **Tennessee Integrated Criminal Justice Program (ICJP)**
    10. **Texas Department of Public Safety (TX DPS)**

- **Online Program Resources**

  To learn more, please see the NIEF Web site at https://nief.gfipm.net/.

- **Program Point(s) of Contact**

Mr. John Wandelt
Research Fellow and Division Chief
Information Exchange and Architecture Division
Georgia Tech Research Institute
Executive Director, National Identity Exchange Federation
Atlanta, GA
Phone: (404) 386-1264
E-Mail: John.Wandelt@gtri.gatech.edu

Identity, Credential, and Access Management (ICAM)

Wireless Mobility in Law Enforcement, Justice, and Public Safety

National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8-9, 2014

- **Program Name:** National Strategy for Trusted Identities in Cyberspace (NSTIC)

- **Program Description and Business Case**
  - *Program description and maturity:* NSTIC was the first new cybersecurity program launched by the Obama Administration. Released in in April 2011, NSTIC calls for the private sector to partner with government to spur creation of an Identity Ecosystem, where all Americans can choose from a variety of different identity solutions that they can use for online experiences that are more secure, convenient, and privacy-enhancing than the password-based systems that dominate today.

  - *Who manages the program? Explain program governance:*
    - The White House directed the National Institute of Standards and Technology (NIST) to establish a National Program Office (NPO) to lead implementation of NSTIC.
    - Separate from the NPO, a privately led Identity Ecosystem Steering Group (IDESG) has been established to help coordinate development of an Identity Ecosystem Framework of standards, policies, and business rules that can enable the NSTIC vision to take hold in the marketplace.

  - *Relationship to other ICAM programs?*
    - NSTIC is unique among ICAM programs in that its primary focus is not government but, rather, the private sector. NSTIC is looking to spur creation of a new set of identity solutions that consumers and businesses can use to improve trust online.

- **That said, the President calls for the U.S. government to be an early adopter of the Identity Ecosystem. As part of this effort, we work closely with many agencies, as well as the GSA FICAM program – FICAM today runs the Trust Framework Solutions program, which accredits private-sector credential provider for government use, and agency use of these credentials is key to the early success of NSTIC.**

- ***How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety?"*** **NSTIC does not focus much on law enforcement and public safety applications; however, the solutions developed to support NSTIC should ideally be able to help law enforcement and public safety programs more easily accomplish their missions–since it will spur creation of a wider array of COTS identity solutions.**

- **Planned next steps, increasing adoption and implementation, and future activities.**
  - **Build off the success of 15 NSTIC pilots**
  - **Develop v.1 of an Identity Ecosystem Framework by early 2015**
  - **Ensure U.S. government as an early adopter this fall through launch of the Connect.gov initiative, which will enable all agencies to easily leverage a growing array of FICAM-approved credentials for U.S. government use.**

- **Program Users**
  - ***Constituency served:*** **NSTIC focuses primarily on the private sector, particularly consumers and businesses. Government is an important partner, however, particularly as an adopter of new identity solutions to enable people and businesses to engage in new types of transactions online.**
  - ***Current state of implementation*****: NSTIC is on pace to meet its 3- to 5-year goals, as articulated in the strategy:**
    - **Subjects have the ability to choose trusted digital identities:**
      - **For personal or business use.**
      - **Between at least two identity credential and media types.**
      - **That are usable across multiple sectors.**
    - **There exists a growing marketplace of both trustmarked, private-sector identity providers at different levels of assurance and private-sector-relying parties that accept trustmarked credentials at**

different levels of assurance. This relying-party population is not confined to one or two sectors.

- Trustmarked attribute providers are available to assert validated attributes. Services available include the ability to assert validated attributes without providing uniquely identifiable information.
- The number of enrolled identities in the Identity Ecosystem is growing at a significant rate, and the number of authentication transactions in the Identity Ecosystem is growing at least at the same rate.
- Building on FICAM, all online Federal Executive Branch services are aligned appropriately with the Identity Ecosystem and, where appropriate, accept identities and credentials from at least one of the trustmarked private-sector identity providers.

All references to a trustmark indicate that the service provider complies with the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms of the Identity Ecosystem Framework.

- ***Program scope and stakeholders:*** **As a national strategy, everyone in the nation is considered a stakeholder. We also view the international community as a key stakeholder, since identity does not stop at the nation's borders.**

- **Online Program Resources**
  http://www.nstic.gov
  http://nstic.blogs.govdelivery.com/ (blog)
  https://www.idecosystem.org/ (Identity Ecosystem Steering Group)
  @nsticnpo

- **Program Point(s) of Contact**
  Jeremy Grant
  Senior Executive Advisor for Identity Management
  National Strategy for Trusted Identities in Cyberspace (NSTIC)
  National Institute of Standards and Technology (NIST)
  (202) 482-3050
  jgrant@nist.gov

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8–9, 2014

- **Program Name:** Personal Identity Verification (PIV-I)/First Responder Authentication Credential (FRAC) Technology Transition Working Group (TTWG)

- **Program Description and Business Case**
  - Program description and maturity: The PIV-I/FRAC TTWG is composed of state and local emergency management, fire, law enforcement, health, and fusion center personnel, as well as state and local government representatives implementing innovative and secure identity-management solutions in their own jurisdictions.

  - The purpose of the working group is to:
    - Provide federal policy makers with a unified state emergency manager perspective on Federal/Emergency Response Official (F/ERO) attributes.
    - Baseline current identity infrastructure and best practices to share with stakeholders.
    - Identify technological gaps where DHS S&T Cybersecurity Division can provide test-bed research and development support.
    - Share information: state to state, state to federal, federal to state.

  - Who manages the program? DHS S&T in collaboration with FEMA.

  - Explain program governance:
    - DHS S&T sponsors the logistics requirements and supports state and local officials with cybersecurity technology gaps and requirements.
    - FEMA chairs the TTWG with a state or local representative as the cochair, and FEMA facilitates the quarterly meetings.

  - Relationship to other ICAM programs? Endorses the FICAM and SICAM road maps as well as promotes the National Incident Management System (NIMS) Guideline for the Credentialing of Personnel; develops technologies that meet NIST 800 series and FIPS 201 standards.

  - How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety?"
    - TTWG endorses a medium hardware token credential and Federal Information Processing Standard (FIPS) 201 technology to achieve credentialing interoperability to make informed physical, logical, or emergency access control decisions.

- S&T is developing standards, processes, and technologies that provide attribute-based access control methods for mobile end points based on FEMA and state and local requirements.

- Planned next steps, increasing adoption and implementation, and future activities:
  - Continue quarterly meetings to promote routine and emergency use cases for credentialing interoperability across multiple domains.
  - S&T is supporting FEMA and members of the TTWG to conduct operational pilots and implementations for both physical and logical access control using mobile devices.

- **Program Users**
  - Constituency served: federal, state, local, and private sector emergency response, recovery, and relocation officials.
  - Current state of implementation: mandated for the Federal Executive Branch and encouraged per NIMS Guideline for the Credentialing of Personnel using Grant Funds.
  - Program scope and stakeholders (local, tribal, state, federal?): All of nation/whole community emergency response, recovery, and relocation stakeholders.

- **Online Program Resources:**
  - http://www.ahcusa.org/PIV-I%20TTWG.htm
  - http://www.dhs.gov/csd-idm
  - http://www.dhs.gov/cyber-research

- **Program Point(s) of Contact;**

Karyn Higa-Smith
Program Manager
Cyber Security Division (CSD)
Homeland Security Advanced Research Projects Agency (HSARPA)
Science and Technology (S&T) Directorate
U.S. Department of Homeland Security
Office: (202) 254-5335
E-mail: karyn.higa-smith@dhs.gov

Craig A. Wilson
Deputy Director, Operations Division
Officer-in-Charge, Continuity Readiness Center
DHS/FEMA National Continuity Programs
FEMA HQ: (202) 212-1523
MW CRC: (540) 722-1934
Mobile: (202) 368-2139
E-mail: craig.wilson@fema.dhs.gov

Identity, Credential, and Access Management (ICAM)

Wireless Mobility in Law Enforcement, Justice, and Public Safety

National Strategy Summit

Bureau of Alcohol, Tobacco, Firearms and Explosives
U.S. Department of Justice
99 New York Avenue, NE ♦ Washington, DC 20226

October 8-9, 2014

- **Program Name:** Trustmark Framework
  (This Briefing Sheet specifically discusses the National Strategy for Trusted Identities in Cyberspace Trustmark Pilot: "Scaling Interoperable Trust through a Trustmark Marketplace")

- **Program Description and Business Case**

  - Program description and maturity:

    The federated identity landscape is maturing, but it is currently fragmented into a collection of various noninteroperable identity frameworks and federations. A significant amount of effort has been spent on developing basic federated identity concepts and implementing those concepts in operational identity federations; to date, however, there is no clear vision for how these various implementations will merge into a single, cohesive Identity Ecosystem that properly accounts for all aspects of trust and interoperability.

    In late 2013, the National Institute of Standards and Technology (NIST) awarded a grant to the Georgia Tech Research Institute (GTRI) under the 2013 NSTIC Pilots Cooperative Agreement Program. Under the grant, titled "Scaling Interoperable Trust through a Trustmark Marketplace," GTRI is developing an innovative solution to the "trust and interoperability scaling problem" that currently plagues the Identity Ecosystem. This problem, also commonly known as the "inter-federation" challenge, represents a major barrier to the deployment of cost-effective, wide-scale, federated identity solutions. The GTRI solution to this problem is based on the concept of a *Trustmark Framework*. A trustmark is a rigorously defined, machine-readable

statement of compliance with a specific set of technical or business requirements. Trustmarks are a vehicle for clearly expressing and componentizing trust and interoperability requirements from disparate communities and facilitating the formalization and reuse of those requirements by others. They can therefore enable the cost-effective scaling of interoperable trust across multiple communities within the Identity Ecosystem.

The following figure illustrates the basic Trustmark Concept Map, which provides a high-level description of what a trustmark is, how it is defined, and how it is used. Terms and concepts represented are as follows:

- **A trustmark is a statement of conformance to a well-scoped set of identity trust and/or interoperability requirements.**

- **A Trustmark Provider (TP) is an organization or other business entity that issues a trustmark to a Trustmark Recipient (TR) based on a formal assessment process. The trustmark is issued under a Trustmark Policy (not shown) and is subject to a Trustmark Recipient Agreement (also not shown). A Trustmark Recipient is always an organization or other business entity; trustmarks are not issued to individuals.**

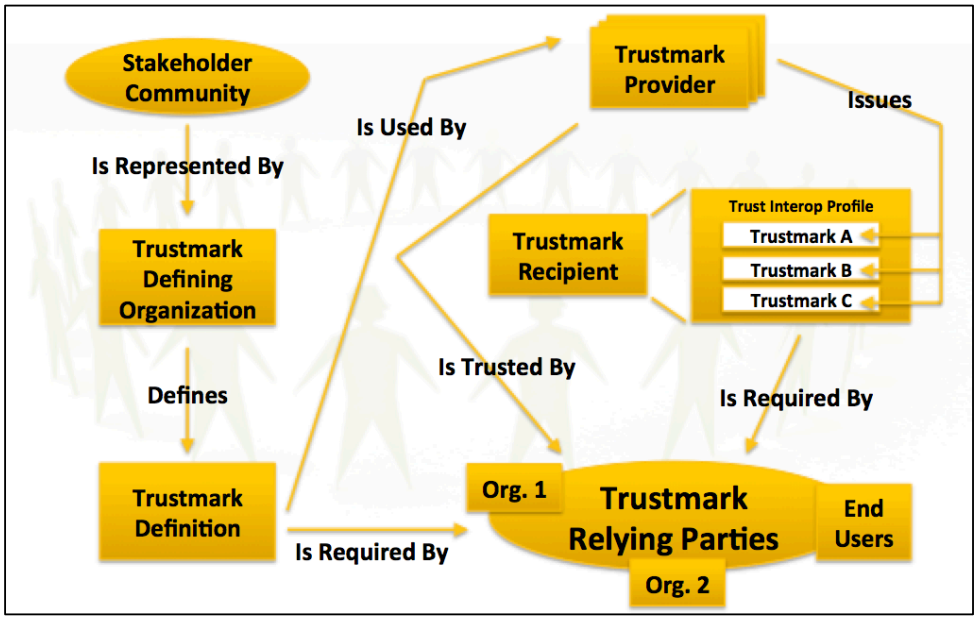
- **A Trustmark Definition (TD) specifies the conformance criteria that the Trustmark Recipient must meet, as well as the formal assessment process that the Trustmark Provider must perform to assess whether the Trustmark Recipient qualifies for the trustmark. There can be many different types of trustmarks, and each type of trustmark has its own Trustmark Definition. A Trustmark Definition is also sometimes called a Trustmark Component Definition (TCD).**

- **A Trustmark Definition is developed and maintained by a Trustmark Defining Organization (TDO), which represents the interests of one or more Stakeholder Communities. A TDO is similar in function to a Standards Development Organization (SDO).**

- **Possession of a Trustmark by the Trustmark Recipient is required by a Trustmark Relying Party (TRP), which treats the trustmark as third-party-verified evidence that the Trustmark Recipient meets the trust and/or interoperability criteria set forth in the Trustmark**

Definition for the trustmark. When it relies on a trustmark, a Trustmark Relying Party enters into a Trustmark Relying Party Agreement (not shown) with the Trustmark Provider. A Trustmark Relying Party may be either an organization or an individual.

- **A Trustmark Relying Party defines a Trust Interoperability Profile (TIP) that expresses a trust and interoperability policy in terms of a set of trustmarks that a Trustmark Recipient must possess in order to meet its trust and interoperability requirements.**



- **Relationship to other ICAM programs?**

  The pilot project leverages GTRI's experience in developing federated identity and authorization standards such as the Global Federated Identity and Privilege Management (GFIPM) (http://gfipm.net/) and leading the National Identity Exchange Federation (NIEF) (https://nief.gfipm.net/) for the law enforcement and public safety community with membership that spans federal, state, local, and tribal boundaries. The pilot includes strategic partnerships with the National Association of State Chief Information Officers (NASCIO) and several NIEF member agencies, such as Los Angeles County and the Regional Information Sharing Systems (RISS).

- **How does the program fit into an overall strategy for "wireless mobility in law enforcement, justice, and public safety?"**

GTRI's goal in this pilot is to develop and demonstrate a technical solution that enables greater opportunities for trust and interoperability among participants in the Identity Ecosystem, both within and across communities.

- **Current state of implementation; planned next steps, increasing adoption and implementation, and future activities.**

  Throughout the first year of the NSTIC Trustmark Pilot, GTRI has developed a comprehensive trustmark framework that implements the concepts described in the previous section. The framework includes the following artifacts.

  - **A comprehensive set of *normative technical specifications* for the artifacts that will exist within the framework, including trustmarks, Trustmark Definitions, and Trust Interoperability Profiles**

  - **A set of *60+ Trustmark Definitions*, representing the trust and interoperability requirements for both the Federal Identity, Credentialing, and Access Management (FICAM) initiative and the National Identity Exchange Federation (NIEF), which serves the U.S. law enforcement community**

  - **A *legal framework* that enables the issuance and use of trustmarks while also allowing for proper placement of liability and risk-based decision making in a scalable manner**

  - **A set of *software tools* that leverage the trustmark framework specifications to enable various critical functions involving trustmarks**

  As the GTRI NSTIC pilot nears the end of its first year, the GTRI team is transitioning from the design and implementation of the trustmark framework to an "Initial Operational Capability" phase. During this phase, GTRI plans to issue trustmarks to a variety of recipients to demonstrate the viability of the trustmark concept for solving the problem of cross-community trust and interoperability. Specific demonstration opportunities and objectives that GTRI plans to meet during the second year of the project are as follows:

- **Demonstrate that trustmarks can enable organizations to achieve limited or partial participation in a law enforcement community trust framework without having to meet all of the framework's monolithic requirements.**

- **Demonstrate that trustmarks can enable organizations outside the law enforcement community to participate in cross-community data exchange scenarios with law enforcement agencies.**

- **Demonstrate that trustmarks can serve as the foundation for trust and interoperability within statewide Information Sharing Environments (ISEs).**

- **Demonstrate that trustmarks can serve as the foundation for trust and interoperability across disparate identity federations and trust frameworks within a single community.**

- **Demonstrate that trustmark definitions can be reused across multiple communities.**

- **Demonstrate that trustmark definitions are sufficiently well-defined and well-specified to enable multiple trustmark providers to issue trustmarks based on them, such that the trustmarks issued are widely considered to be equivalent by those who rely on them.**

- **Program Users**

  - **Constituency served; Program scope and stakeholders (local, tribal, state, federal?)**

    As previously noted, the pilot includes strategic partnerships with the National Association of State Chief Information Officers (NASCIO) and several NIEF member agencies, such as Los Angeles County and the Regional Information Sharing Systems (RISS). As the GTRI team transitions to an "Initial Operational Capability" phase, additional trustmarks will be issued to a variety of recipients to demonstrate the viability of the trustmark concept for solving the problem of cross-community trust and interoperability.

- **Online Program Resources**

  To learn more about the GTRI NSTIC Trustmark Pilot, please see the project Web site at https://trustmark.gtri.gatech.edu/.

- **Program Point(s) of Contact**

Mr. John Wandelt
Research Fellow and Division Chief
Information Exchange and Architecture Division
Georgia Tech Research Institute
Executive Director, National Identity Exchange Federation
Atlanta, GA
Phone: (404) 386-1264
E-mail: John.Wandelt@gtri.gatech.edu

Identity, Credential, and Access Management (ICAM)
Wireless Mobility in Law Enforcement, Justice, and Public Safety
National Strategy Summit

Appendix G

ISE Brochure: Introduction to ICAM Principles—Identity, Credential, and Access Management

INTRODUCTION TO ICAM PRINCIPLES

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

ICAM—**IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT**—is the set of security disciplines that allows an organization to enable the right individual to access the right resource at the right time for the right reason.

We perform ICAM-related functions dozens of times per day, often without realizing it: when we unlock our cars, swipe into and out of the subway/metrorail, check our email, and withdraw cash at an ATM. Can you imagine if anyone could withdraw cash from your account? Or if anyone could start your car?

1 IDENTITY MANAGEMENT

Identity Management is the set of practices that allow an organization to establish, maintain, and terminate identities.

An **IDENTITY** is the set of characteristics (also called "attributes") that describe an individual **within a given context**:

- Your identity within the context of the Department of Motor Vehicles (DMV) is different from your identity within the context of your bank.
- Similarly, a person who is both a government contractor and an Army Reservist will have two identities, one in each context. These identities are often called "personas."

Identities change and evolve over time (you may get a promotion, change your hair color, or receive additional training) and may be terminated (you may turn in your driver's license when you move to another state), but **identities do not expire**.

IDENTITY PROOFING is the process by which an identity is first established. This process can be simple or complicated, depending on the Level of Assurance (strength) that is required of the identity:

- The process for a frequent shopper program at the local grocery store is weak.
- The processes required by the DMV is stronger, typically requiring multiple forms of evidence, such as leases, mortgages, and utility bills.
- The process required by the Federal Government is stronger still.

An **IDENTIFIER** is a unique attribute that can be used to locate a specific identity within its context:

While the DMV may issue many driver's licenses bearing the same name (there is more than one John Smith in the state), each will have a different driver's license number.

2 CREDENTIAL MANAGEMENT

Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for **identities within their context**.

A **CREDENTIAL** is authoritative evidence of an individual's claimed identity. Credentials come in many types, from physical papers and cards (such as a passport or ATM card) to electronic items (such as a password or digital certificate), and often incorporate anti-tamper features.

All credentials, no matter what type, associate an identity with an individual (typically via an identifier) and identify the organization that issued it:

- Your driver's license includes a license number, your name, and a state seal.
- An ATM card includes a card number, your name, and a corporate symbol.

Some credentials indicate authorizations granted to the identity by the issuing organization. For example, a driver's license includes the authorization to drive a car.

Unlike identities, **credentials generally expire**. If an identity continues past the expiration date of the credential, a new credential is issued:

- Your driver's license expires after so many years and you receive a new one.
- Your ATM card expires after so many years and you receive a new one.

A credential that is lost or compromised before it expires may be revoked by the organization that issued it.

Credentials can incorporate something you know (such as a password or PIN), something you have (such as a card), or something you are (such as a fingerprint or iris). Some credentials incorporate more than one, and are referred to as two-factor or multi-factor.

As with identity proofing, credentials have different Levels of Assurance depending on the strength required. The credential for accessing your bank account is likely stronger than the credential for accessing your health club.

3 ACCESS MANAGEMENT

Access Management is the set of practices that enables only those permitted the ability to perform an action on a particular resource.

POLICY MANAGEMENT is the process by which laws, regulations, rules, and organizational/corporate access policies are put into effect. These policies may be extremely simple, extremely complicated, or anywhere in between.

For example:

- "Grant access to anyone who knows the secret handshake."
- "Grant access to anyone on this list of people."
- "Grant access to anyone in Human Resources."
- "Grant access to anyone who is a federal employee, GS-12 or higher, cleared Top Secret, trained in first aid, and certified as a project manager."

AUTHORIZATION is the adjudication of requests. Please see the section on Authorization on the reverse side of this page for more details.

4 BRING YOUR OWN IDENTITY

Bring your own identity is the ability to use an identity and credential from one context in another.

For example, a bar does not conduct an Identity Proofing process to establish your identity and issue you a credential within the context of that specific bar. Rather, the bar accepts your driver's license even though it is from a different context.

This same idea is being applied in the electronic space as well: many websites now accept external identities (such as Facebook®, Twitter®, LinkedIn®, Google+® or Amazon®) for access, rather than having to obtain a new credential (such as a login name and password) for each website. These websites accept the external identity and credential, even though they are from a different context.

5 AUTHENTICATION

Authentication is the process by which a claimed identity is confirmed, generally through the use of a credential:

- When going through airport security, you present your driver's license, confirming your identity as the ticketed passenger.
- When you attempt to withdraw cash at an ATM, you present your ATM card and enter your personal identification number (PIN), confirming your identity as the account holder.

Authentication is generally a two-step process:

Step 1. Authenticate the credential itself:

- Was the credential issued by a trusted organization?
- Has the credential expired?
- Has the credential been revoked, voided, or tampered?

Step 2. Ensure that the individual the credential was issued to is the same individual that is presenting it:

- Does the photo and height/weight on the driver's license match the person who presented it?
- Does the person know the PIN for the ATM card that was presented?

Authentication is how you **confirm who you are**. Identity proofing is performed to **establish** an identity, whereas authentication is performed to **use** an identity.

6 AUTHORIZATION

Authorization is the decision portion of Access Management: the process by which a request to perform an action on a resource is decided, typically based on a policy. The range of possible requests is very broad:

- A request to read a certain document.
- A request to receive a benefit.
- A request to enter a facility or location.

In some cases, it is necessary to perform authentication in order to perform authorization:

When you present your driver's license at a bar, you are simultaneously authenticating (the bartender ensures the photo on the license matches the person) and authorizing (the bartender ensures you are old enough).

In other cases, authorization can occur without authentication:

When you unlock your car, the car is authorizing you without knowing who is holding your keys. If you give your keys to a friend, he or she is just as able to unlock your car as you are, and the car does not know the difference.

Authorization is how your **request for a resource is decided**.

7 FEDERATION

Federation is the ability of one organization to accept another organization's work. Federation is based on **inter-organizational trust**. The trusting organization has to be comfortable that the trusted organization has similar policies, and that those policies are being followed:

- A credential issued by your local library will not likely be trusted by the security staff at the White House.
- A credential issued by your bank may be trusted by your health club.

Federation can occur at different points within ICAM. Examples include:

An organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally:

A passport issued by the U.S. Department of State is accepted as a valid credential by a foreign country, but that country's immigration office still authenticates the holder and requires a visa (authorization).

An organization can accept specific characteristics (attributes) describing an individual from another organization:

Your bank will request your credit score from one of the credit bureaus, rather than maintaining that information itself.

An organization can accept an authorization decision from another organization:

A driver's license authorizing you to drive in one state is accepted by another.