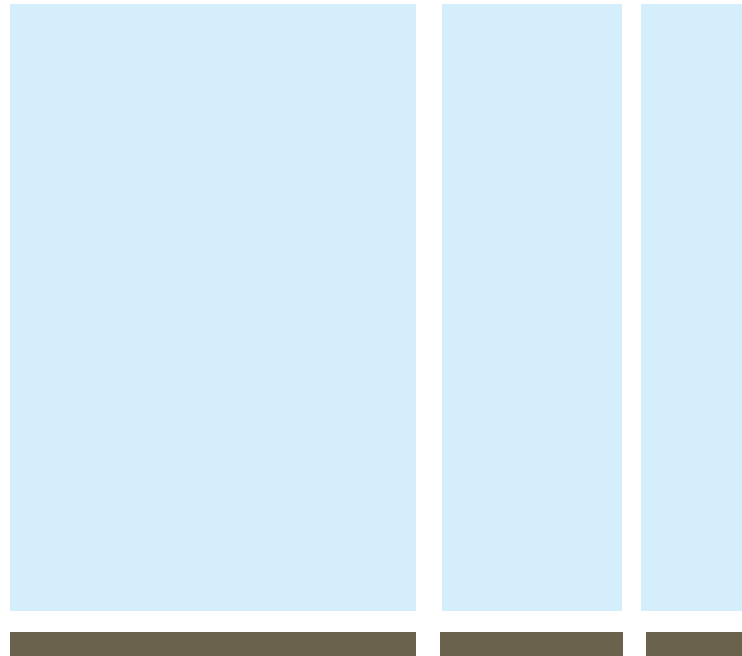


# UNDERSTANDING FEDERAL IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT (FICAM)



A look at the FICAM program, funding availability and steps to creating an implementation plan.

The United States government faces widespread security threats from criminals and terrorists in the form of data breaches, identity theft, unauthorized access to secure facilities and more. Combating these threats has become increasingly difficult due to the disparate security systems and protocols used across government agencies. Recognizing the need for a comprehensive, holistic approach to security, the federal government is moving forward with initiatives designed to standardize Identity, Credential and Access Management (ICAM) activities.

The key organization charged with aligning federal ICAM (FICAM) activities is the Identity, Credential and Access Management Subcommittee (ICAMSC). This subgroup of the government's Chief Information Officers (CIO) Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing and performance of federal government agency information resources.



SECURITY

## “ICAM represents the intersection of digital identities (and associated attributes), credentials and access control into one comprehensive approach,” according to the Federal Chief Information Officers (CIO) Council. <sup>(1)</sup>

The ICAMSC has developed a roadmap document titled: “Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.” It provides implementation guidance for common FICAM initiatives across the federal government. This document will help government agencies foster effective policies and enable trust across organizational, operational, physical and network boundaries. It sets formal policies and one comprehensive management approach related to FICAM to boost security, advance compliance, improve accessibility between agencies and enhance efficiencies agency wide.

This paper will define the goals and objectives of the FICAM initiative, address the availability of funding to help agencies implement FICAM policies and outline the appropriate steps to follow when developing a comprehensive FICAM implementation plan to comply with federal policies.

### FICAM Defined

According to the ICAMSC, “ICAM represents the intersection of digital identities (and associated attributes), credentials and access control into one comprehensive approach.” <sup>(1)</sup>

The activities associated with managing identities, credentials and access control are highly interconnected. A digital identity refers to a collection of data, commonly biographic and biometric elements, from an individual that is stored electronically as a representative record of that individual. Data associated with a digital identity may include identity attributes, such as height, weight and eye color; biometrics, such as fingerprints, iris scans and voice recognition; and biographical data, such as an address, phone number and e-mail address. Federal agencies use digital identity characteristics to develop credentials for individuals, including employees, contractors and visitors. Credentials are objects, such as passwords, digital certificates and identification cards, that individuals must present to authenticate their identities when using physical access control systems (PACS) or logical access control systems (LACS) to gain access to physical and logical (information systems) assets.

Digital identity information collected across the federal government, and even within individual agencies, is far from standardized. For example, one department within an agency may collect biometric and biographical data, and another agency department may only collect biographical data. An employee of the second department will encounter difficulties when interacting with the first department if biometric data is required to authenticate his or her identity when using a PACS or LACS system. That employee will need to undergo additional processing by the first department to update his credential and enable usage. This activity takes time, adds expense and decreases employee productivity. The FICAM initiative strives to eliminate such inefficiencies by standardizing digital identity processes across all departments of an agency – and the government as a whole. In this case, the agency’s FICAM solution may be to redefine the employee onboarding process to ensure that all relevant employee data is collected agency wide, regardless of the department.

Digital identity creation is just one area of focus for FICAM initiatives. The government is also addressing compliance, system interoperability, the integration of PACS and LACS systems, the protection of personally identifiable information (PII) and more. The ICAMSC’s Roadmap outlines a government-wide standard FICAM approach that will serve to:

- Enhance security across the government by closing gaps in user identification and authentication, encryption of sensitive data, and logging and auditing. Better PACS and LACS will help agencies reduce identity theft, data breaches and trust violations.
- Improve government agency compliance with regulations and standards by aligning federal policies and key FICAM initiatives.
- Make federal agencies more accessible to each other, as well as to the American public, while supporting the privacy and security of information and transactions. Qualified PII and personal identity verification (PIV) credentials that are interoperable between agencies will enable accessibility.

- Address identity management and physical access control issues for federal employees who must interface with disparate systems across facilities and sites. Integrated PACS and LACS systems will “enable information sharing across systems and agencies with common access controls and policies.”<sup>[2]</sup>
- Reduce costs and improve efficiencies in FICAM processes by eliminating redundant activities and systems.

Through the above actions, the FICAM initiative will help government agencies “create trusted digital identity representations of individuals and [non-person entities (NPEs)], bind those identities to credentials that may [be used for] access transactions and leverage the credentials to provide authorized access to an agency’s resources.”<sup>[2]</sup>

### FICAM Segment Architecture

To achieve the desired state of streamlined, interoperable FICAM processes, the ICAMSC Roadmap outlines a FICAM segment architecture that provides “federal agencies with a standards-based approach for implementing government-wide ICAM initiatives.”<sup>[2]</sup> Guidelines closely follow the approach defined by the CIO Council’s Federal Segment Architecture Methodology (FSAM), which strives for consistency in identifying baseline and target states for systems, processes and technologies, as well as uniformity in determining transition strategies to achieve the target state.

Based on FSAM guidelines, the ICAMSC Roadmap breaks the FICAM segment architecture into the following five interrelated framework layers:

- **Performance Architecture:** Aligns strategic goals and objectives with metrics to evaluate the ability of processes, systems and technologies to improve FICAM-related activities.
- **Business Architecture:** Delivers solutions that improve the delivery of business services to agencies and the public.
- **Data Architecture:** Covers the planning and implementation of data assets to determine what data is collected, how it is collected and the technologies and processes used to manage that data.
- **Service Architecture:** Provides a functional framework for identifying and evaluating opportunities to group and/or share services across agencies, including digital identity, credentialing, privilege management, authentication, authorization and access, cryptography, and auditing and reporting services.

- **Technology Architecture:** Presents the technical foundation for services components, including how technology will support desired business functions; what, if any, systems are duplicated; and how technology can be reused across agencies to reduce costs and enhance efficiencies.

The interrelated nature of these five architectures enables the federal government to focus on a holistic approach for government-wide FICAM activities. In short, the FICAM segment architecture techniques “...will help ensure alignment, clarity and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the federal government.”<sup>[2]</sup>

### FICAM Origins

FICAM directives are part of the progression of federal policies and standards that have advanced the principles of efficient identity management, as well as credential usage for physical and logical access control. Some of the policies that are influencing FICAM initiatives include:

- **Office of Management and Budget (OMB) Guidance M-04-04 “E-Authentication Guidance for Federal Agencies”:** Provides the basis for government-wide trusted authentication for online government service transactions. This guidance is accompanied by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 “Electronic Authentication Guideline.”
- **Homeland Security Presidential Directive-12 (HSPD-12):** Establishes a government-wide standard for secure and reliable forms of identification for federal employees and contractors for access to federally controlled facilities and networks.
- **Federal Information Processing Standards Publication 201 (FIPS 201):** Specifies PIV requirements for federal employees and contractors.
- **Federal Public Key Infrastructure (PKI) Program:** Addresses encryption methods for exchanging confidential data across PKI domains.
- **Open Government Initiative:** Promotes transparency, participation and collaboration between the federal government and the public.

The FICAM initiative is designed to:

- Enhance security across the government
- Improve government agency compliance with regulations and standards
- Make federal agencies more accessible to each other and to the American public
- Address identity management and physical access control issues for federal employees
- Reduce costs and improve efficiencies in FICAM processes

### FICAM Roadmap and Funding

The ICAMSC has outlined a series of steps that will facilitate implementation of target FICAM segment architectures. This “FICAM Transition Roadmap” provides recommendations for performance improvements that will close any gaps between existing and target systems, processes and technologies. It also prioritizes initiatives and milestones to achieve the target architecture and defines government-wide performance metrics to measure the success of FICAM-related activities and investments. While each government agency will experience a different transition based on its existing architecture, the transition Roadmap serves as a guide for federal agencies to assist in the planning, implementation and execution of their FICAM program architectures.

Each federal executive branch agency is responsible for the following initiatives as outlined in the FICAM Transition Roadmap:

- Streamline collection and sharing of digital identity data to eliminate redundancies and inefficiencies and reduce security and privacy risks.
- Fully leverage PIV and PIV-interoperable credentials by adhering to Homeland Security Presidential Directive-12 (HSPD-12) standards and leveraging credentials that are compliant with PIV-interoperable specifications.
- Modernize PACS infrastructures by updating physical security processes and systems for PIV cardholder and visitor access.

- Modernize LACS infrastructures by upgrading systems to fully leverage PIV cards, better utilize encryption technologies, automate systems to increase efficiency and improve security.
- Implement federated identity capabilities to support streamlined service delivery to external consumers and reduce redundancy in FICAM programs.

To help federal agencies meet these directives, the government has recommended that agencies include funding requests for FICAM-related activities in their annual budget submissions. Funding requests should include a clear definition of the scope of the proposed FICAM project, details about existing solutions and target outcomes and cost data for the proposed solutions.

Within the funding request, agencies need to demonstrate that the proposed target state aligns with federal segment architectures as defined in the ICAMSC Roadmap. The business case should demonstrate “the relationship between the investment and the business, performance, data, services, application and technology layers of the agency’s [enterprise architecture].” [3] In addition, agencies may need to perform a risk assessment of the proposed investment, develop a risk-adjusted life cycle cost estimate and show how they will actively manage risk throughout the investment’s life cycle. As a means of assisting agencies in prioritizing projects, the National Institute of Standards and Technology (NIST) has issued a guidance document that outlines steps for assigning weighted scores to projects to determine a rank-order for funding requests (see the “Security Capital Planning and Investment Control (CPIC) Process Overview” sidebar).

The Office of Management and Budget (OMB) defines budgeting request categories as part of “Circular No. A-11, Part 7 – Planning, Budgeting, Acquisition and Management of Capital Assets.” The OMB specifies Exhibit 300 documents that provide specific topic categories related to FICAM projects. Agencies typically submit separate Exhibit 300s for various FICAM programs. However, it may make sense for agencies to consolidate individual programs into one, agency-wide Exhibit 300. Doing so would promote collaboration across the agency and facilitate the incorporation of a holistic approach to FICAM. A consolidated approach could also help eliminate redundant funding requests for program elements that overlap between agency departments.

**The FICAM Roadmap will help government agencies foster effective policies and enable trust across organizational, operational, physical and network boundaries.**

## Security Capital Planning and Investment Control (CPIC) Process Overview

To help federal agencies better understand the FICAM initiative's integration of information security planning into the Capital Planning and Investment Control (CPIC) process, the National Institute of Standards and Technology (NIST) has issued Special Publication 800-65. This guidance document provides "considerations and frameworks agencies can use to prioritize security investments and help ensure that security concerns are incorporated into the capital planning process."<sup>[4]</sup>

Agencies must carefully plan information security investments to ensure they adequately fund initiatives, meet goals and implement new, existing and corrective systems in a cost-effective manner. As such, the CPIC process consists of three phases:

- **Select:** Assess and prioritize current and proposed projects based on needs and priorities.
- **Control:** Monitor investments during their operational phases to determine if they meet cost and schedule milestones.
- **Evaluate:** Determine if and how well investments are delivering expected results and performance goals.

As part of the select phase, the NIST guidance document suggests that agencies consider ranking security requirements via a risk-based prioritization process. This process will help agencies determine which security requirements should be addressed immediately, which ones may be delayed for future funding requests and which ones can remain unfunded and considered as acceptable risks. Rankings may be determined by inputs such as continuous monitoring results, vulnerability assessments, new mandates and evolving threats.

Based on these considerations, agencies may then prioritize security needs such that the most pressing needs are addressed first when planning capital investments. To do so, the agency may rank investments by assessing security considerations against prioritization criteria. NIST suggests that agencies assign each security consideration "a quantitative value that represents [its] ability to meet the intent of the criterion."<sup>[4]</sup> This value can be multiplied against the criterion weight. Then, all weighted values can be added together, providing a total score for the security consideration. Finally, total scores may be compared to rank-order security considerations.

The highest scoring considerations represent top priorities for security investments. According to the NIST guidance document, "the objective is to apply the first security dollar to the most critical security investment," with the next dollar applied to the next critical investment until the budget is exhausted.<sup>[4]</sup>

**The FICAM initiative will help government agencies create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials and leverage the credentials to provide authorized access to an agency's resources.**

### Developing a FICAM Implementation Plan

Before completing a funding request, an agency must have a very clear picture of its goals and plan for implementing an enterprise-wide FICAM solution. Defining the scope and role of the target FICAM state can be a massive undertaking. The OMB is assisting agencies with this process by issuing a variety of guidelines for preparing or refining FICAM implementation plans.

For example, the OMB's "Guidance for HSPD-12 Implementation," issued May 23, 2008, includes questions agencies should consider when addressing the use of PIV credentials with PACS and LACS systems.

In addition, a consultant may be a valuable partner for an agency during the FICAM planning and implementation process. To achieve the best results, a consultant should have a clear understanding of the ICAMSC

The Federal CIO Council and the Federal Enterprise Architecture note that FICAM segment architecture techniques “will help ensure alignment, clarity and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the federal government.”<sup>[2]</sup>

Roadmap, as well as extensive knowledge and experience in implementing PACS and LACS protocols. Together, the agency and consultant will be well-positioned to adhere to FICAM policies.

In a collaborative process, the agency and consultant should carefully consider all requirements outlined by FICAM policies while carrying out the following steps:

- Complete an “as-is” analysis of the agency’s current system architecture
- Determine a target architecture for the system
- Conduct a gap analysis to define what pieces are needed to achieve the target architecture
- Develop a migration strategy to reach the desired state
- Present a solution architecture that will drive project planning activities and funding requests

An explanation of each of the above steps follows, along with a related example associated with the process of creating and maintaining digital identity records for internal users. These users typically include employees, contractors or affiliates who must be vetted to determine their viability to gain access to buildings, campuses and systems across an agency’s enterprise. Agencies may collect physical, biometric, biographical and other data from individuals to create unique digital identities, which are then used to authenticate an individual when assigning physical credentials, passwords, access to IT systems and other permissions.

Completing an “As-Is” Analysis. The first step in developing and implementing a comprehensive FICAM solution involves an “as-is” analysis of an agency’s current PACS and LACS platforms across its entire enterprise. Consultants can help complete this analysis by documenting every existing system related to physical and logical access control. During this process, consultants will help agencies identify any specific challenges associated with their current systems, develop process flow narratives and diagrams and complete detailed analyses of segment architecture components.

When establishing digital identities for internal users, agencies

Initiating the FICAM process involves:

- Completing an “as-is” analysis
- Determining a target architecture
- Conducting a gap analysis
- Developing a migration strategy
- Presenting a solution architecture

commonly collect personal data during an individual’s onboarding process when he or she first becomes affiliated with the organization. This information may include identity, biographic and context-specific attributes; biometrics; and affiliation information. Agencies typically collect this personal data via various paper and/or electronic-based requests for information from the individual. Agency data administrators or other authorized users then input that data into applicable systems, which may include human resources, payroll, contract management, PACS and LACS platforms.

To complete an as-is analysis of an agency’s digital identity creation process, consultants will document what information the agency collects during the process, how the information is collected and stored, what processes the agency uses to input data, what precautions the agency takes to secure data and any other activities involved. This analysis serves as the basis for determining a target architecture.

Determining the Target System Architecture. The next step in the FICAM implementation process is to examine the wide array of data collected during the as-is analysis and determine what an agency’s systems should entail in the future to meet FICAM directives. This proposed future state is known as the target system architecture. Reporting for this architecture includes descriptions of the primary differences between the current system and what the target architecture will cover in terms of processes, data, services and technologies. The reporting also includes process flow narratives and diagrams, as well as a detailed analysis of components that support the target architecture.

Looking again to the digital identity creation process, an as-is analysis may reveal inefficiencies related to data entry during an individual's onboarding process. For example, multiple people may input the same identity data multiple times into multiple systems. These redundancies create an administrative burden for inputting and maintaining identity records. They also create problems with provisioning and onboarding/offboarding an identity, as these activities would not occur simultaneously across a number of systems. Therefore, a consultant may recommend that an agency's target system architecture include measures designed to streamline management of digital identity information. The target architecture may call for the creation of core identity records that parties can access across the agency. It would designate one data administrator group – potentially human resources – to input individuals' identity information one time into a centralized database. Other groups would then access that digital information to complete their respective activities. For example, parties responsible for issuing access control cards could pull up the digital identity and proceed with card issuance without having to re-enter already logged data. In addition, the system architecture would allow records to be automatically and instantaneously updated to all PACS and LACS systems. This streamlined system would help the agency ensure that changes in an individual's status, such as termination, are reflected agency wide to make sure access privileges are revoked or granted as appropriate.

A key concept to remember is that individuals have one identity, and that identity will be asserted (used) to gain access to many applications based on the given identity's role in an agency.

**Conducting a Gap Analysis.** With the proposed target system architecture in place, agencies and consultants must next turn to analyzing any gaps between the as-is system and the desired target state. This process determines if any obstacles exist that may prevent the agency from achieving its future goals and meeting FICAM directives. Gaps may be present in data, technology, business and/or service functions and “span a variety of issues, from outdated technologies, to poor business process fit, to redundancies” and more.<sup>[2]</sup> The gap analysis includes explanations about each gap and the relative impact each one has on agency processes. Strategies to close gaps are addressed in the migration strategy and solution architecture stages of the FICAM implementation process.

An example of a gap in a digital identity creation process would be the lack of common definitions or data specifications for collecting identity information. If human resources groups at an agency's different branch offices don't collect common information, there will be holes in employees' digital identities. If those human resources groups collect the same information but utilize different databases to input information, disparities are also likely to occur. The gap analysis

stage of the FICAM development process identifies those gaps to ensure that fixes are planned to implement consistent data collection and sharing processes.

**Developing a Migration Strategy.** Based on the as-is analysis, desired target state and gap analysis, a consultant will next help the agency determine how to achieve the preferred system architecture. This process involves developing a migration strategy that seeks to:

- Determine how to eliminate any process, service or technology gaps
- Recommend appropriate PACS and LACS solutions to close gaps
- Identify appropriate budgeting needs
- Develop a timeline for implementation
- Ensure that the proposed strategy fits an organization's complete architecture across its enterprise
- Provide efficiency in implementation

For example, the migration strategy for updating an agency's digital identity creation process may include measures designed to ensure the collection of consistent data from all agency employees during onboarding. The strategy may outline how to standardize data collection processes across all agency offices, propose solutions designed to streamline these processes, note budgetary guidelines for investing in those solutions and recommend a tiered approach to implementation.

**Presenting a Solution Architecture.** Finally, a consultant will present a proposed solution architecture designed to help the agency achieve its FICAM goals. The solution architecture is a comprehensive framework consisting of all the relevant architectural layers for the overall FICAM solution, which may include performance, business, data, service and technology segments. It often consists of four interconnected views of the proposed solution architecture, including:

- **All View:** Establishes the architecture's purpose, scope and context, describing attributes, assumptions, metrics and a summary of findings.
- **Operational View:** Describes the as-is model and defines the activities, operational elements and information flows required to accomplish or support the target state.
- **Systems View:** Correlates physical resources and their performance attributes to the operational view and its requirements to ensure interoperability and a streamlined migration from the as-is state to the target state.
- **Technical View:** Presents the technology components, standards and supporting guidelines that will lead to an efficient migration to the target state.

## To help agencies meet FICAM directives, the government has recommended that agencies include funding requests for FICAM-related activities in their annual budget submissions.

A portion of the solution architecture for an improved digital identity creation platform may include operational, systems and technical views associated with centralizing an agency's core identity record system. These views would detail how a centralized system promotes efficiency in capturing changes in an individual's job status, training or security clearance. The solution architecture would define processes in which a single data update carries across an enterprise, thereby reducing the number of times an individual has to be credentialed. This adjustment would close a security gap associated with using disparate identity record systems. For example, an employee termination update may be completed in one system but not in others. Conflicting identity records could lead to a security breach, as the dismissed employee may be able to gain unauthorized access to areas or systems if the agency has not revoked his card access control privileges across all PACS and LACS systems.

### Moving Forward

Standardizing FICAM policies will help the United States government enhance security, improve efficiencies and reduce costs across all federal agencies. The FICAM Roadmap established by the ICAMSC sets the stage for improving accessibility between agencies and between agencies and the public, establishing common PACS and LACS protocols across the government and fostering agency compliance with federal regulations and standards. Federal agencies need to fully understand their current systems and what they need to do to realize a target state that complies with FICAM policies. Consultants can

play a vital role in this process. They can help agencies develop a solution architecture that takes into account a complete assessment of the existing system architecture, an agency's desired goals for the system and any roadblocks that need to be overcome to enable an agency to reach its desired solution. Consultants can also help agencies better understand the budgeting process to submit appropriate FICAM funding requests. With this third-party assistance, agencies can be better positioned to comply with FICAM policies.

### END NOTES

[1] "Identity, Credential, and Access Management Segment Architecture handout." Federal Chief Information Officers (CIO) Council. [www.IDManagement.gov](http://www.IDManagement.gov).

[2] "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance – Version 1.0." Federal Chief Information Officers (CIO) Council and the Federal Enterprise Architecture. Nov. 10, 2009.

[3] "Circular No. A-11, Part 7 – Planning, Budgeting, Acquisition and Management of Capital Assets." Executive Office of the President Office of Management and Budget. November 2009.

[4] "NIST Special Publication 800-65, Revision 1; Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process." National Institute of Standards and Technology. July 2009.

Call on Diebold for the latest in product, service and security solutions.  
Since 1859, Diebold has put the customer first.

Contact Information:  
Diebold, Incorporated  
5995 Mayfair Rd  
North Canton, Ohio 44720

E-mail: [securityintegrator@diebold.com](mailto:securityintegrator@diebold.com)  
[www.dieboldsecurity.com](http://www.dieboldsecurity.com)

© Diebold, Incorporated, 2010. All rights reserved.  
Litho in USA. 08.10 File No. 70-1475.

**DIEBOLD**  
SECURITY