U.S. Nuclear Regulatory Commission

Office of the Chief Information Officer

Identity, Credential, and Access Management Governance
ICAM Program Charter

Version: 2.0
Release Date: 01 29 2020

James R. Peyton Jr.

Revision History

Date	Version	Description	Author
01 31 2013	0.1	Initial Draft	Christian Palmhede, Emergent, LLC
03 27 2013	1.0	NRC Review	David Sulser, NRC / OIS
06 26 2013	1.1	Revisions	David Sulser, NRC / OIS
06 27 2013	1.2	The team applied the latest document template.	Christian Palmhede, Emergent, LLC
07 11 2013	1.3	Additional References	David Sulser NRC / OIS
11 26 2013	1.4	Revisions based on comments from CIO and CSO	David Sulser NRC/OIS
05 09 2014	1.5	Remove the role of Oversight Board	David Sulser NRC/OIS
08 22 2014	1.6	Add text from CSO concurrence email of 8/6/2014	David Sulser NRC/OIS
01 24 2020	2.0	Changed office names; updated to comply with requirements of OMB M-19-17; and updated to align with current NRC Strategic Plan.	James Peyton NRC/OCIO

SUNSI Review

Date	Version	SUNSI Item Codes	Review Finding	Reviewer
08 22 2014	1.6	Publicly Available	The ICAM Program Charter is designated as Publicly Available because the content is based on Federal Government publications that are publicly available. The information does not contain personally identifiable information (PII) or sensitive NRC information. This designation does not require any markings on the document.	David Sulser, NRC
01 28 2020	2.0	Publicly Available	The ICAM Program Charter retains its designation as Publicly Available for the reasons stated above.	James Peyton, NRC

Signature Page

David J. Nelson, Chief Information Officer (CIO) and Authorizing Official (AO) authorizes this Charter.

Handwritten Signature (Optional)

Date

Digital Signature

X David J. Nelson

Digitally signed by David J. Nelson
Date: 2020.01.29 17:33:19 -05'00'

David J. Nelson
CIO and AO

Table of Contents

Table of Tables

Table of Figures

1 Introduction

The Identity, Credential, and Access Management (ICAM) Program of the Office of the Chief Information Officer (OCIO) evolved from the Authentication and Credentialing Services Program, which in turn grew out of the Managed Public Key Infrastructure program. The ICAM Program was initiated when OCIO was structured as "the Office of Information Services" out of a desire to streamline credentialing and account management services and to integrate new identity and privilege management services to reap benefits from agency investments in PKI digital certificates and Personal Identity Verification (PIV) smart cards. The term ICAM comes from the Federal Enterprise Architecture segment of the same name. The Office of Management and Budget (OMB) in OMB M-11-11[1] mandated agency adoption of ICAM and PIV to replace the username and password to maintain a minimally acceptable level of security for federal facilities and systems. OMB M-11-11 has since been superseded by OMB M-19-17[2], which has further strengthed the federal government's commitment to ICAM.

The ICAM Program Charter grants authority and rights to the ICAM Program. All other artifacts produced and services provided under the ICAM Program stem from this authority and associated rights and responsibilities. The program has designed its artifacts and services and the activities described in this Charter to comply with NRC standards and processes contained in the NRC Management Directive (MD)[3] 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework."

1.1 Purpose

The purpose of the ICAM Program Charter is to formalize the authority of the ICAM Program. The Charter specifies the objective, goals, responsibilities, membership, roles, and primary stakeholders of the program.

The primary audience for the Charter is the members of the program, to further their understanding of the program objective and associated goals, and their respective duties in support of the program. The secondary audience is the members of collaborating projects as well as other stakeholders so that they are aware of the mission of the program.

1.2 Scope

The scope of ICAM, as defined by the Federal Chief Information Officer Council and the Federal Enterprise Architecture, includes functions performed by both divisions of OCIO and the Division of Facilities Security in the Office of Administration (ADM). The scope of ICAM includes all of the implementation activities of Homeland Security Presidential Directive 12 (HSPD-12) and the Federal ICAM (FICAM) Roadmap and Implementation Guidance from the Federal CIO Council. The staff and management of OCIO and ADM have formed an ongoing partnership to deliver HSPD-12 tailored to the needs of the NRC. When the NRC's ICAM Program was initially chartered, the OMB Memorandum M-11-11 directed agencies to "designate an agency lead official for ensuring the issuance of the agency's HSPD-12 implementation policy." Due to the

[1] OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, February 2011)
[2] OMB M-19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management (PDF, May 2019)
[3] All NRC management directives are available at https://www.nrc.gov/reading-rm/doc-collections/#man.

inter-office scope and significance of HSPD-12 and PIV for agency facilities and network security, the NRC named its Chief Information Officer (CIO) to fill this role.

OMB Memorandum M-19-17 has superseded M-11-11 and states that:

> "1. Each agency shall designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts.
>
> - This structure should include personnel from the offices of the Chief Information Officer, Chief Financial Officer, Human Resources, General Counsel, Chief Information Security Officer, Senior Agency Official for Privacy, Chief Acquisition Officer, Senior Official(s) responsible for Physical Security, and component organizations that manage ICAM programs and capabilities, including ICAM capabilities deployed through the CDM Program.
> - Chief Operating Officers (COOs) or the agency equivalent role shall ensure that there is regular coordination among agency leaders and mission owners to implement, manage, and maintain the agency's ICAM policies, processes, and technologies.
> - While the agency governance structure described above will facilitate oversight of the implementation of Government-wide and agency enterprise-specific requirements, all bureaus, components, and other organizations at the subenterprise level must support efforts to harmonize ICAM across their respective agency by adhering to requirements and fostering accountability at all levels of the organization."

The ICAM Program Charter outlines the activities undertaken by core stakeholders to ensure that associated projects meet the requirements outlined by the FICAM Roadmap. All resulting projects will follow NRC policy guidance for Information Technology (IT) projects. This guidance includes, but is not limited to, existing MDs (e.g. MD 2.8, MD 12.5) and governance boards (e.g. the Information Technology Board and the Information Technology/Information Management Portfolio Executive Council (IPEC)) to ensure that appropriate controls are in place to provide assurance that projects adhere to all NRC requirements. The IPEC, specifically, provides the inclusive, agency-wide governance structure called for in M-19-17. Its membership is comprised of senior executive leadership from NRC Program Offices. The CIO and CFO oversee the IPEC, and are in regular, direct communication with the EDO (who serves as NRC's COO) and the Chairman. The majority of ICAM implementation and operational activities occur within OCIO; therefore, the agency lead official for ensuring the issuance of the agency's HSPD-12 implementation policy is designated as the NRC's CIO.

The ICAM Program Charter specifies the entirety of the authority granted the ICAM Program. Figure 1 outlines the scope of activities of ICAM. The core services for PIV are provided by the partnership between OCIO and ADM. The digital signature component also encompasses services provided by the Office of the General Counsel (for determining legal sufficiency) and the Office of the Secretary of the Commission (for advising on implementations for external partners).

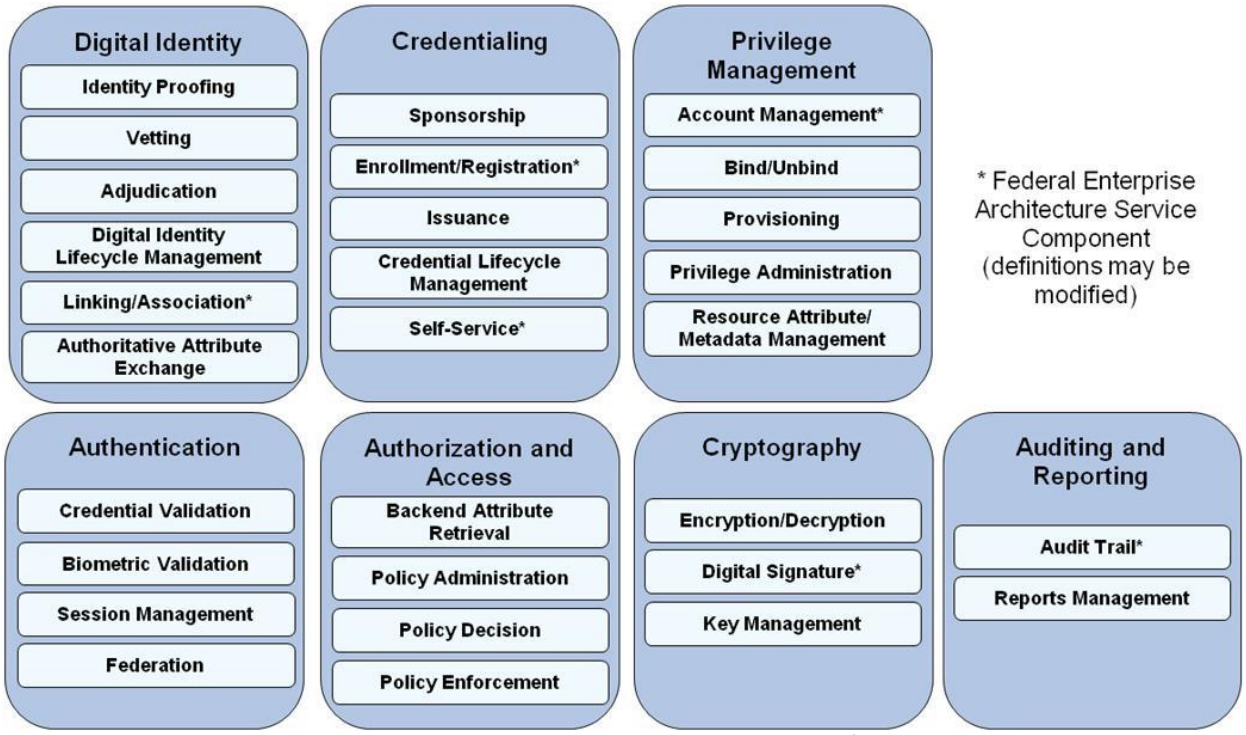

Figure 1: ICAM Services Framework[4]

2 Overview

The following sections describe the administration priority for ICAM; the foundations for the NRC ICAM Program; and the program's mission, goals, and objectives.

2.1 ICAM in the Federal Government

The President in the December 2012 *National Strategy for Information Sharing and Safeguarding* states that information is "a national asset that must be both protected and shared, as appropriate. The threats to our national security are constantly evolving, so our policies to ensure this information is used and protected as intended must evolve as well. This includes protecting private and personal information about United States persons and upholding our commitment to transparency." The Strategy includes in its list of accomplishments that the government and its partners have "established a plan to unify and align user identification and authentication on systems, through the FICAM framework under the National Strategy for Trusted Identities in Cyberspace. This represents a critical step toward establishing individual accountability and facilitating the appropriate level of information access."

The FICAM framework referenced in the President's strategy is the FICAM Roadmap and Implementation Guidance published by the FCIO Council in 2009 and updated in 2011. The FCIO Council launched the ICAM effort to address the growing concern within the Federal

[4] Source: FICAM Roadmap and Implementation Guidance Version 2.0, December 2, 2011, page 34.

Government and beyond over these aspects of the nation's increasing cyber security threats. In so doing, they defined the parameters of the national debate on how to improve the trustworthiness of identities in cyberspace.

ICAM for the first time formally unites the disciplines of Identity Management, Credential Management, and Access Management under a common practice. Identity Management is the lifecycle of electronic identity information and attributes about persons and non-persons that interact in cyberspace. Credential Management is the lifecycle of electronic identity credentials held and used by persons and non-person entities to facilitate electronic identification and access. Access Management is the granting, monitoring, and removing of access privileges to physical facilities and resources in cyberspace. The common practice has been documented as a segment architecture under the Federal Enterprise Architecture.

As explained in the President's Strategy, strong and reliable ICAM capabilities across the entire Federal Government are seen as a critical factor in the success of all government work. This point is emphasized in the "Top 5 Priority Objectives," one of which is to "extend and implement the FICAM Roadmap across all security domains." The NRC ICAM Program, including the NRC FICAM Transition Plan, is an important next step in the implementation of the FICAM Roadmap and the President's Strategy, and for maintaining security at the NRC.

2.2 The NRC ICAM Program

The NRC ICAM program serves as an enterprise-wide focal point for all ICAM activities and is integrated with the Capital Planning and Investment Control (CPIC) and other processes to ensure that applications have the necessary guidance to conduct upgrades and implementations in accordance with the stated ICAM direction. The program follows standardized project management policies, processes, and methods. It provides opportunities to share ICAM lessons learned both within the agency and across agencies. The program serves as an advisor to agency program offices or programs impacted by the ICAM segment architecture to ensure interoperability with other agency-wide capabilities. Additionally, it acts as a single, centralized point of contact for the ICAM topic.

Ensuring adequate representation of ICAM objectives in the IT governance process calls for the assignment of an ICAM Program to provide oversight, management, development, and enforcement of agency policies, processes, and performance measures. ICAM governance encompasses the relationship between the oversight effort, mechanisms put in place to ensure compliance, the enterprise's overall business direction, and the accountability framework to encourage desirable behavior. It also encompasses all of the decision-making roles and responsibilities involved in executing the program across the agency enterprise. The ICAM Program governance is structured to facilitate coordination between the offices and to promote stakeholder buy-in.

Finally, the program has the primary authority for performing ICAM-related acquisition planning and requirements definition. As a result, it offers the agency many efficiencies, streamlined overhead costs, minimized redundancy of ICAM-related processes, validated alignment with architectural and technical standards, fostered communication and cooperation between interrelated programs, consistent communication to both internal and external stakeholders, timely and accurate reporting, minimized uncertainty, facilitated agency-wide adoption, and minimized risk.

2.3 Mission

The mission statement guides program decision-making and provides the framework for formulating the program goals, objectives, and strategies.

Table 1: Mission

ICAM Mission Statement
The mission of the NRC ICAM Program is to provide security infrastructure and services to the NRC staff and external partners, for: • electronic identities, attributes, and privileges; • credentialing and authentication; • physical and logical access management; • cryptography, key management, and digital signature; • trusted credential validation; • internal and external identity federation; and, • secure Internet communication.

2.4 Vision

The vision statement describes the ambition of the ICAM Program as an agent of change.

Table 2: Vision

ICAM Vision Statement
To create an IT environment at the NRC where people see authentication, credentials, access controls, and levels of assurance as enablers of their work.

2.5 Goals

The high-level goals of the ICAM Program express desired business outcomes across the agency. The goals also align with the NRC IT/IM Strategic Plan for 2016-2020. Specifically, the ICAM Program embraces Goal 6, Strategy 2, “Reduce information and cybersecurity vulnerabilities” and its associated measures and key activities.

Table 3: Goals

ICAM Program Goals
1. NRC staff and stakeholders can enroll quickly and easily for access to needed information through facilitated data sharing between the Office of the Chief Human Capital Officer, the Personnel Security Branch and Facilities Security Branch of the Office of Administration, and the Office of the Chief Information Officer.
2. The number of login passwords each user must maintain is minimized.
3. The number of NRC-controlled systems able to use the agency-wide sign-on infrastructure built around the PIV card is maximized.
4. System owners securely and reliably identify users through agency-wide enrollment standards and authentication services.

5. Access privileges to logical and physical resources are securely managed through agency-wide access control standards.
6. Secure communication with external entities is facilitated through the controlled exchange of electronic identity information.
7. Alignment with laws and federal mandates including the Privacy Act, the Government Paperwork Elimination Act, HSPD-12, the FICAM Roadmap and Implementation Guidance, and OMB memoranda, including M-07-16, M-11-11, and M-19-17 is optimized for results.

2.6 Objectives

The objectives are major activities that are underway today and will create long-lasting improvements in the effectiveness of IT support for agency business needs. The objectives take responsibility for accomplishing the key activities of the IT/IM Strategic Plan, Goal 6 (Prevent Unauthorized Access to Agency Information and Use of Government-Issued Credentials) Strategy 2, “Reduce information and cybersecurity vulnerabilities” The objectives also directly support the NRC Strategic Plan as shown in Table 5: Alignment with NRC and IT/IM Strategic Plans.

Table 4: Objectives

ICAM Objectives
1. Provide and support an agency-wide sign-on infrastructure so that new and existing applications will not need a separate user identification and password and can accept an NRC Badge (PIV card) for access.
2. Implement policies to ensure that new systems or major enhancements use the agency’s sign-on infrastructure.
3. Develop guidance and implement policies and technical support services to enable the agency’s business process owners to satisfy the legal and technical requirements of adopting electronic signatures to streamline work.
4. Design, develop, and implement the ICAM segment architecture of the Federal Enterprise Architecture at the NRC.

Table 5 shows how the ICAM Program Objectives align with the NRC Strategic Plan 2018-2022 and the IT/IM Strategic Plan 2016-2020.

Table 5: Alignment with NRC and IT/IM Strategic Plans

ICAM Alignment with NRC and IT/IM Strategic Plans		
Strategic Plan	Strategy	ICAM Objectives
IT/IM Strategic Plan, Goal 6 (Prevent Unauthorized Access to Agency Information and Use of Government-Issued Credentials) Strategy 2	Reduce information and cybersecurity vulnerabilities	Primary: 1, 2 Secondary: 4

NRC Strategic Plan, Accompanying Objectives for Each Strategic Goal	Key corporate functions, such as financial management, human resources management, acquisition planning and execution, and information technology management, play a key role in the agency's effective and efficient use of its resources to deliver mission value.	Primary: 3 Secondary: 1, 2, 4

3 Program Authority

3.1 Executive Sponsor

The CIO and AO formally recognizes the prerogative of the ICAM Program to exercise the rights specified in this section.

3.2 Program Manager

The ICAM Program Manager and members of the ICAM Team are vested with specific governance authority in support of the ICAM Program and the ICAM Segment Architecture.

Table 6: Governance Authority

ICAM Governance Authority
1. Halt activity that affects — or, is affected by — the NRC ICAM segment architecture, when such activity does not comply or cannot be shown to comply with the ICAM segment architecture, with Federal laws, regulations, and standards, with the NRC ICAM policy, or with NRC strategic objectives.
2. Spend funds allocated to the ICAM program at its discretion in conjunction with the ICAM mission, strategic objective, and goals.
3. Approve and deny distribution of an ICAM communications message.
4. Approve and deny ICAM related acquisition actions.
5. Chair the NRC PKI Policy Management Authority (PMA) to review and approve the NRC PKI Registration Practices Statement, as required under the Federal PKI Shared Service Provider program.

Appendix C, Program Responsibilities, provides additional detail on the governance practices employed by the ICAM Program.

4 Stakeholders

The ICAM Program changes the way access control is managed, to the benefit of all stakeholders. Before ICAM, the component processes for system authentication were managed in stovepipes, which led to challenges for all stakeholders. ICAM stakeholders across the agency have distinct business requirements (for example, security and public access) and can

at times conflict with each other or the ICAM program objectives. Decisions made in one program area may affect another; therefore, the ability to communicate and coordinate across stakeholder groups, combining their inputs to the benefit of all, is vital to the success of the ICAM program. The *ICAM Program Guidance* identifies the current stakeholders and addresses how the program engages those stakeholders and promotes collaboration across the agency's ICAM portfolio to help overcome many of the challenges associated with ICAM management.

A representative list of Office-level stakeholders is shown in Table 7. The projects listed are dependent on or directly related to the ICAM Program and its governance.

Table 7: Related Efforts

Project/Effort	Responsible Organization
PIV PKI-enabled Facility Access Control	ADM
Integrated Source Management Portfolio	NMSS
EIE digital signature	SECY
Federal Register digital signature	NMSS
New Employee On-boarding	OCHCO
FISMA Compliance	OCIO
Enterprise Risk Management	OEDO
Personnel Security Program	ADM

5 Program Management

The ICAM Program drives the adoption of management processes; especially, communication management, risk management, and performance management. Equally important to the success of ICAM are acquisition management and privacy management. Additional information about ICAM program management can be found in Appendix D Management Processes, and in the separate *ICAM Program Guidance* document.

5.1 Communication Management

In order to communicate consistently and effectively, the *ICAM Program Guidance* addresses the communication management strategy. Some goals of the plan include the distribution of project information, management of stakeholders' expectations, and communication of project performance. The overall goal of the plan is to keep stakeholders regularly informed and involved by providing appropriate and well-structured communications, ultimately helping to foster and maintain stakeholder support and reduce risk.

In fulfillment of federal agency responsibilities expressed in the E-Government Act of 2002, Section 3544(e) to provide for public notice and comment when "policies and procedures affect communication with the public," the ICAM Program will to the fullest extent possible, post its documents in public ADAMS and on icam.nrc.gov as appropriate, and provide a forum for public comment as necessary.

5.2 Risk Management

Due to the interdependency of ICAM projects and frequent interaction with other NRC offices, risks that threaten the success of the ICAM program can have sweeping effects. The *Program Guidance* addresses how risks are measured for the ICAM program, provides a process for identifying the appropriate response, and assigns roles and responsibilities for various stages in the process.

The program-level *ICAM Risk Registry* aides in managing, assigning, and tracking risk events. Reviews and updates to the risk registry are incorporated into ongoing ICAM management processes. A separate risk registry is maintained for each ICAM project.

Table 8 provides a representative sample of program-level risks faced by the ICAM program. Risks are defined using the following cause-risk-effect format:

> *Because <definitive cause>, <uncertain event> may occur, resulting in <immediate effect>, which can lead to <long-term effect>.*

Table 8: Risk Register

Definitive Cause	Uncertain Event	Effect
Because of a lack of understanding of the role of ICAM in security,	the agency may not be able to transition from username and password as the primary authenticator,	leading to increased incidents of user account compromises and intrusions into more agency IT systems.
Because the agency plans and budgets do not include ICAM activities,	adequate funding may not be available for the modernization efforts,	preventing the agency from meeting target state requirements and deadlines for the ICAM segment architecture, which can lead to program failure.
Because of competing investment priorities,	the agency's ICAM transition plan may not gain support and adoption from OCIO management, including required compliance indicators,	resulting in a lack of cooperation and support from the stakeholders, which can lead to program failure.
Because of budget constraints,	funding may be reduced,	resulting in an inability to staff implementation efforts with the necessary technical knowledge, which can lead to program failure.
Because of events beyond the control of the ICAM program management,	an ICAM solution vendor may go out of business,	resulting in a need to migrate to new solutions, which can lead to schedule delays and cost increases.

5.3 Performance Management

In addition to mandatory reporting requirements, the ICAM Program uses performance reporting to improve alignment with the ICAM segment architecture and to quantify the benefits of the agency's ICAM investments. The program also incorporates relevant metrics into the OMB Major Investment business case submissions for all ICAM investments to help demonstrate investment value to the agency.

5.4 Acquisition Management

The ICAM Program adheres to NRC Management Directive 11.1, "NRC Acquisition of Supplies and Services." This directive complies with Federal Acquisition Regulation (FAR), which sets forth the rules governing the federal acquisition process and includes several clauses specifically relevant to the ICAM Program. When purchasing products and services for HSPD-12 implementation, the program follows the OMB M-06-18 memorandum and the Approved Products List (APL) of the Federal Information Processing Standards 201 (FIPS 201) Evaluation Program. The program also uses GSA IT Schedule 70 and Schedule 84.

The *ICAM Program Guidance* addresses how the ICAM program uses these resources to achieve more competitive rates and potentially lower implementation costs, shorter procurement time, reduced complexity and effort required to perform due diligence, and elimination of non-compliance with standards and requirements.

5.5 Privacy Management

The ICAM Program manages the agency Privacy Act System of Records NRC-45, "Digital Certificates for Personal Identity Verification." This system collects and stores significant privacy data about individuals inside and outside the NRC, to meet federal credentialing requirements. Consequently, the program team must mitigate potential privacy risks, and provide appropriate security for the identity and credential management systems. Privacy is considered an essential component and mission critical objective of ICAM and the program ensures that implementers understand the privacy principles and that they integrate those principles with their ICAM initiatives.

5.6 Incorporate ICAM into Existing Processes

In addition to ICAM-specific systems and processes, there are numerous other systems and processes within the agency that are affected by the implementation of the ICAM segment architecture. The *ICAM Program Guidance* addresses how the program integrates the ICAM segment architecture with these other systems and processes.

The plan specifically looks at the integration with management accountability processes, capital planning processes, project management processes, and security and risk management processes as well as with the enterprise architecture plan.

6 Amendments to the Charter

This section specifies who reviews and updates the document and at what intervals. All changes to this document are controlled through the configuration management process described in the ICAM Configuration Management Plan.

The Program Manager reviews the ICAM Program Charter periodically.

If the need for charter amendments arises, the Program Manager and the Team review suggested revisions, inform stakeholders, address comments, and concur or disagree with the changes. The Program Manager republishes the revised document with notification to stakeholders. In the event that significant changes are to be made to the Charter or the Program, the CIO shall reauthorize the Charter.

If the need arises, the Team uses the following steps to incorporate any needed changes:

- The program identifies needed changes during normal business operation.
- The program team makes the suggested revisions to the charter.
- The updated charter is submitted to stakeholders for review and feedback.
- The program and other stakeholders concur or disagree with changes.
- Consensus is reached and changes are approved.
- If appropriate, the CIO signs the revised charter.

7 Referenced Documents

This section provides a complete list of documents used as the foundation for the ICAM Program Charter or otherwise referenced in this document.

Table 9: Document References

Title	Publishing Organization
E-Government Act of 2002	U.S. Congress
Fair Information Practice Principles (FIPPs)	U.S. Department of Homeland Security
Federal Acquisition Regulation (FAR)	U.S. General Services Administration
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance	Federal Chief Information Officers Council
Federal Information Processing Standards 201 (FIPS 201)	U.S. Department of Commerce
Government Paperwork Elimination Act of 1998	U.S. Congress
Homeland Security Presidential Directive-12 (HSPD-12)	The White House
ICAM DOC Configuration Management Plan	U.S. Nuclear Regulatory Commission
ICAM Program Guidance	U.S. Nuclear Regulatory Commission
ICAM Transition Plan	U.S. Nuclear Regulatory Commission
National Strategy for Information Sharing and Safeguarding	The White House
National Strategy for Trusted Identities in Cyberspace	The White House

OMB M-06-18, M-07-16, M-11-11, M-19-17	Office of Management and Budget
Personal Identity Verification Interoperability for Non-Federal Issuers (PIV-I)	Federal Chief Information Officers Council
Privacy Act of 1974	U.S. Congress

Appendix A. Tasks

This appendix enumerates some of the high-level tasks that will be performed by the ICAM Program in fulfilling its mission and objectives. This list is subject to quarterly review and refinement based on agency priorities.

Table 10: Tasks

ICAM Tasks	Description
Policy	
Define ICAM Policy	Define an agency policy around the ICAM segment architecture.
Execute ICAM Policy	Align and coordinate agency ICAM policy with project efforts.
Governance	
Manage Communications	Ensure broad awareness and understanding. Leverage existing communication mechanisms.
Manage Risk	Drive the use of a common risk management framework. Identify risks that could hinder implementation and acceptance of the ICAM segment architecture, including cyber security risk.
Measure Performance	Drive the use of a common performance management framework. Improve electronic audit capabilities.
Business Support	
Define and Achieve Increased Usability	Reduce the administrative burden associated with performing ICAM tasks.
Define and Achieve an Improved ICAM Security Posture	Define a target security posture. Support cyber security programs. Integrate electronic verification procedures with physical security systems.
Leverage Existing Investments	Leverage existing technology investments. Leverage existing process investments.
Manage the Adoption of Evolving Federal Standards	Participate in the discussion and formulation of Federal standards. Continuously move to align with and reduce the impact of evolving Federal standards.
Comply with Federal Laws, Regulations, Standards, and Governance	Align and coordinate Federal policies with project efforts. Establish and enforce accountability for ICAM implementation.
Facilitate E-Government	Streamline access to services. Expand secure electronic access to agency data and systems. Promote public confidence through transparent ICAM practices.

Enable Trust and Interoperability	Support communities of interest for information sharing environments. Align processes with external partners. Establish and maintain secure trust relationships. Leverage standards and commercial off-the-shelf technologies.
Control Costs and Implement Processes to Continuously Improve the Efficiency and Benefit of ICAM	Align existing ICAM project efforts. Reduce redundant ICAM project efforts. Increase interoperability and reuse of ICAM project methods. Increase interoperability and reuse of ICAM systems.

Appendix B. ICAM Organization Vision

Figure 2 illustrates the vision for the organization of the ICAM Program. The structure fosters communication and coordination between efforts, and appropriately aligns with the agency's overall organizational structure. In the current state, these roles and functions are accomplished through matrix management, contractor expertise, and multiple roles for team members.

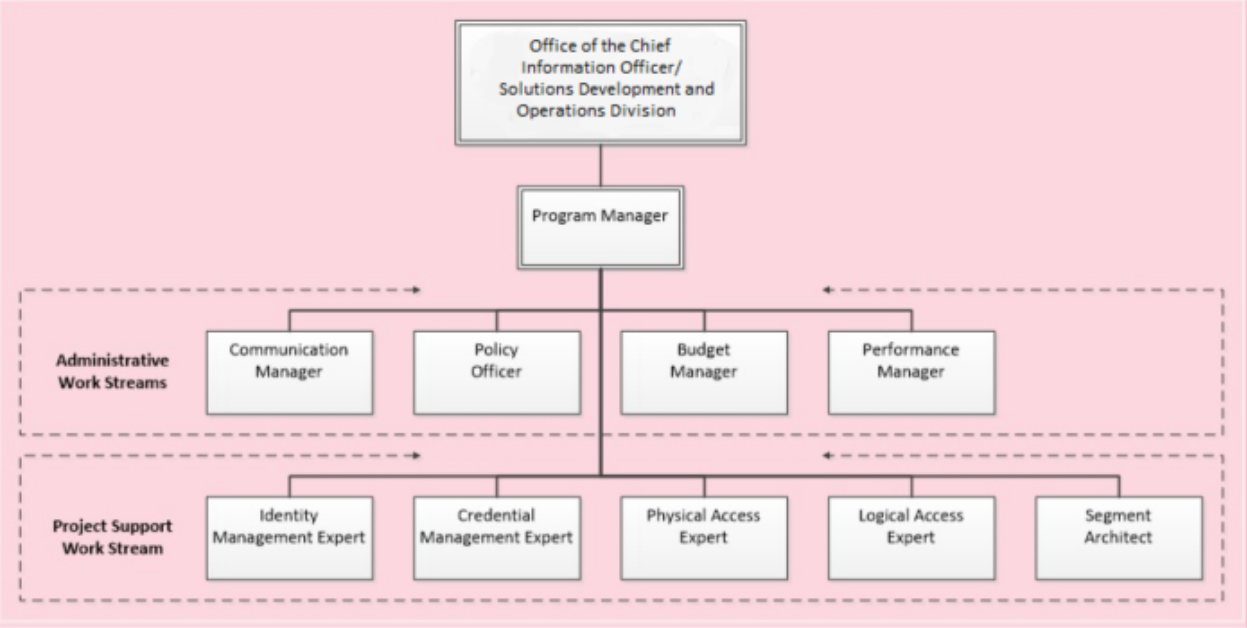

Figure 2: ICAM Program Team

The administrative work streams ensure that both program management and coordinated project management responsibilities are properly carried out. The project support work streams ensure that all technical aspects of the program and the coordinated implementation projects are adequately addressed.

To achieve the objectives with available resources, the program often assigns responsibility for separate work streams to individuals outside of the program who are actively involved and have expertise in a particular area. An ICAM work stream manager coordinates the day-to-day activities of each work stream and provides the ICAM Program with critical and timely information related to the planning, development, deployment, and other activities of these initiatives.

B.1. Roles and Responsibilities

This section identifies the persons involved with ICAM and their responsibilities. These roles will be filled as the ICAM workload and agency resources permit. The Program Team roles may be staffed through matrix arrangements, and one person may serve more than one role.

Table 11: Roles

Role	ICAM Responsibility
Governance	
Program Sponsor	The Program Sponsor is the champion of the program and authorizes the program by signing the ICAM Program Charter. This role is filled by the CIO, who through his role as IPEC Co-Chair, ensures agency alignment and adequate funding for the program, and is ultimately responsible for the program's success. Since the Sponsor is at the executive level, communications should be presented in summary form unless more detail is requested.
ICAM Program Team, Administrative Roles	
Program Manager	The Program Manager is a member of the program team who oversees the ICAM Program at the portfolio level and owns most of the resources assigned to the program. The Program Manager is responsible for overall program costs and delivery and as such requires more detailed communications than the Program Sponsor.
Project Managers	The Project Managers have responsibility for the execution of ICAM implementation projects; they manage day-to-day resources, provide project guidance, and monitor and report on the projects' metrics. As the persons responsible for the execution of the implementation projects, they are the primary communicator for the project, distributing information according to the Communications Management Plan.
Communications Manager	The Communications Manager is a member of the program team who is responsible for developing and executing the ICAM program's Communications Plan, including defining communication message types, media, target audience, and timing, and communicating ICAM program concepts, activities, and progress to promote support for the implementation of improved ICAM capabilities.

Policy Officer	The Policy Officer is a member of the program team who provides policy direction for the ICAM Program and develops and finalizes all policies and standard operating procedures related to the ICAM Program. The Policy Officer monitors and assesses federal ICAM policies, standards, and guidance for impact to the NRC. He maintains close contact with the federal standards community and represents the NRC on ICAM standards and guidance bodies.
Budget Manager	The Budget Manager is a member of the program team who is responsible for developing, managing, monitoring, and reporting on the ICAM program budget. The budget manager interfaces with OCIO Branch and Division management, and OCFO as needed, during budget formulation cycles.
Performance Manager	The Performance Manager is a member of the program team who is responsible for tracking, managing, and reporting on the overall ICAM program performance and metrics.
ICAM Program Team, Project Support Roles	
Identity Management Expert	The Identity Management Expert is a member of the program team who is responsible for ICAM processes and systems related to the management of digital identity data. This includes management and oversight of efforts to modernize the management of digital identities, such as HR modernization, in accordance with the ICAM target state initiatives.
Credential Management Expert	The Credential Management Expert is a member of the program team who is responsible for ICAM processes and systems related to credential lifecycle management activities. Separate work streams may be identified for various credential types, including agency PIV cards and external partner credentials.
Physical Access Expert	The Physical Access Expert is a member of the program team who is responsible for ICAM processes and systems related to physical access control, including modernization efforts in accordance with the ICAM target state initiatives.
Logical Access Expert	The Logical Access Expert is a member of the program team who is responsible for ICAM processes and systems related to logical access control, including modernization efforts in accordance with the ICAM target state initiatives.

Segment Architect	The Segment Architect is a member of the program team who ensures that the NRC ICAM Transition Plan and associated projects adhere to the requirements of Federal ICAM Roadmap and follow emerging direction from federal policymakers, NIST standards and guidelines, and ICAM technical working groups. The Segment Architect also interfaces with the NRC Enterprise Architecture program, and NRC IT governance and architecture councils, to ensure that ICAM projects integrate effectively with other agency programs and business needs.
Customer	
System Owners	The System Owners are responsible for the security posture of the agency systems and for complying with the NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. They are responsible for complying with the agency's security policy and the associated security procedures. They are also responsible for systems' adherence to the agency's enterprise architecture plan, including the ICAM segment architecture. System owners interact with the ICAM Program to accomplish this.
System ISSOs	ISSOs advise their system owner on all aspects of ICAM security, including complying with the agency's security policy and the associated security procedures.
Application Managers	Application managers are responsible for the development, enhancement, and operation of agency applications, including ICAM features.
System Administrators	System administrators install and configure system services, including ICAM components, and monitor systems for compliance with ICAM requirements.
Computer Information Security Officer (CISO)	The CISO ensures that the program activities comply with Enterprise Risk Management targets, FISMA requirements, and addresses agency POA&M items, emerging security needs, audit findings and other related security requirements.

Appendix C. Program Responsibilities

The ICAM Program helps ensure that the individual projects and investments that comprise the ICAM program run smoothly, and achieve the expected results within the defined budgetary and schedule constraints. In addition, it provides the agency with a single coordination point for streamlining management of ICAM programs at an operational level. This allows the program to facilitate close cooperation and synchronization between the agency's ICAM stakeholders and the individual ICAM project activities to ensure alignment across the organization. The program is typically responsible for all supporting functions.

Table 12: Governance Responsibilities

ICAM Governance Responsibilities
Plan and coordinate implementation efforts across various ICAM stakeholders and component programs (for example, credentialing, physical access control, logical access control, digital signature, and so forth).
Maintain an enterprise ICAM perspective to ensure alignment of all component programs with organizational objectives.
Serve as a centralized point of contact for ICAM questions, issues, and concerns.
Plan for and secure program funding to execute ICAM capabilities.
Handle communications and outreach to both internal and external stakeholders.
Manage program risks and issues to resolution across agency office boundaries.
Measure program performance.
Ensure proper resource allocation to ICAM programs and projects.
Take responsibility for overall stakeholder management to include internal and external stakeholders.
Review post-implementation evaluations to ensure that forecasted benefits and outcomes of the ICAM program are met.
Provide program status information to oversight organizations such as the Office of Management and Budget (OMB), Office of Inspector General (OIG), and Government Accountability Office (GAO), upon request.
Establish collaboration to provide guidance, identify common agency challenges, identify best practices, and share solutions.

Each of the responsibilities listed in Table 12 above contributes to the overarching governance and support that is critical to ensuring the success of ICAM at the agency. The program provides the agency with a means to ensure agency-wide adoption of ICAM through strong executive buy-in and support. It also ensures alignment with the organization's business need and mission, and enforces compliance with applicable laws, regulations, and policies.

Appendix D. Management Processes

The ICAM Program drives the adoption of management processes; especially, communication management, risk management, and performance management.

D.1. Communication Management

Communication at all levels is critical for the success of any program in order to facilitate support with stakeholders at various levels in the agency. In order to communicate consistently and effectively, the *ICAM Program Guidance* document addresses the communication management strategy. Some goals of the plan include the distribution of project information, management of stakeholders' expectations, and communication of project performance.

When creating the communications plan, the ICAM Program analyzes the stakeholders that make up the audience and tailor the message and delivery media in such a way that produces the desired response. The goal of the plan is to keep stakeholders regularly informed and involved by providing appropriate and well-structured communications, ultimately helping to foster and maintain stakeholder support and reduce risk.

D.2. Risk Management

Risk management involves the identification of policies, procedures, and practices, as well as the analysis, assessment, control, and avoidance of threats to the continuing efficiency, effectiveness, and success of program operations. Due to the complexity of ICAM management and its inter-office involvement, risks that threaten the success of the ICAM program can have sweeping effects. Therefore, proactive risk management is paramount within the program.

The *Program Guidance* addresses how risks are measured for the ICAM program, provides a process for identifying the appropriate response, and assigns roles and responsibilities for various stages in the process.

The *ICAM Risk Registry* aides in managing, assigning, and tracking risk events. The risk registry defines the risk cause, the risk parameters, and the effects, should the risk be realized. It also lists the date that the risk was identified, how the risk was resolved, whether the resolution was effective, and the owner of the risk or issue. Reviews and updates to the risk registry are incorporated into ongoing ICAM management processes.

D.3. Performance Management

Performance measures for the management and oversight functions contribute to the effectiveness and quality improvement of the ICAM Program. Assigning performance measurements to the program provides decision makers and stakeholders with a useful tool to monitor progress, determine program effectiveness, and identify areas that need more funding or continued process improvement.

In addition to mandatory reporting requirements, the ICAM Program uses performance reporting to improve alignment with the ICAM segment architecture and to quantify the benefits of the agency's ICAM investments.

The *ICAM Program Guidance* addresses how the program incorporates ICAM metrics into its program management practices. The plan also addresses the program's reporting practices.

Moreover, the program incorporates relevant metrics into the OMB Exhibit 300 business case submissions for all ICAM investments to track information and to demonstrate investment value to the agency.

D.4. Acquisition Management

During the acquisition of products and services, the ICAM Program complies with regulations and policies: the primary policy being the NRC Management Directive 11.1. This directive complies with Federal Acquisition Regulation (FAR), which sets forth the rules governing the federal acquisition process and includes several clauses specifically relevant to the ICAM Program.

When purchasing products and services for HSPD-12 implementation, the program follows the OMB M-06-18 memorandum and the Approved Products List (APL) of the Federal Information Processing Standards 201 (FIPS 201) Evaluation Program.

In addition to the APL, the ICAM Program uses several other activities from the Federal ICAM Initiative to identify and recognize specific categories of products and services that meet advertised criteria to support other functions within the program.

- For Path Discovery and Validation (PDVAL) products, the program consults the Federal ICAM Qualified Validation list for approved products. These products are validated through the Public Key Interoperability Test Suite (PKITS) to confirm compatibility and interoperability of solutions within the Federal Bridge Certification Authority (FBCA) operating community.
- For commercial Identity Providers, the program consults the Federal ICAM Trust Framework Provider list of identity providers that are approved for use by the Federal Government.
- For non-federally issued PIV cards, the program consults the Federal ICAM list of non-federal card issuers whose Personal Identity Verification Interoperability (PIV-I) cards are approved for use by the Federal Government.

In addition to the requirements governing federal acquisitions, the program uses the GSA Schedules. The GSA Schedules provide quick, flexible, cost-effective procurement solutions and assist in compliance by including approved products. The benefits provided to the ICAM Program by schedules result in reduced risk and, when applied, allow the agency to achieve the ICAM goals of cost- effectiveness and efficiency. The program uses two of GSA's schedules: IT Schedule 70 and Schedule 84.

The *ICAM Program Guidance* addresses how the ICAM program uses these resources to achieve more competitive rates and potentially lower implementation costs, shorter procurement time, reduced complexity and effort required to perform due diligence, and elimination of non-compliance with standards and requirements.

D.5. Privacy Management

The ICAM Program owns the agency Privacy Act System of Records NRC-45, "Digital Certificates for Personal Identity Verification." This system collects and stores significant privacy data about individuals inside and outside the NRC, to meet federal credentialing requirements. Consequently, the program team must mitigate potential privacy risks, and provide appropriate security for the identity and credential management systems. For this reason, privacy is considered an essential component and mission critical objective of ICAM and the program

ensures that implementers understand the privacy principles and that they integrate those principles with their ICAM initiatives.

The *ICAM Program Guidance* describes how the program addresses the Fair Information Practice Principles and discusses how it assimilates those principles as part of the ICAM Program. The information and guidance presented in that plan assist the agency in providing answers to several common ICAM-related privacy questions, including:

- What are the Fair Information Practice Principles and how do they apply to the agency‘s ICAM program?
- What processes must the agency complete in order to meet applicable privacy requirements?

D.6. Incorporate ICAM into Existing Processes

In addition to ICAM-specific systems and processes, there are numerous other systems and processes within the agency that are affected by the implementation of the ICAM segment architecture. The *ICAM Program Guidance* addresses how the program integrates the ICAM segment architecture with these other systems and processes.

The plan specifically looks at the integration with management accountability processes, capital planning processes, project management processes, and security and risk management processes as well as with the enterprise architecture plan.