Identity, Credential, and Access Management (ICAM) Acquisition Guidance

Science and Technology Directorate

Homeland Security

Science and Technology

Primary Authors

Christine Owen

Larry Kroll

Chris Price

David Shapiro

Contributing Organizations

Oasys International Corporation

Department of Homeland Security (DHS) Science & Technology Directorate

Partner Engagement-Information Sharing Environment (PE-ISE)

DHS Office of Emergency Communications (OEC)

First Responder Network Authority (FirstNet)

Federal Communication Commission (FCC)

National Institute for Science and Technology Public Safety Communications Research Division (NIST PSCR)

PUBLIC SAFETY COMMUNICATIONS

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT WORKING GROUP

Identity, Credential, and Access Management (ICAM) Acquisition Guidance

February 2019

Version 2

Prepared for

Department of Homeland Security

Science and Technology Directorate

Dedicated to the memory of:

Tom Sorley
1965-2018

The Identity, Credential, and Access Management (ICAM) Educational Series is dedicated to the memory of Tom Sorley. Tom was a member of the executive leadership of the DHS-established Public Safety Communications ICAM Working Group, which sponsored this document. He was the Chief Information Officer and Deputy Director of the Information Technology Department for Public Safety for the City of Houston, Texas, and National Chair of the Public Safety Advisory Committee (PSAC). Tom was a thought leader in public safety communications and his vision is reflected in this ICAM Educational Series.

DISCLAIMER OF LIABILITY

The Identity, Credential, and Access Management (ICAM) Educational Series is provided by the Public Safety Communications ICAM Working Group (PSC ICAM WG) "as is" with no warranty of any kind, either expressed or implied, including, but not limited to, any warranty of merchantability or fitness for a particular purpose. This material is provided to support the efforts of public safety information sharing, situational awareness, and key decision making. These documents are intended to guide users for making informed decisions on improving the security posture of their information systems by using ICAM principles.

The ICAM Educational Series is intended to provide guidance for implementing ICAM principles, and does not contain or infer any official requirements, policies, or procedures, nor does it supersede any existing official emergency operations planning guidance or requirements documents. As a condition of the use of the Series, the recipient agrees that in no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected to the Series or the use of information from the Series for any purpose. It is recommended that organizations align their resources with tools that would best fit their infrastructure as well as their own standards and requirements.

The PSC ICAM WG does not endorse any commercial product or service referenced in the ICAM Educational Series, either explicitly or implicitly. Any reference herein to any specific commercial product, process, or service by service mark, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the PSC ICAM WG. The views and opinions of authors expressed herein do not necessarily state or reflect those of the PSC ICAM WG and shall not be used for advertising or product endorsement purposes.

EXECUTIVE SUMMARY

The Public Safety Communications (PSC) Identity, Credential, and Access Management (ICAM) Working Group (WG) performed an assessment of available policy, procurement, grant, and other solicitation sources for ICAM procurement language across the Federal and State marketplace. This document provides guidance to the Public Safety Community (Community) to enhance existing infrastructure to include ICAM principles. To produce this document, gaps were discovered in publicly available documentation that affect an engineer's ability to effectively implement an ICAM-enabled system. These gap analyses and assessments resulted in the development of this ICAM Acquisition Guidance document for state, local, tribal, and territorial (SLTT) program managers and solutions architects. This document includes draft acquisition language that could be used as "boilerplate" for ICAM acquisitions.

The Community's goal is to have the ability to appropriately share critical information among members of the Community, which can aid in saving lives and protecting property. This critical information is at times highly sensitive and can include law enforcement information, as well as personally identifiable information (PII) and protected health information (PHI), so each organization must have assurance the right person with the right credentials is accessing information at the right time. An ICAM-principled solution can provide this assurance.

To support the Community with its mission-critical tasks, ICAM helps to address the growing data management, interoperability, and cybersecurity challenges facing public safety today. ICAM solutions, especially federated ones, align public safety communities around common identity and access management practices.

It is also important for Community members who are sharing information between different organizations to make sure the information is not compromised. This is where ICAM is essential for the Community. Identity proofing an organization's employees and volunteers, providing strong credentials for system access and enabling the use of multifactor authentication, using attributes to provision resources, and creating strong access management all help an organization ensure that the right person is accessing an organization's information through a secure and seamless federation.

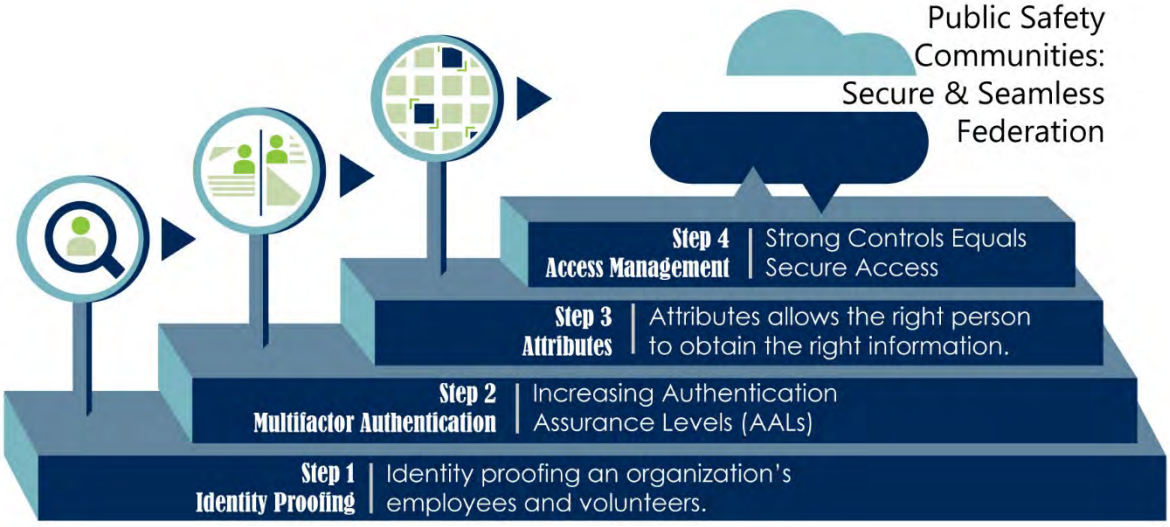

Figure 1 - Steps to Secure and Seamlessly Share Information (Federation)

The intent of this document is to provide ICAM acquisition guidance to the Community. This document does not recommend specific ICAM products, but does strive to create a unifying, straightforward

acquisition approach to aid in the sharing of resources and encourage the adoption of multifactor authentication with a focus on the use of open source products. This document is paired with the ICAM Executive Primer, ICAM Implementation Guides and ICAM Federation System Checklist.

Intended Audience

This document provides guidance to acquire the ICAM solutions needed to enable multifactor authentication to support the Community's missions. The document informs each of the following stakeholder groups[1] about multifactor authentication, ICAM solutions, and ICAM acquisition:

Stakeholder Group	**Responsibilities**	**Documents to Read**
Executive Leadership	…is the responsible authority for the department, state, or agency's fiscal and human resources for ICAM investments. This stakeholder group will use the document to understand the importance of ICAM investments, and to translate the value proposition of ICAM solutions to their mission needs.	ICAM Executive Primer
Program Managers	…are responsible for the operational implementation and oversight of ICAM capabilities to ensure they meet the functional mission requirements defined by the intended users. They must communicate to both the executive leadership and solutions architects to ensure understanding and expectations of the requirements for interoperable ICAM investments. Managers are required to quantify the benefit and resource impacts, including cost and integration savings, to executive leadership to ensure continued support and resource sustainment. This document provides program managers with a description of the key capabilities, processes, services, infrastructure, standards, and procurement language samples that are required of an interoperable ICAM architecture solution.	This document, ICAM Executive Primer & ICAM Federation System Checklist
Solution Architects	…are responsible for acquisition requirements and the design/development/integration of ICAM solutions in accordance with their respective organization's enterprise architecture technical and management requirements. The solution architects will be required to compare and quantify the technical implementation options, alternatives, and cost constraints to the program managers. This document provides structured technical guidance and reference artifacts to assist in achieving an ICAM-enabled system.	This document, ICAM Executive Primer, ICAM Implementation Guides & ICAM Federation System Checklist

[1] Each stakeholder's responsibilities were adopted from the Information Sharing Environment Geospatial Interoperability Reference Architecture (GIRA), available at https://www.dni.gov/files/ISE/documents/DocumentLibrary/GIRA.pdf.

CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

This document serves as a source of Identity, Credential, and Access Management (ICAM) acquisition guidance resulting from an assessment of available public documents. The ICAM landscape is complex and there are many elements to consider. ICAM policies are important to have in enabling technology to share data within a wide variety of applications, including an organization's existing legacy systems as well as emerging nationwide initiatives, such as the Nationwide Public Safety Broadband Network (NPSBN), Next Generation 911 services, and the First Responder Network Authority (FirstNet).

This document focuses on two goals. First, it can assist state, local, tribal, and territorial (SLTT) Public Safety Community (Community) entities in improving the security posture of their systems for safe and secure information sharing. Secondly, this document can guide any organization acquiring ICAM products. This document focuses on implementing multifactor authentication on an organization's systems to fortify the organization's authentication methods, thus improving the systems overall security. Adopting multifactor authentication when upgrading to an ICAM-enabled system is highly recommended for any organization, but it is especially recommended for the Community based on a risk assessment of the typical information stored in the Community's systems. This document is the second of a series of ICAM educational tools, including the ICAM Executive Primer, ICAM Implementation Guides and ICAM Federation System Checklist.

1.1 PURPOSE

The goal of this document is to enable any organization, including the SLTT Community, to spend its resources wisely on thoughtful and well-specified ICAM procurement activities that result in an ICAM-enabled system that includes multifactor authentication. This document references appropriate standards for ICAM based on the assessments of the Community's systems. Additionally, it provides prescriptive language to be used by the Community in Requests for Information (RFIs) and Requests for Proposal (RFPs) to ensure proper implementation of technological solutions. It does not endorse any individual vendor or solution available. This document seeks to leverage existing efforts to maximize the value of existing ICAM products and solutions as well as to avoid duplication. The procurement guidance within this document allows the Community to leverage current best practices for ICAM procurement with draft procurement language.

1.2 BACKGROUND

This document was commissioned by the Public Safety Communications Identity, Credential, and Access Management Working Group (PSC ICAM WG), which is a subsidiary group of the Information Sharing Council (ISC) with a Federal Advisory Committee Act (FACA) exempt status under Section 1016(g)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended). Its member organizations include Department of Homeland Security (DHS) Science and Technology Directorate (S&T) First Responder Group (FRG), Partner Engagement Information Sharing Environment (PE-ISE), DHS Office of Emergency Communications (OEC), First Responder Network Authority (FirstNet), Federal Communications Commission (FCC), as well as National Institute of Standards and Technology (NIST) Public Safety Communications Research Division (PSCR). The PSC ICAM WG supports the ISC in fulfilling the ISC's duties (with a focus on public safety) pertaining to the interchange of information between public safety agencies by addressing policy, governance, standards, technology and acquisition guidance on ICAM capabilities for the public safety community.

1.3 APPROACH

Through outreach to various communities (including FirstNet Stakeholders, the Federal ICAM Subcommittee, DHS Cyber, and the Office of the Director of National Intelligence's Sensitive But Unclassified (SBU) Technical Advisory Committee (STAC)) and utilization of the tech foraging capabilities at DHS, the PSC ICAM WG gathered existing procurement and acquisition language. Sources assessed include existing RFIs, RFPs, and statements of work (SOWs) across all levels of government. Information was also collected from building ICAM-enabled systems in a test environment (i.e., sandbox). After gathering existing procurement and acquisition language and completing builds in the sandbox, the PSC ICAM WG created this procurement guide. While creating this guide, the PSC ICAM WG assessed best practices from all available sources and provided procurement guidance for use as language that can be used as "boilerplate" for acquiring a federated ICAM-enabled system with multifactor authentication.

1.4 ENABLING MULTIFACTOR AUTHENTICATION

ICAM concepts appear in everyday life. When leaving our homes or cars, most of us choose to lock our doors and restrict access only to those with a key.[2] Likewise, anyone who accesses the internet creates a username and password to access a computer system, email or social network, which are examples of *single factor authentication*.

Most people only use a username and password when accessing computer systems, likely due to a perceived notion of convenience. A username and password combination or pin number are examples of single factor authentication when they are used on their own. Single factor authentication is simple and easy to implement, but it only provides a minimal level of assurance that authentication is legitimate. The practice is akin to leaving a door unlocked for malicious actors. Since passwords are easily obtained via email phishing, single factor credentials played a factor in 81 percent of the systems that were hacked in 2016.[3]

Multifactor authentication uses a combination of credentials to provider higher assurance that the individual attempting to access a protected resource is that individual. To create this higher assurance, multifactor authentication requires the use of at least two of three "factors." The factors include something you have (an ATM card), something you are (a fingerprint or other biometric), or something you know (a password or personal identification number [PIN]). Multifactor authentication employs small measures to save us from breaches that deplete organizations of time, money, and most importantly, information.

When organizations connect their systems with others within their community, the organizations will need to know who is accessing which pieces of information at what times to ensure only authorized users are within the system. Multifactor authentication becomes useful in information sharing scenarios. After performing a risk assessment based on the type of information held in the SLTT Community's systems, it was determined that multifactor authentication would reduce the risk of a system intrusion. As a result, this document, as well as the Implementation Guides and Executive Primer, are all tailored towards ICAM systems with multifactor authentication.

[2] Most public safety communications systems, radio sites, public safety facilities, data centers, and radios are physically secured against internal and external threats.

[3] Verizon Enterprise Solutions, 2017 Data Breach Investigations Report, which can be found at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

1.5 How to Use

The content within this document gives an overview to program managers of what to look for while acquiring ICAM products and teaches solutions architects about the lessons learned from sandbox builds of ICAM-enabled systems with multifactor authentication. This document is part of a progressive series that begins with the ICAM Executive Primer, a high-level, educational dive into ICAM through ICAM concepts and real-world scenarios for executive leadership and others. The series continues with Implementation Guides that provide a deeper view into an ICAM-enabled system configured with multifactor authentication for solutions architects. The series ends with an ICAM Federation System Checklist, which includes five topics that should be addressed by a system owner before federating a system. This series also contains several helpful sections and appendices, including reference architecture, implementation guidance and procurement language.

This document was developed by the DHS-established Public Safety Communications (PSC) Identity, Credential, and Access Management (ICAM) Working Group (WG); questions and comments can be sent to DHS S&T at: SandTFRG@hq.dhs.gov.

2 ACQUIRING AN ICAM-ENABLED SYSTEM

Building a sophisticated ICAM-enabled system can be complicated and time consuming. Systems architects should set preliminary standards for their respective systems prior to building physical systems. This process can be described as Acquisitions Management.[4] Determining system requirements (security level, capacity), is often the first step, followed by setting system evaluation criteria. Organizations should also have a mature Change Management program and a set of approved technology vendors and products. This section provides recommendations and suggestions to aid in the acquisitions management process.

While acquiring technology, organizations can unknowingly be locked into a certain product offered by a specific vendor. Such capability-limiting and potentially expensive acquisitions (i.e., acquiring a product that does not work well within a pre-existing system or is difficult to implement) can occur regardless of the acquisition department's expertise and sophistication. As such, an organization should maintain their data ownership, and organize that data in a standardized format that is usable by more than just that vendor's products, and that data migration will occur when the contract ends. The organization should also know whether it will be the owner of a product/system before it enters into a contract with a vendor.

2.1 DETERMINE SYSTEM REQUIREMENTS

During your investigation into an ICAM solution, you should conduct research on the technology topic, talk to system owners while drafting requirements, and obtain executive buy-in for your organization's system requirements. There are many sources from which you could obtain information, including ICAM-centric organizations, white papers from vendors, National Institute of Standards and Technology (NIST) Special Publications,[5] National Cybersecurity Center of Excellence (NCCoE) Building Blocks,[6] the SICAM Roadmap,[7] and ICAM materials found on https://www.idmanagement.gov/.

When obtaining executive buy-in for your technology acquisition, you should include system architects as well as system owners in the discussions to ensure your requirements are feasible and resilient for the new acquisition. As you build requirements, it is important to ensure that they are realistic and necessary.

2.2 EVALUATION CRITERIA

While this document provides sample language for various procurement scenarios in Appendix A: ICAM Procurement Language, it is important to discuss evaluations of responses to an RFI or RFP. Outside of an evaluation of whether the vendor meets the requirements prescribed in the language provided in the RFI, RFP, etc., evaluation criteria is dependent on the organization procuring the technology. Questions to be considered when reviewing a proposed technical solution for ICAM are:

[4] https://www.state.gov/m/a/c8020.htm

[5] https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5

[6] https://nccoe.nist.gov/projects/building-blocks

[7] While the SICAM Roadmap has not been updated since 2012 and includes some older concepts of identity (including levels of assurance), its general concepts and correlation to the FICAM Roadmap are still valid. It can be found at https://www.nascio.org/Publications/ArtMID/485/ArticleID/161/The-State-Identity-Credential-and-Access-Management-Guidance-and-Roadmap-SICAM.

Does the vendor provide a solution that fits the system requirements?

- System requirements should be determined by the organization and communicated in the solicitation.
- Are there gaps between the product's capabilities and the organization's requirements?
- Is the product interoperable within the organization's current infrastructure?

Does the vendor provide evidence that demonstrates a high maturity level of experience?

- What is the vendor's past performance and references, including recent and *relevant* contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers, and other relevant information, which should be checked and verified)?
- Does the vendor have any white papers, prototypes, or demonstrated test results?
- Does the vendor demonstrate knowledge and experience for compliance with established open standards and/or authorities?

Does the vendor offer a proprietary solution purported to be compatible with established standards and/or authorities?

- Will the vendor give a demonstration of product interoperability?
- What benefits would a proprietary solution offer?
- Is the vendor solution interoperable with other products or does the vendor suggest purchasing related products from its company?[8]
- What is the ultimate, multi-year cost of the proprietary solution?

What other items/services are included with the vendor's solution?

- Is the product open source?
- If it is not open source, is the product low-cost?
- What is the total cost of the solution and what does that cost include?
- Is there an intuitive interface that results in end-user usability?
- What is the vendor's capability or service?
- Are there any required product licenses or hardware?
- Can the system be customized? Will the vendor customize the system?
- Will the vendor include product and system testing in the overall cost?
- Will the vendor include installation / implementation of the system in the overall cost?
- Will the vendor operate and maintain the system?

Another important consideration in evaluating proposed solutions is end-to-end evaluation. Just because each component is compliant with the standards does not mean that it will work well with the other

[8] Vendor "lock-in" traps you into continuing to obtain your solutions from a single vendor because their products are not interoperable or can't easily be swapped for a solution using open standards. Aside from the obvious cost risk vendor lock-in introduces, other risks of lock-in include maturing your enterprise based on the vendor's development priorities and the potential for non-interoperability within your own system. You may also find your product is discontinued, causing a forced, abrupt migration.

components that are either proposed by the vendor or within the pre-existing system. Organizations should ensure everything they purchase is evaluated as an integrated solution. A good way to accomplish this is to ask for the vendor to demonstrate their solution in your test environment to simulate the solution's interaction with your in-place products.

2.3 CHANGE MANAGEMENT TO MULTIFACTOR AUTHENTICATION

When determining which type of credential to choose for multifactor authentication, it is important to think about change management within the organization. Users may be reluctant to change; initiate early, open, and frequent communication to ready users for multifactor authentication (or any technology change).

There are many different types of credentials on the market. While finding the right one for your organization might take a large amount of research, finding the right credentials for your users is crucial for a successful implementation of multifactor authentication. Credentials should not be bulky or hard to use – an organization should choose a credential that is intuitive to use and fits its users' needs. If typing a six-digit one-time password takes too much time for a user, then those types of credentials should be avoided.

2.4 CERTIFIED ICAM PRODUCTS/SERVICES

Both the federal government and ICAM-centric organizations have vetted many ICAM-related products and services. If a provider of ICAM products or services is on one of these lists, it indicates that its product/service may not need your organization to undergo extensive testing. Regardless, you should still vet these products and services against your specific requirements and current system architecture.

2.4.1 Approved Products List (APL)

The Federal FIPS 201 Evaluation Program is maintained by the General Services Administration and performs testing and certification of ICAM services and commercial products used in credentialing systems, physical access control systems, mobile devices, and public key infrastructures (PKIs). This list includes the products and services related to federal ICAM implementation that have been approved after completing tests to ensure interoperability of products under federal requirements. The APL can be found at https://www.idmanagement.gov/approved-products-list/ and a list of approved PKI providers that the community can use to interoperate with the federal government can be found at https://www.idmanagement.gov/trust-services/.

3 LESSONS LEARNED FOR SYSTEM ARCHITECTS

To create this and other guidance, multiple ICAM-enabled systems were built with different configurations. These builds assumed most organizations use Microsoft products, including Microsoft Active Directory for their access management – giving employees and volunteers a username and password to sign into computer systems. However, Microsoft Active Directory only supports single factor authentication; to obtain multifactor authentication, an organization must install additional software in its system. As a result, the builds included free and low-cost, proprietary and open source products along with Microsoft products and systems. This section includes questions for system architects to ponder on topics determined from lessons learned while completing ICAM-enabled builds.[9]

3.1 SHOULD YOU HIRE AN ICAM EXPERT/SYSTEMS INTEGRATOR?

Because there are many different products on the market and several different combinations and configurations for ICAM-enabled systems, there is a dearth of publicly available documentation to help engineers with little ICAM knowledge build a system. While there is generally documentation on each individual piece, configuring an entire system is difficult without guidance.

Organizations might want to hire (or contract) someone with experience in systems and software engineering to build their ICAM-enabled systems. If the project's engineer has never created an ICAM-enabled system before, an organization could benefit from contracting a subject matter expert in ICAM and system requirements to help engineers understand the direction they need to take for the build.

Hiring ICAM expertise or an experienced integrator who has implemented ICAM solutions may shorten the installation and customization phases. The ICAM expert should have a strong understanding of ICAM-enabled systems as well as ICAM policy, governance, and best practices. A recurring problem in ICAM systems is the risk introduced by organizations that implement ICAM systems without considering best practices. In these cases, system security can be seriously compromised by errors in implementing the solution or where the ability for an organization to federate is blocked by a homegrown identity process that cannot interoperate with other organizations.

Regardless of your organization's determination to hire an expert, reference architecture and implementation guides have been provided to aid organizations and their engineers and can be found in the ICAM Implementation Guides.

3.2 IS A FREE, OPEN SOURCE PRODUCT RIGHT FOR YOU?

While there are free, open source products available that have many capabilities, the written documentation for those products sometimes do not include key pieces of configuration information for a non-ICAM expert. If there is a help desk associated with the product, it is generally for a fee. Lack of documentation and a free help desk could result in higher engineering costs.

Documentation for a product should be evaluated for timeliness of updates and completeness, and the organization should evaluate the robustness of the user community as a source of support in place of a commercial help desk. Similarly situated organizations that are also using the product could be an additional source of documentation, best practices, and community support.

An organization might determine that purchasing a product or an open source's service is worth the money, because it could include well-written documentation and a responsive help desk.

[9] The companion document, ICAM Implementation Guides, was created from these sandbox builds.

3.3 SHOULD YOU CHOOSE A FRAMEWORK FOR RESOURCE SHARING (FEDERATION)?

Modern public safety organizations have identified the need to engage in cross-jurisdictional information sharing. A *federation* is a community of organizations that come together to form an information sharing coalition with a standard set of practices and requirements for access to their resources. It allows for a person to use their local authentication policy across different organizations' systems.

Federations help facilitate information sharing and communication across unique organizations. Organizations may have different local identity management policies, and will have to ameliorate that obstacle by adopting community standards and an agreed set of requirements when entering a federation. Organizations in the same federation agree to trust one another through legal agreements and transparency in system audits.

The Community may create a federation in the future based on their communities of interest. Determining whether to participate in a federation should include a risk-based analysis of the overall system security of all the organizations that want to enter the federation against the opportunities of having additional users from other organizations to access your resources. It should also include the usefulness of resources that would be available to your users from federated networks. It's important to remember that each computer system within the federation is only as secure as the least secure system in the entire federation when considering how widely you would share sensitive resources.

If an organization does not have an IdP or domain controller, it cannot federate with another organization's system. Federations allow one organization to exchange information about its users in a standard, agreed-upon format, requiring all organizations to trust each other's authentication assertions that communicate a user's identity and their characteristics to external services and/or other organizations' identity hubs.

4 GRANTS AND OTHER FUNDING SOLICITATION SOURCES

Funding technology upgrades and modernization can be costly and beyond an organization's limited technology budget. Below is a list of organizations that may help locate grants and funding sources that could help cover procurement costs. Note that researching and applying for these grants could prove to be a drain on your organization's resources; this list is only a jumping-off point for finding funding for your solution.

4.1 DHS GRANT RESOURCES

Offered by government agencies, the DHS Grants Resources page provides a list of grants offered by government agencies. The list covers a wide range of topics including but not limited to firefighter grants, emergency medical service grants, and pre-disaster mitigation grants.

Link: https://www.dhs.gov/how-do-i/find-and-apply-grants

4.2 GRANTS.GOV

For a comprehensive list of federal grant funding opportunities, searchable by keyword or relevant criteria, visit Grants.gov. There, the community can learn more about the federal grants lifecycle, policies on grants management, and profiles on grant-making agencies.

Link: www.grants.gov

4.3 BUREAU OF JUSTICE ASSISTANCE

The Bureau of Justice Assistance posts funding announcements as funding becomes available. Each grant announcement contains detailed information about the opportunity, applicant eligibility, application requirements, and directions on how to apply.

Link: https://www.bja.gov/funding.aspx

4.4 OFFICE OF JUSTICE PROGRAMS

The Office of Justice Programs provides innovative leadership to federal, state, local, and tribal justice systems, by disseminating state-of-the art knowledge and practices across America and providing grants for the implementation of these crime fighting strategies. Because most of the responsibility for crime control and prevention falls to law enforcement officers in states, cities, and neighborhoods, the federal government can be effective in these areas only to the extent that it can enter into partnerships with these officers.

Link: https://ojp.gov/funding/

4.5 FEDERAL EMERGENCY MANAGEMENT AGENCY GRANTS

This site contains information on preparedness grants funding provided by FEMA to state, local, tribal, and territorial governments in the form of non-disaster grants by building, sustaining, and improving their capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. These grants support highest-risk transit systems, ports, and borders to prevent, protect against, respond to, recover from, and mitigate terrorism as well as other high-consequence disasters and emergencies.

Link: https://www.fema.gov/grants

4.6 SAFECOM

SAFECOM was founded as part of the Presidential E-Government Initiative in 2001 to improve public safety interoperability by allowing the community to communicate effectively throughout an emergency and disaster. It maintains a list of funding solutions to maintain interoperable networks.

Link: https://www.dhs.gov/safecom/funding

APPENDIX A: ICAM PROCUREMENT LANGUAGE

The section headers and language in this Appendix are designed to be directly cut and pasted into requests for proposal (RFPs) after tailoring the language based on an organization's specific requirements. Each section provides multiple options for contract language. Use the paragraph(s) that are applicable to your procurement. Areas where the organization should enter missing information based on their specific requirements will be indicated in brackets and bold font. The organization should add language using the headers to identify clauses that will be relevant to its procurement. All clauses under the particular header (e.g., Infrastructure) should be included to fully capture procurement requirements.

This Appendix is split into four sections. The first section, General Procurement Language, should be used for technology procurements. Section two outlines the procurement language definitions for a basic ICAM-enabled system with multifactor authentication. The third section details procurement language for a third-party consultant and/or contractor guiding an organization through a federation of a framework or implementation of an ICAM-enabled system. The fourth and final section, Authoritative Attribute Service (AAS), includes procurement language for attribute-based access control (ABAC) or role-based access control (RBAC) solutions.

Section One	Section Two	Section Three	Section Four
General Procurement Language	Definitions for a Basic ICAM Solution	Implementation Consultant/ Contractor	Authoritative Attribute Service
• Infrastructure • Customers • Compliance • Audit • Security • Privacy • Assurance Levels • Data Rights	• Identity Management • Credential Management • Access Management • Verification • Users	• Execution • Target State Analysis • Gap Analysis • Solution Prototyping • Supplemental Services • Solution Requirements • Operationalization • Additional Advisory Services	• Definitions • Analysis • Solutions • Supplemental Services • ABAC Specific Requirements • Capabilities • Architectural Interfaces & Specifications • Vendor Services

SECTION ONE: GENERAL PROCUREMENT LANGUAGE

Infrastructure:

- The solution SHALL be capable of interoperating with the architecture(s) and infrastructure(s) of **[insert organization's name]** while maintaining **[organization's]** requirements and applicable standards.
- The software, systems, and infrastructure employed by the solution SHALL be secured sufficiently to comply with the Customer's risk management plan to prevent fraudulent activities, security breaches, any compromise of the solution in a way that it is no longer able to provide reliable and trusted services, or other risks as addressed in NIST Special Publication 800-63-3 (or current version thereof).
- The Contractor SHALL ensure data communication between the Customer and partner systems SHALL be facilitated by secure protocols and methodologies. If any protocol or methodology necessary to achieve interoperability is deprecated per NIST guidance (e.g., NIST Special Publication 800-131A) or has otherwise been demonstrated to be vulnerable to known exploits (such as outdated software or hash algorithms such as SHA-1), the Contractor SHALL identify a remediation strategy for the risk introduced by such weakness, and the Contractor SHALL provide a timeline and transition process to remediate the weakness once it is no longer necessary to maintain interoperability.
- The Contractor SHALL support lifecycle / integration testing between the Contractor services and solutions, and/or other Customer applications utilizing Contractor services, including, but not limited to, Service Providers or Certification Authorities.
- Contracts with vendors for any modifications to software, systems, or code SHALL provide for continued use or rights to use by the Customer upon completion of contract.
- The Contractor SHALL support data export into open, non-proprietary format from the contracted system, software, or infrastructure.
- Infrastructure SHOULD favor standardized and open source configurations over proprietary configurations.

Customers:

- The solution SHALL provide all Identity, Credential, and Verification services and solutions necessary to enable users to access resources within the following systems: **[insert the names of applications and/or organization name**].
- The services and solutions SHALL be interoperable with the Customers' systems/infrastructure and SHALL consider all necessary policy, procedure, protocol, and payload interoperability considerations.
- The services and solution SHALL ensure that attribute data aligns syntactically and semantically with relying parties and can be exchanged and communicated with the appropriate relying parties to enable users to access the resources they require, and the Contractor SHALL coordinate with the appropriate Relying Parties to ensure the proper execution of this task.
- The Contractor SHALL ensure that attribute data fully complies with data format/schema specified by the Customer.

Compliance with Governance/Policy: **[Start Here]**

- All aspects of the solution SHALL be compliant with NIST SP 800-63-3: *Digital Identity Guidelines,*[10] or the most current version thereof.
- If the Customer's systems are interoperating with federal government information systems, all aspects of the solution and services provided SHOULD be compliant with the latest version of the *Federal Identity, Credential, and Access Management Guidance and Roadmap* (FICAM Roadmap).[11]
- If the Customer's systems are not interoperating with federal government information systems, all aspects of the solution SHALL be compliant with the latest version of the *State Identity, Credential, and Access Management Guidance and Roadmap* (SICAM Roadmap).[12]
- The services and solutions provided SHALL be compliant with the specifications of **[insert name of federation, if applicable]**

Audit:

- The Contractor SHALL perform audits of the performance of their services and solutions in compliance with the *Federal Identity, Credential, and Access Management Guidance and Roadmap* (FICAM Roadmap),[13] or SHALL outsource this activity to a third-party, which must still perform the activity in compliance with the above standard.
- The Contractor SHALL provide reporting services to include, but not limited to, usage reports, status reporting, security reports, etc. in formats as specified by the customer (e.g., STIX/TAXII/CybOX for security incident reporting).
- The Contractor SHALL actively retain transaction audit logs and provide auditing capabilities such as logging of information in an open accessible format around, but not limited to, changes to credentials or attributes, failed authentication attempts, security breaches, customer support transactions, etc. The Contractor SHALL clearly identify and ensure access to other logging capabilities, which would be beneficial to the Customer.

Security:

- The Contractor SHALL ensure that all aspects of the solution employs robust security and fraud detection and protections against threat outlined in NIST SP 800-63-3: *Digital Identity Guidelines,*[14] or the latest version thereof, or other security issues that may arise in the provision of these services and solutions. The Contractor SHALL fully and clearly describe their security capabilities and any limitations of their protection services.
- All communications between and within Identity, Credential, and Verification aspects of the solution SHALL be protected sufficiently to comply with the Customer's risk management as addressed in NIST Special Publication 800-63-3 (or current version thereof) and other applicable guidance such as NIST Special Publication 800-37 or 800-53.

[10] https://pages.nist.gov/800-63-3/sp800-63-3.html

[11] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf

[12] http://www.nascio.org/Publications/ArtMID/485/ArticleID/161/The-State-Identity-Credential-and-Access-Management-Guidance-and-Roadmap-SICAM

[13] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf

[14] https://pages.nist.gov/800-63-3/sp800-63-3.html

- The Contractor SHALL coordinate with the service providers identified to the appropriate extent to ensure that the identity management, credential management, and access management processes flow together resulting in the secure access of users to the desired resources.
- The Contractor SHALL fully and clearly describe the security capabilities of the end solution and any limitations on the security capabilities.
- When making any changes to the Customer's ICAM operations, the Contractor SHALL ensure all data exchanges between and within the Customer's ICAM systems SHALL be protected to the extent required by the Customer.
- The Contractor SHALL coordinate with the Customer to ensure that the identity management, credential management, and access management processes are integrated sufficiently to provide for the secure access of users to the desired resources.
- If the Customer's systems are interoperating with federal government information systems, all aspects of the solution and services provided SHALL be compliant with the security considerations in NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations.*[15]
- If the Customer's systems do not interoperate with federal government information systems, all aspects of the solution and services provided WILL be compliant to the greatest extent possible with the security considerations in NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organization.*[16] The Contractor may reasonably modify these requirements, so long as the modifications meet State security requirements of the State(s) in which the Customer is receiving or operating services and solutions. The Contractor SHALL specify the differences between its down-scoped set of requirements and Federal requirements if it chooses to modify these requirements.
- If the Customer's systems are interoperating with federal government information systems, all aspects of the solution and services provided SHALL be compliant with the security considerations in Federal Information Processing Standard (FIPS) Publication 140-2: *Security Requirements for Cryptographic Modules*[17] (or the latest version thereof) encryption standard and industry best practices.
- If the Customer's systems do not interoperate with federal government information systems, all aspects of the solution and services provided SHALL be compliant to the greatest extent possible with the security considerations in Federal Information Processing Standard (FIPS) Publication 140-2: *Security Requirements for Cryptographic Modules*[18] (or the latest version thereof) encryption standard and industry best practices. The Contractor may reasonably modify these requirements, so long as meet the State security requirements of the State(s) in which the Customer is receiving or operating services and solutions. The Contractor SHALL specify the differences between its down-scoped set of requirements and Federal requirements if it chooses to modify these requirements.

[15] http://csrc.nist.gov/publications/PubsSPs.html

[16] http://csrc.nist.gov/publications/PubsSPs.html

[17] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[18] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Privacy:

- All aspects of the solution SHALL be compliant with the privacy considerations in NIST SP 800-63-3: *Digital Identity Guidelines*, or the most current version thereof.
- If the Customer's systems are interoperating with federal government information systems, all aspects of the solution and services provided SHALL be compliant with the privacy considerations in M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, or any superseding privacy guidance.[19]
- If the Customer's systems do not interoperate with federal government information systems, all aspects of the solution and services provided WILL be compliant to the greatest extent possible with the privacy considerations in M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, or any superseding privacy guidance.[20] The Contractor may reasonably modify these requirements, so long as they still adequately protect user Personally Identifiable Information (PII), and meet the state privacy requirements of the state(s) in which the Customer is receiving or operating services and solutions. The Contractor SHALL specify the differences between its down-scoped set of requirements and Federal requirements if it chooses to modify these requirements.
- If the Customer's systems are interoperating with federal government information systems, all aspects of the solution and services provided SHALL be compliant with the privacy considerations in NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations* and comply with all applicable federal privacy laws and regulations.[21]
- If the Customer's systems do not interoperate with federal government information systems, all aspects of the solution and services provided WILL be compliant to the greatest extent possible with the privacy considerations in NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organization.*[22] The Contractor may reasonably modify these requirements, so long as they still protect user Personally Identifiable Information (PII), and meet the State privacy requirements of the State(s) in which the Customer is receiving or operating services and solutions. The Contractor SHALL specify the differences between its down-scoped set of requirements and Federal requirements if it chooses to modify these requirements.

Assurance Level:

- The solution SHALL be capable of providing Identity Management, Credential Management, and Verification services at the proper Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL) (as defined in NIST SP 800-63-3) specified by the customer to be **[insert levels of assurance necessary]** and SHALL ensure that services pass necessary audits as achieving such Assurance Levels for any applicable federation.

[19] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

[20] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

[21] http://csrc.nist.gov/publications/PubsSPs.html

[22] http://csrc.nist.gov/publications/PubsSPs.html

Data Rights:

- **If the Customer is a federal organization:** The Contractor SHALL agree to the policies and procedures regarding rights in data and copyrights and acquisition of data set forth in Subpart 27.4 – *Rights in Data and Copyrights* of the Federal Acquisition Regulation (FAR)[23]
- **If the Customer is NOT a federal organization:** The Contractor SHALL agree to the policies and procedures regarding rights in data and copyrights and acquisition of data set forth in Subpart 27.4 – *Rights in Data and Copyrights* of the Federal Acquisition Regulation (FAR)[24], and any reference to the Customer as a Federal Agency SHALL be interpreted to mean the appropriate designation of the Customer.

[23] https://www.acquisition.gov/?q=browse/far/27/4&searchTerms=data%20rights

[24] https://www.acquisition.gov/?q=browse/far/27/4&searchTerms=data%20rights

SECTION TWO: DEFINITIONS FOR A BASIC ICAM SOLUTION

Core Services and Solution Requirements for an ICAM System:

Identity Management Definition**:**

Identity management consists of the set of practices required to establish and maintain a digital identity over its lifecycle. The core practices required within identity management include:

- *Identity Proofing* – the ability to prove the identities of individuals to establish confidence that the individual is who they claim to be.
- *Identity Creation* – the ability to create a unique digital representation of an individual's unique identity including all necessary attributes.
- *Identity Maintenance* – the ability to maintain this digital representation over time to ensure the accuracy, integrity, and protection of the information it contains, reflecting any necessary changes or updates.
- *Identity Resolution* – the ability to identify duplicate digital identities.
- *Identity Deactivation* – the ability to terminate a digital representation of an individual's identity.

Credential Management Definition**:**

Credential management consists of the set of practices required to establish and maintain a credential over its lifecycle, and to provide authentication services for credentials. The core practices required within credential management include:

- *Credential Sponsorship* – the process of accepting a recommendation for an individual to be issued a credential.
- *Credential Registration* – the ability to register an individual and their associated digital identity to receive a credential.
- *Credential Issuance* – the ability to physically issue authenticators to individuals and bind an individual's digital identity to a credential.
- *Credential Maintenance* – the ability to maintain this credential over time to ensure the integrity and protection of the information it contains; the ability to prevent any fraudulent activity around the use of the credential; the ability to renew credentials and handle incidents pertaining to lost or compromised credentials.
- *Credential Revocation* - the ability to invalidate a credential.
- *Authentication* – the ability to validate the authenticity and status (i.e. current, expired, revoked) of and proof of possession of a credential as a means of verifying an individual's digital identity.

Access Management:

Access Management grants authorized users the right to use a service, while preventing access to non-authorized users.

Authorization is the adjudication of access requests; it determines whether the system's policies allow a user to perform a requested action and enforces the applicable policy.

The Contractor SHOULD include all of Customer's policies into the access management system to allow for automation, when possible.

Verification Definition**:**

Verification consists of the set of practices required to provide secure assertions that testify to an attribute of an individual or an authentication or authorization decision made by another party.

- *Assertions* –testify to an attribute of an individual or an authentication or authorization decision made by another party in a secure manner; can be trusted and understood by a Service Provider or Relying Party; and interoperate with the systems of a Service Provider or Relying Party.

Users:

- The solution SHALL be capable of providing Identity Management, Credential Management, Access Management, and Verification services to **[insert number of users]** users
- The solution SHALL be capable of providing Identity Management, Credential Management, Access Management, and Verification services to users in the **[insert the names of communities of users being served (e.g. state fire department, state law enforcement, etc.)]**
- The Contractor SHALL provide customer support capabilities for all aspects of their services and solutions where users may require support in interacting with or using their services and solutions. These support capabilities SHALL include, but will not be limited to, a call center, **[insert additional customer support capabilities or requirements]**

SECTION THREE: IMPLEMENTATION CONSULTANT/CONTRACTOR

Note: If the organization chooses not to join a federation, it could remove all references to Federations to obtain an ICAM-enabled system implementation.

Core Service and Solution Requirements:

Execution:

- The Contractor SHALL execute on the strategy outlined in the Transition Plan to fill the gaps, in the prioritized order, necessary for the Customer to align their current set of ICAM practices with the access requirements of the Federation(s).

Target State Analysis:

- The Contractor SHALL perform an analysis of the requirements for joining and becoming interoperable with the following Federation(s): [**insert names of Federations**]. The Contractor SHALL present this analysis in a Report of Findings.
- The Contractor SHALL develop a target state architecture for the Customer's Access Management capability that aligns with the requirements identified for joining the above Federations and SHALL present this analysis in a Report of Findings.

Gap Analysis:

- The Contractor SHALL perform a gap analysis comparing the Customer's As-Is state and the Customer's target state, and include the findings of this analysis in a Report of Findings.
- The Contractor SHALL determine the level of effort necessary to fill all the gaps that have been identified by the Contractor and, with the input of the Customer, prioritize these gaps for resolution.
- The Contractor SHALL develop a Transition Plan with specific identified policy and technical implementation, development and/or procurement steps to communicate the Contactor's strategy for addressing the prioritized gaps in the Customer's current ICAM practices.

Modification and Solution Prototyping:

- The Contractor with the input of the Customer SHALL prioritize gaps that need to be filled to enable to Customer to reach the target state.
- The Contractor SHALL develop a Customer-approved number of prototype solutions to fill the gaps that have been prioritized by the Customer.
- The Contractor SHALL perform pilots for each of these prototype solutions in a sequence approved by the Customer.
- The Contractor SHALL coordinate with the Federation to incorporate them in the pilots of these prototype solutions where necessary.

Supplemental Services:

- The Contractor SHALL provide supplemental services to the Customer covering any additional measures necessary the Customer must take to become an active member of the Federation(s) it aims to join. This may include, but is not limited to, legal agreements necessary for joining the Federation(s), and audits of the Customer's Access Management implementation to ensure compliance with Federation specifications.
- The Contractor SHALL support lifecycle / integration testing between, but not limited to, the Customer's Access Management implementation and Federation systems and applications.

Solution Requirements:

- The solution SHALL be capable of providing Identity Management, Credential Management, and Verification services and solutions as defined above.
- The Contractor SHALL guide the Customer through the all necessary legal agreements and SHALL advise the Customer throughout the process for identifying necessary documents and support Customer engagement with the Federation until the legal agreements are in place and the solution is operational.
- Identity:
    - The solution SHALL be capable of providing [**choose one or both: in-person and/or remote identity proofing**].
- Credential:
    - The authenticators provided by the solution SHALL consider all usability requirements of the users, and when necessary different authenticators will be provided to different users based upon their specific needs (e.g. Public Safety Grade, etc.).
        - **[insert specific usability requirements for authenticators]**
    - The solutions and services SHALL include the ability to provide multifactor authentication services.
- The Contractor SHALL have a comprehensive Service Level Agreement (SLA), with measurable objectives that are acceptable to the Customer, including proposed penalty or insurance offering should SLA's not be met. At a minimum, but not limited to, the SLA shall include measurements for assertion content accuracy, transaction speeds, usage, error reporting, and system availability.
    - **[insert Service Level Agreement]**
- The Contractor SHALL perform an analysis of the Customer's current Access Management implementation to determine the As-Is state. The purpose of this analysis SHALL be to determine to the Customer's requirements for access to their resources, so that these requirements may be later stated for information sharing with other organizations. This analysis SHALL include, but is will not be limited to, the following factors:
    - Policy – The standards/requirements documents that govern service provider (SP) practices.
    - Procedures – The procedures the SP follows to implement and adhere to policy.
    - Protocol – The communications method and interface between SP systems and partner systems.
    - Payload – The semantic and syntactic structure of the data exchanged between the SP and partner systems.
    - Infrastructure – The architecture and implementation of SP ICAM hardware and software.
    - Risk – The risks pertaining to the access or breach of SP resources or end-user personal information.
    - Security – The security measures necessary to protect SP resources and end-user personal information based on an assessment of risk.
    - Privacy – The privacy measures necessary to protect end-user privacy based on an assessment of risk.

- Access Policies – The rules around who can access which resources when.

Operationalization:

- The Contractor SHALL identify all necessary legal agreements and the guide the Customer through the process for engaging with the federation. The Contractor SHALL carry out portions of this process where direct Customer participation is not necessary when approved by the Customer.
- The Contractor SHALL guide the Customer through the process of installing all necessary processes, procedures, hardware, and software components to operationalize their Federation. The Contractor SHALL carry out portions of this process, where feasible, to reduce the level of effort required of the Customer.
- The Contractor SHALL support lifecycle / integration testing between the Customer's ICAM operations, and any additional partner systems necessary to demonstrate that the desired capabilities are operational and identify any changes that must be made to reach an operational state.

Additional Advisory Services:

- The Contractor SHALL guide the Customer through the process of installing all necessary processes, procedures, hardware, and software components to operationalize its infrastructure. The Contractor SHALL carry out portions of this process and, where feasible, reduce the level of effort required of the Customer.
- The Contractor SHALL perform all additional work necessary to ensure that the Customer's implementation of ICAM operations enable them to access the resources desired by the Customer.
- The Contractor SHALL support lifecycle/integration testing between the Customer's ICAM operations, and any additional partner systems necessary to demonstrate that the desired capabilities are operational and identify any changes that must be made to reach an operational state.

SECTION FOUR: AUTHORITATIVE ATTRIBUTE SERVICE (AAS)

Service Specifications for an Authoritative Attribute Service (AAS):

Definitions:

Authoritative Attribute Service (AAS):

After a user has been authenticated, and their identity confirmed, they must be authorized to access the resources they seek. In role-based access controls (RBAC) and attribute-based access controls (ABAC), an authorization engine requires access to attributes that describe users and resources —and potentially attributes describing the user's or resource's computing environment—being accessed to make an authorization decision. The engine compares these attributes to a set of policies that govern access to a resource dependent on a given set of attributes. Access is either provisioned or denied based on the attribute profile of the requestor. The source of the user attributes in this scenario is an Authoritative Attribute Service (AAS).

Since these attributes may be stored across many different systems, it is the role of the AAS make these attributes available to the authorization engine. Many of these attributes may also contain sensitive Personally Identifiable Information (PII) about the user that must be protected.

The following are the core activities performed by an AAS:

- Authoritative Attribute Identification – Identifies the authoritative sources of user attributes.
- Privacy – Protects the privacy of end-users' PII through masking and assertion mechanisms, sending actual attribute values only when absolutely necessary, and otherwise passing claims about those values.
- Attribute Sharing – Makes all necessary authoritative attribute sources available to the authorization engine either through aggregation or redirects to the authoritative sources themselves.

As-Is Analysis:

- The Contractor SHALL perform an analysis of the Customer's current Access Management implementation to determine the As-Is state and develop a Report of Findings based on the results of this analysis. This analysis SHALL include, but is not limited to, the following factors:
    - Risk – The risks pertaining to the access or breach of SP (or federation member) resources or end-user personal information.
    - Security – The security measures necessary to protect SP (or federation member) resources and end-user personal information based on an assessment of risk.
    - Privacy – The privacy measures necessary to protect end-user privacy based on an assessment of risk.
    - Access Policies – Existing rules around who can access which resources when and what attributes are necessary to enforce these access policies.
    - Infrastructure – The architecture and implementation of SP (or federation) ICAM hardware and software.
    - Protocols – The communications methods and interfaces between SP (or federation member) systems and partner systems used during Access Management.

- This analysis MAY include, the following factors:
    - Policy – The standards/requirements documents that govern SP (or federation if applicable) practices.
    - Procedures – The procedures the SP (or federation if applicable) follows to implement and adhere to policy.
    - Payload – The semantic and syntactic structure of the data exchanged between the SP (or federation member) and partner systems.

Attribute Analysis:

- The Contractor SHALL perform an analysis of the attributes necessary to implement the authorization capability to determine:
    - The user and resource attributes required for access to the Service Providers included in the scope of this solution.
    - The authoritative sources of the required user attributes and resources attributes.
    - The accessibility of the authoritative sources of required user attributes and resource attributes.
- In collaboration with the Service Providers included in the scope of this authorization solution, the Contractor SHALL identify the policies and business rules regarding access to resources, develop those policies and rules into a set of machine-executable Access Policies (if such policies do not already exist and meet the necessary requirements) to map out the logic behind the authorization capability. Where possible, attributes will be re-used to minimize the attributes necessary for any given access decision.
- The Contractor SHALL develop a blueprint for the AAS capability to map out necessary communications between systems that must occur to stand up this capability.

Target State Analysis:

- The Contractor SHALL develop a target state architecture for the Customer's Access Management capability that aligns with the requirements identified for joining the above federations and SHALL present this analysis in a Report of Findings.
- The target state SHALL minimize cost to the Customer and reduce requirements for operations and maintenance where feasible.

Gap Analysis:

- The Contractor SHALL incorporate the findings from the As-Is analysis, Target State analysis, and Attribute analysis to determine the gaps stand in functionality that must be filled to realize the target state solution.
- The Contractor SHALL prioritize the gaps that need to be filled to enable to Customer to reach the target state.

Solution Prototyping:

- The Contractor SHALL develop a Customer approved number of prototype solutions to fill the gaps that have been prioritized by the Contractor.
- The Contractor SHALL perform pilots for each of these prototype solutions in a sequence approved by the Customer.

- The Contractor SHALL coordinate with the owners of all partner systems to incorporate them in the pilots of these prototype solutions where necessary to demonstrate a fully functional target state capability.

Solution Adoption:

- After prototyping and piloting the authorization solution, the Contractor SHALL install a fully functional target state authorization capability that interoperates with all necessary partner systems and meets all Customer requirements.
- The solution SHALL be fully interoperable with all necessary authentication capabilities to enable a complete access transaction (including authentication and authorization) for users.

Supplemental Services:

- The Contractor SHALL provide training in the operation of the solution for all necessary stakeholders

ABAC Specific Requirements:

- As a baseline of needs, the Attribute Based Access Control (ABAC) solution must be capable of implementing ABAC for generating and enforcing externalized access control policy decisions as described in the latest version of NIST SP 800-162: *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.[25]
- The ABAC model combines user attributes, resource metadata, environmental attributes, and access control policy defined at various levels of the enterprise. The ABAC solution must support interoperability between separate systems within the scope of the Customer's enterprise, and must be capable of federation with other Service Providers as mandated by the Customer.
- The required support services include working with the Customer to support the integration of the proposed ABAC solution and providing input into standard configuration guidance, test documentation, and test procedures. The contractor shall also provide engineering, system architecture, security, and maintenance support for the ABAC solution. The ABAC solution must use standards that will work across multiple autonomous Customer systems and be interoperable with external federal agencies and other public safety partners as defined by the Customer. The ABAC solution shall have the following capabilities:

ABAC Capabilities:

- The solution SHALL support an ABAC model which utilizes user, resource, and environmental attributes as input to an access policy evaluation engine to grant or deny access to a requested resource.
- The solution SHALL have a component(s) identified as a Policy Administration Point (PAP) or Policy Enforcement Point (PEP), which provides a user interface for creating, managing, testing, and debugging Digital Policies as well as storing these policies in the appropriate repository.
- The solution SHALL have a component identified as a Policy Decision Point (PDP) to evaluate digital access control policies and render access control decisions.

[25] http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

- The solution SHALL have a component identified as a Policy Information Point (PIP[26]) that acts as a source for the attribute values describing the subject, the resource, and the environment that is required to render an access decision.
- The solution SHALL retrieve user attributes from one or more external attribute sources (which can also be considered PIPs).
- The solution SHALL provide a mechanism for managing access control policies. Although a Graphical User Interface (GUI) is preferred, at a minimum a mechanism that supports Policy creation, modification, deletion, as well as Policy import and export is required.
- The solution SHALL provide a mechanism for logging and auditing all its operations including the behavior of the access control solution as well as access activity, policy edits, configuration changes, etc.

Architectural Interfaces and Specifications:

- The solution SHALL accommodate fine-grained authorization decisions per database. If an application performs fine-grained authorization internally, it SHALL do so using non-proprietary Digital Policy language. If an application does not perform fine-grained authorization internally, it SHALL enforce authorization decisions from an external PDP.
- The solution SHALL support web service protocols such as Representational State Transfer (REST), Simple Object Access Protocol (SOAP), and other OASIS-specified Web Services frameworks (as appropriate: e.g., Web Services Resource Framework (WSRF), WS-Security, or WS-Interoperability).
- The solution SHOULD ingest non-proprietary Digital Policy or Metapolicy rules written in open standards, as defined in NIST SP 800-162.
- The solution SHOULD support at least one open standard for describing and exchanging security assertions between parties.
- To support attribute-based access control, the solution SHALL request and retrieve attributes of the subject identified in the access request.
- The solution SHALL support the secure retrieval of attributes, such as using the LDAP-S protocol or SQL.
- The solution SHALL support at least file-level access control. It shall support the marking and tagging of files, documents, and data either directly or through integration with a 3rd party product.
- The solution SHALL support translation of Digital Policy or Metapolicy rules, PDP determinations, or security assertions provided in other open standards into the standards used for ingestion into or export from the solution.

[26] The Policy Information Point (PIP) can often also be referred to as an Authoritative Attribute Source (AAS). The PIP/AAS may be a source that is not internal to the customer. For instance, a PIP that complies with this requirement may be hosted by DHS to serve a user attribute regarding completion and date of required training, but from which the Contractor solution is capable of retrieving and applying the attribute.

Vendor Services:

- The solution SHALL include analysis/design consulting services.
- The solution SHALL include support in the deployment and operation of the access control solution.
- The solution SHALL include vendor provided product training.
- The solution SHALL include support for development of internal Digital Policy or Metapolicy rules or the translation of external Digital Policy or Metapolicy rules into a format supported by the solution