U.S. General Services Administration

Identity, Credentialing, and Access Management (ICAM)

Solutions and Shared Services

Roadmap

Record of Changes

VERSION NO.	DATE REVISED	SUBMITTER	SECTION/PAGE NUMBER/DESCRIPTION OF CHANGE
1	NOV 12, 2020	GSA FAS/ITC IDENTITY MANAGEMENT TEAM	INITIAL DRAFT

NOTE: This document is subject to information updates and changes. The use of this Record of Changes table helps manage document modifications throughout the life of this document. All attempts have been made to ensure the accuracy of the information within this document as of the initial distribution date.

Any subsequent adjustments should be logged and coordinated with the author.

Table of Contents

Executive Summary

This document provides a response to the Office of Management and Budget (OMB) memorandum M-19-17, "*Enabling Mission Delivery through Improved Identity, Credential, and Access Management*." The memorandum outlines the federal government's Identity, Credential, and Access Management (ICAM) policy and establishes Government-wide responsibilities that include the General Services Administration (GSA). GSA is specifically tasked with developing and maintaining "a roadmap for providing or updating GSA solutions and shared services that allow agencies to achieve the outcomes in OMB ICAM policy and NIST standards and guidelines." GSA analyzed the current state of ICAM solutions and shared services, and developed activities to address identified gaps based on the ICAM Services Framework.

The roadmap aligns actions to the following three phases:

- **Foundation** focuses on modifications to the existing services catalog to address critical gaps.
- **Federation** focuses on enhancing federation capabilities for government to government, government to constituent, and government to mission partner interactions.
- **Emerging Trends** focuses on recognizing and preparing for emerging trends and expanding support.

The roadmap also identifies five areas that align with GSA's vision:

- **Guidance** provided to agencies for best in class ICAM implementation.
- **Coordination** with organizations to ensure that solutions support ICAM policy, minimize duplication of effort, and verify that agency needs are being met.
- **Acquisition Support** to maintain and update contract vehicles to support agency ICAM needs.
- **Shared Services** provided rather than each agency duplicating efforts.
- **Third-Party validation** for vendors offering ICAM related services.

The table on the next page provides a summary of the roadmap activities. This roadmap is considered a living document; this first iteration is designed to gain leadership support and endorsement. Foundation activities are targeted for completion in the next one to two years. Federation activities are targeted for three to four years. Emerging trend activities are likely to require more than four years to complete, as they may depend on earlier phase activities or require further definition before they can begin.

	FY21-23 Phase One Foundation	FY23-25 Phase Two Federation	FY25 & Beyond Phase Three Emerging Trends
Guidance	● Update the FICAM Architecture and FICAM Services Framework ● Refresh the FICAM Roadmap ● Provide guidance for agency OLT CA	● Establish a capability to create and share best practices	● Maintain the FICAM Architecture and FICAM Services Framework ● Maintain the FICAM Roadmap
Coordination	● Identify existing contracting vehicles ● Identify policy gaps for use of mission partner credentials ● Establish collaboration mechanisms ● Identify and resource projects for implementing the FICAM Architecture	● Address policy gaps for use of mission partner credentials ● Prioritize deliverables for the best practices group ● Maintain collaboration mechanisms ● Update this roadmap to better support agency needs	● Identify emerging technologies that impact the FICAM Services Framework ● Identify contracting vehicles, shared services, and vendor validations needed to support emerging technologies
Acquisition Support	● Implement FICAM Services Framework profile under ICAM SIN ● Develop playbook for contract officers and contract specialists ● Develop playbook for agency ICAM buyers	● Develop SIN for best-in-class ICAM services, ICAM tools, and ICAM SaaS cloud solutions	● Update contracting vehicles to support emerging technologies
Shared Service	● Modernize the FPKI trust infrastructure ● Improve USAccess ● Enhance Login.gov ● Provide publicly trusted web server certificates	● Implement service to provide suitability status ● Implement organizational signature service ● Provide support for validating mission partner credentials ● Implement an Identity Provider (Id) authentication service	● Implement cloud services to support non person entity (NPE) ● Evaluate demand and feasibility for implementation of an attribute mapping service
Third-Party Validation	● Establish criteria for validating third party ICAM	● Design and implement validation process for third	● Begin validating third party providers.

	services	party providers	

1.0 Introduction

On May 21, 2019, the Office of Management and Budget (OMB) released M-19-17, "*Enabling Mission Delivery through Improved Identity, Credential, and Access Management*," which "sets forth the federal government's Identity, Credential, and Access Management (ICAM) policy." The policy recognizes the progress that has been made in reaching the goal of a "federal standard for secure and reliable forms of identification" identified in Homeland Security Presidential Directive (HSPD) 12, but identifies a continuing need to use "identity as the underpinning for managing the risk posed by attempts to access federal resources made by users and information systems." The policy identifies specific activities that federal agencies must undertake in governance, architecture, and acquisition to harmonize the government's enterprise-wide approach to ICAM.

1.1 Responsibilities

M-19-17 identified the following responsibilities:

- OMB is responsible for overall budget development and execution, oversight of agency performance and information technology.
- ICAM Subcommittee provides a government-wide organization to encourage collaboration and cooperation across agencies.
- NIST is responsible for establishing standards for many of the technology and process aspects of ICAM.
- The Department of Homeland Security (DHS) has cybersecurity responsibilities encompassing knowing who is on the network.
- GSA provides shared acquisition vehicles to obtain ICAM technology and professional services, and also provides shared services that can be used by agencies that do not have to recreate them on their own.
- Every Department and Agency is responsible for implementing ICAM both to protect information resources against unauthorized access but also to ensure that these same information resources are accessible by government, business, and constituent users who are authorized to access them.

1.2 Purpose

OMB M-19-17 assigned GSA to: "develop and maintain…a roadmap for providing or updating GSA solutions and shared services that allow agencies to achieve the outcomes in OMB ICAM policy and NIST standards and guidelines." This document presents the current state

of maturity and implementation of federal government ICAM solutions, describes the challenges in the current ICAM environment, and lays out a roadmap for GSA to provide acquisition vehicles and government-wide services to assist agencies in achieving ICAM objectives defined by OMB and NIST.

Although this roadmap primarily focuses on the steps and actions GSA will take to provide solution offerings that enable agencies to efficiently and cost-effectively implement ICAM solutions aligned with OMB M-19-17, it also identifies areas of collaboration between GSA and other agencies supporting ICAM.

1.3 Background

The Federal Identity, Credential, and Access Management (FICAM) architecture[1] defines ICAM as “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. ICAM is the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. These resources may be electronic files, computer systems, or physical resources such as server rooms and buildings.” The FICAM Architecture defines a robust, scalable framework, equally useful to enterprise architects developing their agency’s ICAM program and to those new to ICAM who are learning its core concepts. It depicts principles and practices in the form of diagrams and stories to describe what ICAM is, what it should do, and what is used to provide capabilities to an agency. .

Figure 1 provides a conceptual view of the FICAM Services Framework from the FICAM Architecture with the following practice areas:

- Identity Management is how an agency uses attributes to establish and maintain enterprise identities for employees and contractors.
- Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context.
- Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.
- Governance is the set of practices and systems that guides ICAM functions, activities, and outcomes.

[1] arch.idmanagement.gov

- Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.

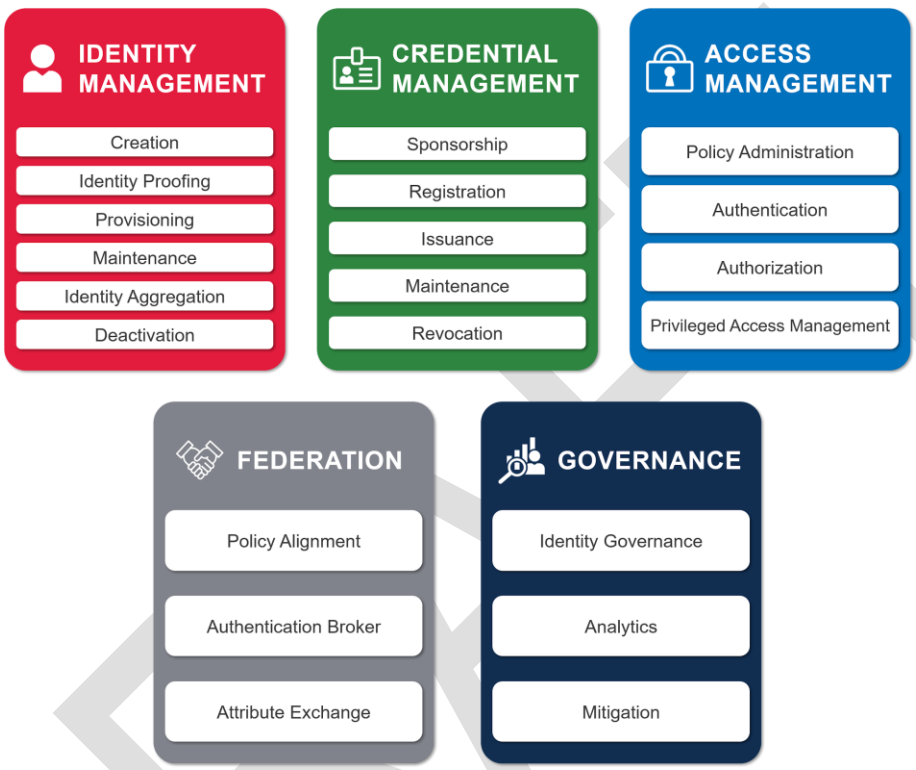

Figure 1.0: FICAM Services Framework

2.0 ICAM Challenges

Deploying ICAM solutions within an agency is complex, as ICAM touches all users across the organization. Also, ICAM capabilities must interoperate with legacy systems that do not support modern standards and be flexible enough to support evolving standards, technologies, and policies. Because ICAM cuts across numerous offices, programs, and systems within an agency's enterprise that are typically directed and managed separately, successful implementation of enterprise ICAM solutions within an agency requires

implementing governance structures that encourage collaboration and cooperation across disparate lines of authority.

Consistently deploying ICAM solutions across agencies that meet common standards and support inter-agency information sharing has also proven to be challenging. As stated in Section 1, different agencies are responsible for different aspects of ICAM. Although ICAM challenges are common, different agencies have taken different approaches to ICAM implementation.

Government-wide shared services have the potential to enhance functionality and save money by investing once to implement capabilities that can then benefit all agencies. However, providing government-wide solutions for ICAM is itself a challenge because the solutions must align with the vision and needs of multiple organizations within the ICAM community while meeting schedule goals within cost constraints.

Determining what ICAM capabilities should be standardized, what capabilities should be shared across the government, and what capabilities should be developed and implemented by individual agencies will be critical as the focus shifts beyond credentials to include identity management and access management. The successful implementation of shared services requires addressing the following considerations:

- Establishing executive level collaboration across the government
- Working with the Shared Solutions Governance Board (SSGB) to determine the potential benefits of operating the service as a shared service
- Collaborating with the OMB designated Quality Service Management Office (QSMO) for Cybersecurity Services to promote standardization, reduce duplication, reduce operating costs, and increase customer satisfaction for government-wide shared ICAM services
- Implementing an agency-wide governance process to identify and define shared services that can be leveraged across all agencies, to provide a mechanism for collecting and prioritizing requirements for service capabilities, and to assign the operation of each shared service to an appropriate agency
- Identifying an equitable mechanism for resourcing and funding needed for development, operations, and maintenance of the shared service

3.0 ICAM Gaps

This roadmap was developed to address gaps identified using a step by step methodology as follows. The ICAM Catalog, released in August 2019, served as the starting point for the gap analysis.

The following table summarizes identified gaps in each of the five FICAM Services Framework areas, along with general gaps.

Area	Gaps
Identity Management	● Identifying and procuring identity management tools and professional services is difficult using current contract vehicles ● NIST SP 800-63 compliant remote or supervised remote identity proofing services do not exist ● Methods for determining identity of constituents interacting with government services have been inconsistent ● Agencies have limited ability to determine suitability status of PIV cardholders across agencies
Credential Management	● Identifying and procuring credential issuance capabilities and professional services beyond PIV Shared Service Providers is difficult, including non-PKI credentials and public facing website TLS certificates ● Credential issuance and management for non-person entities is not well defined or supported and will be needed to support Zero Trust Architecture (ZTA) initiatives
Access Management	● Authentication to cloud based Software as a Service (SaaS) is not well defined or supported ● Managing access for constituent users and other customers is not well supported ● Capabilities to implement dynamic access control are not defined or supported, including data tagging, development of digital policy rules, attribute management, and operation of policy decision points ● NIST Special Publication 800-63-3 defines federation assurance levels for transmitting assertions from an identity provider, but it does not identify minimum requirements for secure operation of the identity provider itself ● Tools to manage physical access for visitors are not available ● Support for key access management capabilities including provisioning, de-provisioning, and access rules is lacking
Federation	● Modernized tools for managing trust stores to appropriately trust mission partner PKIs are not available ● Federated identity provider services provided by login.gov and max.gov are limited in their ability to provide robust assertions to agency applications authentication

Governance	● Contracting vehicles for professional services with expertise in assisting agencies with developing and deploying ICAM governance are lacking
General	● There is no overarching federal government ICAM maturity model that agencies can use to gauge where to focus efforts in improving their ICAM capabilities ● Identity enabled services such as electronic or digital signatures, key management, and email signature and encryption, are not consistently deployed

4.0 ICAM Solutions and Services Roadmap

Existing GSA government-wide acquisition vehicles and shared services are primarily focused on identity management and credential management, specifically around the issuance of PIV cards. Achieving the objectives of OMB Memo 19-17 will require a broader set of solutions that expand the focus of identity and credential management beyond PKI and that support access management. This GSA ICAM Solutions and Services Roadmap aligns activities to three phases. Foundation activities are targeted for completion in the next one to two years. Federation activities are targeted for three to four years, and emerging trend activities are likely to require more than four years to complete. All activities follow these three guiding principles.

1. Make It Easy to Use and Understand – Focus on customer experience. Ensure the acquisition process and how services are marketed is easy to understand.

2. Know our Customers and Know Their Needs – Customers must be engaged consistently to ensure the acquisition process, products, and services meet current and emerging needs.

3. Best in Class - Offer acquisition/procurement solutions reflecting industry best practices and appropriate government oversight.

This roadmap provides activities in five focus areas aligned with GSA's vision to provide effective and efficient government for the American people.

- Guidance – GSA is responsible for maintaining the FICAM architecture, and will continue to provide guidance to agencies to agencies for best-in-class ICAM implementation.

- Coordination – As described in Section 1, responsibilities for ICAM implementation are spread across multiple organizations. GSA will coordinate with these organizations to ensure that solutions support ICAM policy, minimize duplication of effort, and verify that agency needs are being met.
- Acquisition Support – One of GSA's core missions is to provide contracting vehicles to support agencies in acquiring tools and services including ICAM solutions. GSA will maintain and update contract vehicles to support agency ICAM needs.
- Shared Services – The federal government can more efficiently implement some ICAM solutions through the implementation of centralized shared services rather than each agency developing similar solutions individually. GSA will coordinate with agencies to identify these services, then coordinate with OMB to determine how centralized services can be executed.
- Third-Party Validation – Although most ICAM products and professional services meet industry standards, there is currently no mechanism to ensure they meet federal government requirements. GSA will work with NIST to identify and implement processes to validate vendor services that perform ICAM-related functions.

ICAM supports multiple agency needs for information sharing and safeguarding. Agencies must support access management for federal government users, both within and across agencies; coordinate with mission partners from state, local, and tribal governments as well as commercial industry; and provide information and other resources to constituents. Recognizing these needs, each activity in the roadmap is flagged to identify which of the following groups of users is supported by the activity.

Agency – these activities support federal agency implementation of ICAM within the agency and between agencies, including interactions with contractors who are issued PIV credentials.

Citizen – these activities support interactions between federal agencies and constituents.

Partner – these activities support interactions between federal agencies and mission partners including commercial businesses and state and local government agencies that use federated credentials to interact with federal agencies.

4.1 Phase One – Foundation

The activities in the first phase of the roadmap build on the existing services catalog to address critical gaps and lay the foundation for enhanced ICAM solutions in Phase Two.

Guidance

Update the FICAM Architecture and its associated FICAM Services Framework to define common terminology for all areas of ICAM, and to provide clear guidance to agencies in ICAM services. Develop playbooks to supplement the architecture and provide best practices in areas such as procuring ICAM tools, managing entitlement provisioning, deploying non-PIV credentials including derived PIV, and establishing fine-grained access policies. [OMB M-19-17 GSA action #3]

Refresh the FICAM Roadmap to align with the FICAM Architecture and incorporate an ICAM maturity model to assist agencies with gauging, measuring, and planning for FICAM modernization and enhancement. Align the maturity model with executive strategies such as the National Cyber Security Strategy or the National Strategy for Information Sharing and Safeguarding. [OMB M-19-17 GSA action #3]

Publish guidance to assist agencies in transitioning between PKI Shared Service Providers for their PIV issuance. [OMB M-19-17 GSA action #6]

Provide best practices for agency operation of Only Locally Trusted (OLT) Certification Authorities to support internal non-person entity needs. [OMB M-19-17 GSA action #3]

Coordination

Coordinate with DHS Cybersecurity and Infrastructure Agency (CISA) to identify contracting vehicles for ICAM products and services related to CDM and identify gaps. [OMB M-19-17 GSA action #5]

Mature and coordinate with OMB to identify policy gaps regarding the use of high assurance mission partner credentials in conjunction with government adjudicated suitability checks for access to agency resources. [OMB M-19-17 GSA action #6 & 7]

Leverage the ICAMSC to establish a coordination process for agencies to collaborate on defining ICAM needs and sharing best practices. [OMB M-19-17 GSA action #3]

Coordinate with NIST to identify and resource National Cybersecurity Center of Excellence (NCCoE) projects to explain and demonstrate how to implement the FICAM Architecture.

Acquisition Support

Leverage the FICAM Services Framework to implement a profile under the existing ICAM SIN that links disparate ICAM services to a specific FICAM Services Framework element. [OMB M-19-17 GSA action #5]

Develop a playbook for Contract Officers and Contract Specialists assigned to ICAM SINs on ICAM terminology and the FICAM Services Framework. [OMB M-19-17 GSA action #1]

Coordinate with DHS to develop a playbook for agencies buying GSA ICAM solutions on the procurement process.

Shared Services

Modernize the Federal PKI trust infrastructure to better support commercial standards and implementation mechanisms for PKI federation by establishing appropriate Root Certification Authorities and implementing a PKI trust store management service that agencies can use to automatically add or remove Federal or commercial PKI certificates from Agency desktop or mobile configurations. [OMB M-19-17 GSA action #6]

Improve the USAccess program for PIV card issuance to minimize service outages, address agency requirements, and support the issuance of PIV, PIV-I, and derived PIV

credentials. [OMB M-19-17 GSA action #6]

Enhance Login.gov to act as a federation service that can perform direct authentication of both government and commercially-issued credentials for constituents and provide assertions to government-managed web servers or cloud service providers. [OMB M-19-17 GSA action #6]

Provide publicly trusted web server certificates to agencies for use in externally facing web sites. [OMB M-19-17 GSA action #6]

Third-Party Validation

Coordinate with NIST to establish criteria for validating third-party ICAM services including identity proofing, credential issuance, and generation of identity assertions.[OMB M-19-17 GSA action #5]

4.2 Phase Two – Federation

Phase Two activities build on the foundation established in Phase One to enhance federation capabilities for government to government, government to constituent, and government to mission partner interactions.

Guidance

Coordinate with the Federal CIO Council, NIST, and DHS to establish a capability to create and share best practices. Contribute a Knowledge Management Specialist, Solutions Architect, and an ICAM Contracting Subject Matter Expert (SME) to generate white papers and technical encompassing the critical information needed to architect and purchase ICAM Solutions. The Solutions Architect will be available to all agencies to help architect the ICAM Solutions. The ICAM Contracting SME will advise agencies on developing the statement of work and the acquisition strategy. The Knowledge Management SME will review vendor white papers on the website, and ensure the

information is current. [OMB M-19-17 GSA action #3]

Coordination

Coordinate with OMB to address policy gaps and provide guidance for accepting mission partner credentials through federated solutions that enhance security while reducing cost to federal agencies.

Coordinate with the Federal CIO Council ICAM subcommittee, DHS, NIST and OMB to establish and prioritize deliverables for the FICAM best practices group established in Phase One. [OMB M-19-17 GSA action #6]

Maintain the process for agencies to collaborate on defining ICAM needs and sharing best practices. [OMB M-19-17 GSA action #1]

Leverage the coordination process to update the activities in this roadmap annually to better support agency needs. [OMB M-19-17 GSA action #1]

Acquisition Support

Develop a SIN for a best-in-class vehicle for obtaining ICAM solutions, including professional services, tools, and SaaS cloud solutions. [OMB M-19-17 GSA action #1 & 4]

Shared Services

Implement a shared service that provides the continuous monitoring for suitability status of PIV cardholders and other mission partners.

Implement a government-wide service for agencies to digitally sign organizational-level issuances that can be validated inter-agency and by mission partners and constituents.

Provide technical support for validating mission partner credentials to provide cost savings and efficiencies for federal agencies in accepting federated business partner credentials.

Implement an Identity Provider (Id) authentication service to act as a federation hub for agency to agency transactions using PIV, derived PIV, and other multi-factor authentication credentials leveraging max.gov or another service. [OMB M-19-17 GSA action #5 & 6]

Third-Party Validation

Collaborate with NIST to design and implement a validation process for third party provided ICAM services [OMB M-19-17 GSA action #4]

4.3 Phase Three – Emerging Trends

Phase Three continues the roadmap by addressing emerging trends such as enhanced support for non-person entity ICAM.

Guidance

Maintain the FICAM Architecture and Roadmap and update as necessary to address emerging trends and best practices. [OMB M-19-17 GSA action #3]

Coordination

Coordinate with NIST, DHS, and other agencies to identify emerging technologies (e.g., Zero Trust Architecture, Robotic Process Automation, Blockchain, 5G) that may either require alignment and integration with the FICAM Services Framework or new technologies that might meet FICAM requirements in the future. [OMB M-19-17 GSA action #1 & 7]

Coordinate with Federal CIO Council and Agencies to identify contracting vehicles, shared services, and vendor validation capabilities needed to support emerging technologies. [OMB M-19-17 GSA action #5]

Acquisition Support

Update contracting vehicles as required to support emerging technologies. [OMB M-19-17 GSA action #1]

Shared Services

Implement shared services as appropriate to support ICAM for non-person entities as agencies implement initiatives such as zero trust, robotic process automation, and internet of things. [OMB M-19-17 GSA action #1 & 5]

Evaluate demand for and feasibility of implementation of an attribute mapping service that identifies which attributes and values are available from which federal agencies for a specified population. [OMB M-19-17 GSA action #5 & 6]

Third-Party Validation

Begin validating third party providers. Provide mechanisms for feedback and update as needed.

5.0 Conclusion

Achieving the activities defined in this roadmap will provide federal agencies with the tools and processes they need to implement the requirements of OMB Memorandum M-19-17. For example, agencies are required to establish agency-wide governance for ICAM, including a formal governance structure and a comprehensive ICAM policy, process, and technology solution roadmap that aligns with the FICAM Services Framework, CDM, and NIST SP 800-

63-3. The guidance activities identified in this roadmap will result in an updated FICAM Services Framework and align guidance with CDM, which will assist agencies in developing their agency governance.

M-19-17 also directs agencies to establish and implement authoritative solutions for ICAM services that are interchangeable and commercially available, and support federated solutions for mission and business partners. Coordination activities are focused on implementing processes for agencies to collaborate and share best practices. The shared service activities identified in this roadmap will help agencies in standardizing ICAM capabilities. Additionally, the shared service activities will support agency needs for credential issuance, federation, and access control. Agencies are required to issue both PIV credentials and interoperable derived PIV credentials with alternative form factors to support the use of PIV and derived PIV credentials for physical and logical access to agency resources. Use of shared services will help minimize costs and streamline processes needed to implement and maintain credential issuance, federation, and access control.

A fundamental goal of ICAM is to improve the trust and safety of transactions with the public and allow federated authentication of federally or commercially provided credentials that comply with NIST guidance. This goal is supported by shared services as well as third party validation activities. The third party validation activities will not only ensure that commercial ICAM tools and services are consistent with federal government laws and regulations but agencies receive the highest level of service.

Lastly, agencies are required to comply with HSPD-12 and FIPS-201 for affected contractor personnel. Agencies are also required to use best in class contract vehicles that comply with OMB policy and NIST standards and technical specifications. By revamping contracting vehicles as described in the acquisition support activities in this roadmap, GSA will continue to be an active partner in supporting agency needs for obtaining ICAM related tools and services.