Recommendations for Implementing FICAM on U.S. Secret Networks

CIO COUNCIL

COMMITTEE ON NATIONAL SECURITY SYSTEMS

CNSS

SYSTEMS SECURITY FOR THE 21st CENTURY

22 January 2013

This page intentionally left blank.

MESSAGE FROM THE CO-CHAIRS

Increasing efficiencies through interoperability has always been a goal for both National Security Systems (NSS) and non-NSS alike. Through responsible sharing of information and re-use of enterprise capabilities, we have the opportunity to more efficiently execute mission goals while saving valuable resources. In light of recent events and the October 7, 2011 Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, secure information sharing is more of a priority than ever. Together we are tasked with creating a unified Identity, Credential, and Access Management (ICAM) capability for interoperability across the Federal Secret Fabric.

This report represents the next in a series of steps towards meeting these interoperability goals. As an extension of the *Gap Analysis Between the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM) and United States (U.S.) Secret Networks*, this document provides a series of recommendations, objectives, and suggested activities focused on closing the gaps identified in the aforementioned report as well as laying the foundation for the *FICAM Implementation Plan for the Secret Fabric*. Together, this body of work will help guide Federal ICAM governing bodies, Federal Departments, and Agencies as they implement the ICAM capabilities compliant with the requirements embodied within the *FICAM Roadmap and Implementation Guidance* on the Federal Secret Fabric.

We would like to thank the Department of Defense (DoD), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Department of Homeland Security (DHS), Department of Justice (DOJ), Department of State (DOS), National Geospatial-Intelligence Agency (NGA), and the Central Intelligence Agency (CIA) for playing a key role in developing these recommendations by participating in interviews to give a snapshot of their current Secret networks and identifying critical considerations that will help guide a successful implementation of FICAM on the Secret Fabric.

a. Friedman

Arthur R. Friedman	Chi Hickey
NSS IdAM Working Group Co-Chair	NSS IdAM Working Group Co-Chair

This page intentionally left blank.

EXECUTIVE SUMMARY

Threats to Federal information systems are rising as demands for sharing of information and intelligence between Federal Departments and Agencies increase. It is essential that the Federal Government devise an approach that addresses both challenges without compromising the ability to achieve either objective. Developing a common governance framework and set of Identity, Credential, and Access Management (ICAM) capabilities that enhance the security of our systems by ensuring that only authorized persons and systems from different Federal components have access to necessary information is a high priority. The *Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance* was developed to address the need for secure information sharing capabilities across the breadth of the Federal Government.

A recent gap analysis conducted to determine gaps between the current state of the Secret Fabric and FICAM revealed substantive differences between levels of adoption of this framework and served as the catalyst for this document. In addition to varying levels of FICAM maturity, the gap analysis also showed significant variations in levels of sharable information, connectivity, and governance structures which further complicate the aim of a common FICAM framework across the Secret Fabric.

Using the gap analysis as a starting point, this document provides four major recommendations:

- Establish and Empower a Governance Structure for ICAM on All Networks
- Develop a Common Interoperable ICAM Architecture for the Secret Fabric
- Transition to a Common Interoperable ICAM Architecture
- Prepare for the Evolution of ICAM on the Secret Fabric as New Technology Emerges and New Mission and Business Needs Arise

The following progress chart summarizes the recommendations with objective end states and suggested activities required to accomplish the objectives along a snapshot of status of ICAM on the Secret Fabric as of the publication date of this document. These recommendations, objectives and activities will be included in the *FICAM Implementation Plan for the Secret Fabric* currently under development by the National Security Systems (NSS) Identity and Access Management (IdAM) Working Group under the guidance of the Program Manager for the Information Sharing Environment (PM-ISE).

Status icons are represented by the following.

● **On Track**. Line item is on track and progressing as expected

◑ **Moderate Progress**. Line item has made some progress but needs attention.

○ **At Risk**. Line item is not yet started or needs significant attention.

<u>*Note about terminology:*</u> In this document, the term “FICAM” specifically refers to the *FICAM Roadmap and Implementation Guidance* and the set of requirements embodied within the FICAM program. The term “ICAM” is used to refer to the broad set of ICAM functional capabilities needed to ensure a secure information sharing infrastructure. “Implementing FICAM on the Secret Fabric” refers to applying the FICAM requirements to

the ICAM capabilities resident on the Secret Fabric. “Implementing ICAM capabilities” refers to the development and deployment of ICAM technologies on the Secret Fabric.

Recommendation/Objective/Activity	**Status**	**Comments**
Recommendation 1: Establish and Empower a Governance Structure for ICAM on all networks.	◑	While existing policiy establishes authorities for each network [Federal Chief Information Officer (CIO) Council is responsible for the Unclassified fabric, Office of the Director of National Intelligence (ODNI) CIO is responsible for the TS/SCI fabric, and E.O. 13587 created the Senior Information Sharing and Safeguarding Steering Committee (SISSSC) which designated the Committee on National Security Systems (CNSS) as the governance authority for the Secret Fabric], gaps remain in the governance structures needed to manage the ICAM capabilities, ensure interoperability, and establish comprehensive ICAM policy for the Federal Government.
Objective 1.1: Have an efficient governance structure for ICAM on the Secret Fabric.	◑	The CNSS is developing a governance structure for the Secret Fabric. They established the Architecture Panel and Information Sharing Panel to provide technical capability and interoperability governance on the Secret Fabric.
Activity 1.1.1: Identify and analyze existing ICAM governance structures and lines of authority for overlaps and gaps.	◑	Currently the CNSS is performing this activity for the Secret Fabric. Gaps remain in the full picture of ICAM governance across the Federal Government and how each Department or Agency governance structure should integrate with the Federal Governance structures.

Recommendation/Objective/Activity	Status	Comments
Activity 1.1.2: Assign responsibilities for coordination and implementation of FICAM on the Secret Fabric to the appropriate stewards to ensure a minimum set of ICAM capabilities is uniformly deployed.	◑	The Information Sharing and Access – Interagency Policy Committee (ISA IPC) has overall authority for establishing the strategy for implementation of ICAM on the Secret Fabric; CNSS is responsible for coordinating governance; and the Federal CIO Council and its subordinate ICAM Steering Committee (ICAMSC) has responsibility for operationalizing ICAM capabilities on the Secret Fabric. However, gaps remain in responsibility assignments for specific ICAM capabilities and ICAM on the Secret Fabric objectives.
Activity 1.1.3: Establish policy to address governance gaps and mandate adherence to capability deployment as set forth in the *FICAM Implementation Plan for the Secret Fabric*.	◑	CNSS has overall responsibility to establish policy and address governance gaps in ICAM for the Secret Fabric. They also have the authority to mandate adherence to established policy as defined by their authority under the SISSSC. Once the Implementation Plan is published, the CNSS will be responsible for establishing the metrics and management structures to ensure successful implementation – including the publication of relevant policy.
Activity 1.1.4: Publish *FICAM Implementation Plan for the Secret Fabric*.	●	This activity is currently under development by the ISA-IPC and the NSS IdAM Working Group (WG) under the authority of the Federal CIO Council, CNSS, and PM-ISE – although a final signatory authority has not yet been determined.

Recommendation/Objective/Activity	Status	Comments
Recommendation 2: Develop a Common Interoperable ICAM Architecture for the Secret Fabric	○	The CNSS Architecture Panel is currently capturing the as-is state of the Secret Fabric and working closely with the Information Sharing Panel and the ICAMSC to identify specific architecture requirements for the future of ICAM on the Secret Fabric. Several activities are underway; however there is currently no consolidated objective architecture for the Secret Fabric.
Objective 2.1: Have a consolidated set of short-term interoperability and information sharing requirements for ICAM capabilities on the Secret Fabric	○	While multiple requirements exist from numerous authorities, there is no consolidated set of comprehensive requirements for interoperability or information sharing on the Secret Fabric. The *FICAM Implementation Plan for the Secret Fabric* will, among other things, identify specific activities that will enable the consolidation and enforcement of these requirements through an established governance structure.
Activity 2.1.1: Consolidate and document current and near-term (within 2 years) operational capability requirements for ICAM on the Secret Fabric.	◑	Through the CNSS Architecture Panel and Information Sharing Panel, the CNSS is driving the development of an architecture and set of objective requirements for the Secret Fabric. Under authority granted by the *National Strategy for Information Sharing and Safeguarding* (NSISS), the ICAMSC is undergoing efforts to expand the applicability and amount of detail provided by the *FICAM Roadmap and Implementation Guidance* to include specific capability requirements for the Secret Fabric that will be incorporated by the CNSS to satisfy this activity.

Recommendation/Objective/Activity	Status	Comments
Activity 2.1.2: Develop FICAM implementation guidance specific to the Secret Fabric - Develop addendum to *FICAM Roadmap and Implementation Guidance* to address differences between FICAM and ICAM on the Secret Fabric requirements.	○	The Federal CIO Council ICAMSC is currently revising the *FICAM Roadmap and Implementation Guidance* to identify requirements that are inclusive of all fabrics including the Secret Fabric. As new and specific requirements differences are noted by the CNSS Architecture Panel, they will be noted and incorporated into future versions of the FICAM.
Objective 2.2: Have an architecture that supports interoperable Public Key Infrastructure (PKI) with hardware or software tokens for network logon and selected mission applications.	◑	Departments and Agencies are at varying levels of PKI adoption for the Secret Fabric. Most are still using user ID and password tokens. The NSS PKI is in operation and is currently in use by a few Departments and Agencies. Some organizations are waiting for the establishment of a Common Service Provider (CSP) service offering to be provided by the Department of Defense (DoD) (IOC expected June 2013) before they will deploy PKI tokens and interoperate with the NSS PKI.
Activity 2.2.1: Identify dependencies and mission impacts of the PKI implementation timeline.	●	Departments and Agencies are currently assessing the dependencies and impacts of delays and complications inherent in the establishment of the CSP. An executive understanding of mission impacts related to the NSS PKI mandate needs to be developed.
Activity 2.2.2: Provide technical implementation guidance for PKI and PK-enabled (PKE) systems.	◑	DISA is currently developing technical implementation guidance for NSS PKI implementation under the direction of CNSS Member Governing Body (MGB).

Recommendation/Objective/Activity	Status	Comments
Objective 2.3: Have an architecture and requirements that support interoperable information sharing and protection capability.	◑	The CNSS Architecture and Information Sharing Panels are generating architecture and a set of information sharing and protection requirements for the Secret Fabric. It is incumbent upon each of the Departments and Agencies to ensure they establish subordinate architectures and requirements for information sharing and protection. Currently, some Departments and Agencies have more mature information sharing capabilities than others.
Activity 2.3.1: Identify information sharing requirements based on mission and business needs.	◑	The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and the National Strategy for Information Sharing and Safeguarding (NSISS) define and mandate these requirements and charge the PM-ISE with establishing methods for managing information sharing needs. Currently, information sharing needs are managed on an ad-hoc basis between agencies. This activity provides for a more robust way of documenting and managing the information sharing interfaces across the Secret Fabric.
Activity 2.3.2: Identify digital policy requirements for authorization.	○	SISSSC is currently identifying an approach to address this need with inputs from Departments and Agencies and will ensure a common methodology for all classified fabrics. The National Security Agency (NSA), as the executive agent for Digital Policy for the IC, will play a significant role in defining this approach.

Recommendation/Objective/Activity	Status	Comments
Activity 2.3.3: Identify common attributes needed to protect and share enterprise shared information.	○	SISSSC is currently identifying an approach to address this need with inputs from Departments and Agencies and will ensure a common methodology for all classified fabrics. The Intelligence Community (IC) and the DoD have made significant progress in defining and maintaining attributes needed for authorization decisions and their work should be significantly leveraged.
Activity 2.3.4: Mandate the provisioning / mapping of minimum attributes needed to satisfy enterprise information sharing requirements.	○	No progress. This activity is dependent upon the identification of a minimum set of authorization attributes (Activity 2.3.3).
Activity 2.3.5: Establish information sharing architecture and interface requirements	◑	The CNSS Architecture and Information Sharing Panels are generating architectural design documents and a set of information sharing and protection requirements for the Secret Fabric. The PM-ISE is generating an Interoperability Reference Architecture that will help establish these requirements.
Recommendation 3: Transition to a Common Interoperable ICAM Architecture.	◑	The NSISS mandates FICAM as the common identity and access management architecture on all fabrics. To meet that target, a set of transition objectives and activities is necessary to ensure that legacy capabilities transition cleanly to the target state with minimal mission impact. While the *FICAM Implementation Plan for the Secret Fabric* details the milestones necessary for implementation of FICAM requirements in the near term, long term transition of legacy ICAM capabilities within each Department and Agency should be coordinated.

Recommendation/Objective/Activity	Status	Comments
Objective 3.1: Have a transition plan and identify the governance body required to manage the transition across agencies	○	Authority for managing the transition has not yet been determined.
Activity 3.1.1: Assemble a project team charged with coordinating Department and Agency transition to the target end-state.	○	The governance structure identified in Objective 1.1 will identify the coordinating project team. This has not yet started.
Objective 3.2: Deploy a comprehensive, interoperable identity management, authentication, authorization, and information sharing capability on the Secret Fabric.	○	Some progress has been made (e.g., NSS PKI), however, without a set of end-state requirements and architecture, the Departments and Agencies do not have the ability to deploy a comprehensive set of ICAM capabilities compliant with the FICAM requirements. Objectives and activities above will provide the framework and prerequisite efforts for deploying ICAM capabilities in an interoperable and integrated manner.
Activity 3.2.1: Implement interoperable authentication capabilities with PKI on the Secret Fabric.	◑	NSS PKI is already implemented and the CSP is being established. Departments and Agencies are at varying degrees of adoption with regards to PKI and PKE. An integrated implementation plan has not yet been developed.
Activity 3.2.2: Implement interoperable information sharing and protection capabilities on the Secret Fabric.	◑	The majority of the responsibility for completing this activity lies with the Departments and Agencies. Departments and Agencies are at various levels of completion across the Secret Fabric – most awaiting a set of definitive and authoritative requirements that establish the desired end-state for ICAM on the Secret Fabric. The ISA IPC will need to identify additional shared enterprise capabilities and owning service providers as well as enforcement mechanisms for meeting ICAM on the Secret Fabric requirements.

Recommendation/Objective/Activity	Status	Comments
Activity 3.2.3: Transition legacy ICAM systems to meet ICAM on the Secret Fabric and interoperability requirements.	◑	The majority of the responsibility for completing this activity lies with the Departments and Agencies. Departments and Agencies are at various levels of completion across the Secret Fabric – most awaiting a set of definitive and authoritative requirements that establish the desired end-state for ICAM on the Secret Fabric. The ISA IPC will need to identify additional shared enterprise capabilities and owning service providers as well as enforcement mechanisms for meeting ICAM on the Secret Fabric requirements.
Recommendation 4: Prepare for the Evolution of ICAM on the Secret Fabric as New Technology Emerges and New Mission and Business Needs Arise.	○	As initial target architectures are implemented, consideration must be paid to the evolution and emergence of new capabilities that need to be incorporated into the existing requirements.
Objective 4.1: Assign an existing governance body to survey technology and trends and evaluate them against short-term and long-term architectural requirements.	○	The Federal CIO Council and the ICAMSC has overall responsibility for maintaining the FICAM requirements and architecture. The CNSS Architecture Panel will be responsible for incorporating new technologies into the architectural requirements for ICAM capabilities on the Secret Fabric.
Activity 4.1.1: Assign responsibilities dedicated to perform research on emerging technologies and updated policy.	○	The Federal CIO Council has overall responsibility for determining the direction of ICAM capabilities on all networks. Executive Agency assignments have been made for a number of capabilities (e.g., NSA is the Executive Agent for Digital Policy, etc.) but the need for additional responsibility assignments remains.

Recommendation/Objective/Activity	**Status**	**Comments**
Objective 4.2: Have an acquisition process that incorporates ICAM on the Secret Fabric and interoperability requirements into acquisition approvals.	○	The NSISS mandates FICAM on all networks. However, no process currently exists to ensure FICAM requirements are incorporated into new acquisitions.
Activity 4.2.1: Establish acquisition criteria for new ICAM systems that ensure new systems meet ICAM on the Secret Fabric and interoperability requirements.	◑	Although acquisition programs are responsible to ensure FICAM requirements are incorporated into their acquisitions, currently there are few mechanisms to enforce the inclusion of those requirements.
Activity 4.2.2: Engage acquisition process mechanisms to align and enforce ICAM on the Secret Fabric and interoperability requirements.	◑	The Federal CIO Council has the overall responsibility to ensure FICAM requirements are injected into Federal and Department and Agency acquisition processes.
Objective 4.3: Have a management plan for updating ICAM on the Secret Fabric architecture and project plans.	○	The *FICAM Implementation Plan for the Secret Fabric* will address responsibilities for updating architecture and milestones for transition and sustainment activities for ICAM capabilities on the Secret Fabric.
Activity 4.3.1: Develop a management plan for approving and processing changes to approved ICAM on the Secret Fabric architecture and project plans.	○	The *FICAM Implementation Plan for the Secret Fabric* will address responsibilities for updating architecture and milestones for transition and sustainment activities for ICAM capabilities on the Secret Fabric.

Table of Contents

This page intentionally left blank.

1 BACKGROUND

Over the past ten years, the Federal Government has made concerted advances in the development and implementation of Identity, Credential, and Access Management (ICAM). This progress includes capabilities designed to promote interoperability, assured information sharing, and efficiencies of scale across all agencies within the Federal Government. Recently, several high-visibility events have focused attention on classified networks with a renewed emphasis on information protection within the information sharing paradigm.

In response to these and other drivers, Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* was published on October 7, 2011. This new executive order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks including the coordinated interagency development and reliable implementation of policies and minimum standards. Pointing to recent events as the driver for near-term action, the executive order highlighted the partnership among the Federal Chief Information Officer (CIO) Council / Information Security and Identity Management Committee's (ISIMC's) ICAM Subcommittee, the joint National Security Staff / Program Manager – Information Sharing Environment (PM-ISE) Information Sharing and Access Interagency Policy Committee's (ISA IPC) Assured Secret Network Interoperability (ASNI) Working Group, and Committee on National Security Systems' (CNSS's) Identity and Access Management (IdAM) Working Group as the mechanism for developing and implementing "a holistic solution for efficient, interoperable ICAM for the Federal Secret Fabric"[1]and established the Senior Information Sharing and Safeguarding Steering Committee (SISSSC) to oversee efforts to improve the Federal Secret Fabric.

In response to this directive, the ICAM Subcommittee (ICAMSC), ASNI Working Group (WG), and IdAM WG collaborated to evaluate the applicability of the *Federal ICAM Roadmap and Implementation Guidance* (FICAM) to United States (U.S.) Secret networks and identify obstacles to the future interoperability of the Federal Secret Fabric. The resulting *Gap Analysis Between the FICAM and U.S. Secret Networks* document was based on the analysis of the ICAM capabilities of six predominant Secret networks in use within the Federal Government:

- Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNet)
- Federal Bureau of Investigation (FBI) Network (FBINet)
- Department of Energy-National Nuclear Security Administration (DOE-NNSA) Enterprise Secure Network (ESN)
- Department of Homeland Security (DHS) Homeland Secure Data Network (HSDN)
- Department of Justice (DOJ) Justice Consolidated Office Network - Secret (JCON-S)
- Department of State (DOS) ClassNet

In June 2012, the National Security Systems (NSS) IdAM Working Group, under the direction of CNSS and ICAMSC, was directed to conduct follow-up interviews with the original six agencies to gauge any progress made since the first interviews, discuss any comments the agencies had regarding the gap analysis, and collaborate on detailed recommendations to address the identified gaps. Two additional agencies were also interviewed as part of this follow on task: the Central Intelligence Agency (CIA) and

[1] Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; 07 October 2011.

the National Geospatial-Intelligence Agency (NGA). This report contains the recommendations that were developed from these interviews in conjunction with the gap analysis.

On 20 December, 2012, the President signed the *National Strategy for Information Sharing and Safeguarding* (NSISS) which directs the Federal CIO Council to extend and implement the *FICAM Roadmap and Implementation Guidance* across all security fabrics. Upon completion of these recommendations and in accordance with the NSISS, the CNSS, in coordination with the Federal CIO Council ICAMSC, will release the *FICAM Implementation Plan for the Secret Fabric* – providing a set of activities and milestones for Departments, Agencies, and governance bodies to execute the implementation of ICAM on the Secret Fabric.

1.1 Purpose

The purpose of this document is to provide Federal Departments and Agencies with recommendations for implementing an interoperable set of ICAM capabilities on the Secret Fabric that are compliant with the requirements represented in the FICAM. This document outlines high level recommendations, subordinate objectives, and a set of activities necessary to implement ICAM on the Secret Fabric. Additionally it defines responsibilities, categorizes the status of current progress and outlines a set of considerations for successful implementation. These recommendations also provide an understanding of the government-wide scope of activities for implementing FICAM on the Secret Fabric to guide funding and acquisition decision making.

1.2 Scope

This document provides recommendations applicable to Federal IT, Information Sharing, and ICAM governance bodies; Department and Agency CIO's, and IT and ICAM infrastructure managers; and Federal acquisition and research and development components. While this document provides the recommendations for transitioning to a common interoperable ICAM architecture including managing the transition across agencies and deployment of an interoperable information sharing capability on the Secret Fabric, more detailed guidance including timelines and prioritization of activities will be provided in the subsequent *FICAM Implementation Plan for the Secret Fabric*.

2 RECOMMENDATIONS

All Objectives and Activities are structured under four high-level recommendations.

- Establish and empower a governance structure for ICAM on all networks
- Develop a common interoperable ICAM architecture for the Secret Fabric
- Transition to a common interoperable ICAM architecture
- Prepare for the evolution of ICAM on the Secret Fabric as new technology emerges and new mission and business needs arise

These recommendations are designed to cover all critical success factors for improving the security posture, ability to share information, and efficiency of ICAM capabilities on U.S. Secret Networks to be compliant with the *FICAM Roadmap and Implementation Guidance*. Each recommendation consists of a set of objective future states of FICAM implementation which, in turn, consist of a set of activities designed to achieve each objective.

2.1 *Recommendation*: Establish and Empower a Governance Structure for ICAM on All Networks

While a high level structure exists for overall responsibility of networks in various security fabrics, additional organizational components, policies, and directives are needed to fill gaps in the current FICAM governance structures for Unclassified, Secret, and Top Secret. Overall, the Federal CIO Council has authority over the Unclassified Fabric, Office of the Director of National Intelligence (ODNI) CIO has authority over the Top Secret Fabric, and Executive Order 13587 created the SISSSC which has designated the CNSS as the governance authority for the Secret Fabric. While no single authority has oversight over FICAM capability evolution on all networks, the NSISS empowers the Federal CIO Council – and consequently the ICAMSC – with the responsibility for extending and implementing the *FICAM Roadmap and Implementation Guidance* across all security fabrics. In this role, it will be incumbent upon the ICAMSC to help establish formal relationships between each fabric's authorities to ensure coordination, cooperation, and consistent implementation of FICAM capabilities on all three fabrics.

2.1.1 *Objective*: Have an efficient governance structure for ICAM on the Secret Fabric

The future governance structure for ICAM on the Secret Fabric is comprehensive, cohesive, and tightly integrated with the structures governing Federal implementation of FICAM on all security fabrics as well as with the internal governance structures of each Department and Agency hosting a Secret network. Where possible, overlaps in authority are leveraged to ensure that forward progress of FICAM implementation and that no activities are overlooked. Responsibilities for FICAM implementation are clearly defined and acknowledged by owning organizations. Redundant working groups are dissolved and conflicts are resolved at the lowest levels possible, only escalated to the CNSS Subcommittee when all other avenues are exhausted. Newly identified gaps in authority or responsibility are quickly routed to the appropriate authority to identify an owner or policy need.

2.1.1.1 **Activity**: Identify and analyze existing ICAM governance structures and lines of authority for overlaps and gaps

This activity includes identifying existing steering committees and working groups that currently contribute to ICAM-related activities for the Secret Fabric and documenting the ICAM-related sections of their charters, authorities, current participation, lines of communication, and major endeavors.

Artifacts. Documented summary of ICAM on the Secret Fabric Governance Structures, Authorities, and Lines of Communication.

Responsibilities. The Information Sharing and Access Interagency Policy Committee (ISA IPC) is responsible for coordinating this activity. All ICAM on the Secret Fabric governance or advisory bodies will support CNSS by providing current charters, membership, and lines of communications with other NSS organizations and ICAM on the Secret Fabric governing bodies.

Status. The SISSSC assigned the governance responsibility of the Secret Fabric to the CNSS. CNSS chartered the Architecture Panel and the Information Sharing Panel to determine governance and technical requirements for the Secret Fabric. Additionally, CNSS stood up the CNSS Enterprise Risk Management Board (CERMB) which will work with the Architecture Panel to manage risk for the Secret Fabric. Despite progress, gaps remain in governance responsibilities for specific ICAM capabilities.

Considerations. It will be important to include representatives of Department and Agency ICAM organizations to help identify needs from higher authorities and gaps in existing governance. Note that not all Departments and Agencies are organized similarly with a dedicated ICAM organization. Often ICAM responsibilities are split between Security, Engineering, IT, and Mission entities within the Department or Agency so ensuring the right governance participants empowered to make decisions on behalf of the Department or Agency is critical. This activity is complicated by the challenges of getting components to share information due to the stove-piped nature of their secret networks. It is recommended that each Department and Agency conduct a similar activity to identify their own ICAM governance and how they will integrate with Federal ICAM governance structures. Without a specifically assigned set of governance interfaces, policy decisions and compliance will vary from Department to Department.

2.1.1.2 <u>**Activity**: Assign responsibilities for coordination and implementation of FICAM on the Secret Fabric to the appropriate stewards to ensure a minimum set of ICAM capabilities is uniformly deployed.</u>

At a minimum, stewards should be assigned to the following ICAM on the Secret Fabric capabilities:

- Information Sharing Needs Identification (PM-ISE ISA IPC)
- Identity Lifecycle Management
- Identity Attribute Sharing/Protection
- Digital Policy Development and De-confliction (PM-ISE ISA IPC / NSA)
- Resource Tagging / Metadata Management
- Public Key Infrastructure (PKI) Implementation and Public Key Enablement (PKE) (CNSS PKI Member Governing Board (MGB))
- Auditing and Insider Threat Detection (SISSSC)
- Cross Domain Management (UCDMO)
- Interoperability Standards and Specifications (PM-ISE ISA IPC)
- Risk Management (SISSSC)
- Future Planning/Technology Evolution

Artifacts. Input to policy and coordination and maintenance of a unified functional delivery roadmap for FICAM services on the Secret Fabric. Collection and coordination of quarterly progress report against metrics established by the *FICAM Implementation Plan for the Secret Fabric*. These metrics should reinforce progress toward milestones included in the unified functional roadmap for FICAM services delivery on the Secret Fabric.

Responsibilities. The Information Sharing and Access – Interagency Policy Committee (ISA IPC) has overall authority for establishing the strategy for implementation of FICAM on the Secret Fabric; CNSS is responsible for coordinating governance; and the Federal CIO Council and its subordinate ICAM Steering Committee (ICAMSC) has responsibility for operationalizing ICAM capabilities on the Secret Fabric. However, gaps remain in responsibility assignments for specific ICAM capabilities and FICAM on the Secret Fabric objectives.

Status. There remain gaps in responsibility assignments for specific ICAM capabilities and FICAM on the Secret Fabric objectives. Steward assignments are developed by SISSSC and established in the NSISS but are not yet fully assigned.

Considerations. This will be further documented and addressed in the *FICAM Implementation Plan for the Secret Fabric*.

2.1.1.3 **Activity**: Establish policy to address governance gaps and mandate adherence to capability deployment as set forth in the *FICAM Implementation Plan for the Secret Fabric*

Governance gaps exist, in part, because current efforts to improve ICAM capabilities have not been fully coordinated and Departments and Agencies are at different levels of adoption. CNSS has been directed to stand up the governance capability and is working through the IdAM Working Group which it co-chairs with the ICAMSC.

Artifacts. Guidance and Policy.

Responsibilities. CNSS has overall responsibility to establish policy and address governance gaps in ICAM for the Secret Fabric. They will also have the authority to mandate adherence to established policy as defined by their authority under the SISSSC. Once the Implementation Plan is published, the CNSS will be responsible for establishing the metrics and management structures to ensure successful implementation.

Status. The CNSS/ICAMSC NSS IdAM WG is currently developing a CNSS Policy focused on Identity and Access Management that will be published in late government Fiscal Year 2013 (FY13).

Considerations. This will be further documented and addressed in the *FICAM Implementation Plan for the Secret Fabric*.

2.1.1.4 **Activity**: Publish *FICAM Implementation Plan for the Secret Fabric*

The *FICAM Implementation Plan for the Secret Fabric* should include a list of activities to implement FICAM on the Secret Fabric, responsibilities, timelines, authorities, and financial considerations including cost estimates. Additionally, the plan should include a concept of operations for the implementation and management of FICAM on the Secret Fabric as well as methods for managing trust between organizations, a transition plan for the evolution of legacy capabilities, and metrics for validating the success and impact of FICAM capability deployment.

Artifacts. *FICAM Implementation Plan for the Secret Fabric*.

Responsibilities. The ISA IPC, CNSS, and Federal CIO Council share responsibility for completing this activity, however a final signatory authority has not yet been determined.

Status. This activity is currently under development by the ISA-IPC and the NSS IdAM WG under the authority of the Federal CIO Council, CNSS, and the Program Manager for the Information Sharing Environment (PM-ISE). A final draft is due out for coordination in late February 2013.

Considerations. It is important to note that, due to the diverse fiscal constraints and varying levels of FICAM capability maturity between Departments and Agencies, deployment of target-state FICAM capabilities will be staggered requiring additional mechanisms for interoperability until all Departments and Agencies meet SISSSC Initial Operating Capability (IOC) and Full Operating Capability (FOC) dates. NSISS policy decisions expected to be published in Spring 2013 may affect the the execution of the implementation plan.

2.2 *Recommendation:* Develop a Common Interoperable ICAM Architecture for the Secret Fabric

Just as Departments and Agencies are at different levels of compliance and maturity with FICAM implementation, their requirements and architectural implementations also differ. Consolidation of short-term requirements prior to the development of long-term ICAM capability goals is a necessity to give Departments and Agencies clear direction for acquisition and development decisions. A common ICAM architecture is necessary to implement secure and FICAM-compliant interoperability.

2.2.1 *Objective:* Have a consolidated set of short-term operational interoperability and information sharing requirements for ICAM capabilities on the Secret Fabric

The SISSSC has defined the IOC and FOC for all five priority objectives: removable media, insider threat, enterprise audit, access management and reduced anonymity. This recommendations document is focused on access management and reduced anonymity since they relate directly to ICAM on the Secret Fabric and need to be integrated with various agency plans. It is important to integrate SISSSC IOC/FOC capabilities with current agency plans in order to develop a short-term way forward that takes advantage of current efforts without compromising the longer-term end state.

2.2.1.1 **Activity**: Consolidate and document current and near-term (within 2 years) operational capability requirements for ICAM on the Secret Fabric

While the SISSSC IOC/FOC requirements outline high-level needs for Secret network interoperability, there is no consolidated set of ICAM requirements for the Secret Fabric. Given that the target end-state of ICAM on the Secret Fabric will be many years off, a requirements document – which includes detailed requirements based on IOC – should be developed that captures current and near term requirements to serve as a checklist for evaluating Department and Agency compliance as they progress toward IOC. The need for this should be documented as part of the *FICAM Implementation Plan for the Secret Fabric* and each Department and Agency should address their requirements in their internally focused FICAM implementation plans.

Artifacts. Requirements Document including suggested key performance indicators and a minimum set of interoperability characteristics.

Responsibilities. The Federal CIO Council and ICAMSC in their role as extender and implementer of FICAM on all security fabrics has the primary responsibility to ensure this activity is completed.

Status. Through the CNSS Architecture Panel and Information Sharing Panel, the CNSS is driving the development of an architecture and set of objective requirements for the Secret Fabric. Under authority granted by the NSISS, the ICAMSC is undergoing efforts to expand the applicability and amount of detail provided by the *FICAM Roadmap and Implementation Guidance* to include specific capability requirements for the Secret Fabric that will be incorporated by the CNSS to satisfy this activity. Additionally, PM-ISE is creating an Interoperability Reference Architecture that will have an IdAM appendix based on the FICAM Segment architecture.

Considerations. While this is being addressed in the *FICAM Implementation Plan for the Secret Fabric*, each Department and Agency should extend and tailor these requirements to address their individual capabilities and infrastructures.

2.2.1.2 **Activity**: Develop FICAM implementation guidance specific to the Secret Fabric - Develop an addendum to FICAM Roadmap and Implementation Guidance for differences between FICAM and FICAM on the Secret Fabric requirements

Future development and deployment activities should be focused on the specific needs of the Secret Fabric and the interoperability needs which will sometimes differ from the wider population of Unclassified networks. The need for this should be documented as part of the *FICAM Implementation Plan for the Secret Fabric* and each agency should work with the appropriate ICAMSC working group to document their needs in the updates to the *FICAM Implementation Plan for the Secret Fabric*.

Artifacts. Inputs to the FICAM on the Secret Fabric Addendum in the FICAM Roadmap

Responsibilities. The Federal CIO Council ICAMSC is responsible for this activity.

Status. The ICAMSC is currently revising the *FICAM Roadmap and Implementation Guidance* to identify requirements that are inclusive of all fabrics including the Secret Fabric. As new and specific requirements differences are noted by the CNSS Architecture Panel, they will be noted and incorporated into future versions of the FICAM.

Considerations. Some capabilities may need to have tailored requirements specific to sensitive mission needs that may not be applicable on unclassified networks. For example, the sharing of identity information between Departments and Agencies on the Secret Fabric may entail special requirements for handling and authentication – especially within the Intelligence Community (IC). The FICAM addendum should make provisions for these specific types of requirements.

2.2.2 *Objective:* Have an architecture that supports interoperable PKI with hardware or software tokens for network logon and selected mission applications

An early, required capability for ICAM on the Secret Fabric is to adopt PKI for network logon and secure interoperability in accordance with CNSSD No. 506, dated 9 October 2012. PKI is a core enabling technology for protecting networks and providing secure interoperability and is a predecessor capability for other information sharing strategies and architectures and should be matured early in the effort. This should be addressed in the existing FICAM Segment architecture and CNSS policy. In addition, the SISSSC Common Service Provider (CSP) guidance also addresses this.

Departments and Agencies are at varying levels of PKI adoption for the Secret Fabric. Most are still using user ID and password tokens. The NSS PKI is in operation and is currently in use by a few Departments and Agencies. Some organizations are awaiting the establishment of a Common Service Provider (CSP) service offering to be provided by the DoD (IOC expected June 2013) before they will deploy PKI tokens and interoperate with the NSS PKI.

Overall responsibility for moving this forward rests with ISA IPC and individual Departments and Agencies will have implementation teams assigned to this effort. Due to the varying maturity and timelines for PKI implementation, mandate of PKI for logon and authentication to specific networks and mission applications will impact Departments and Agencies that use major networks (like SIPRNet) as the backbone for their mission applications. This may cause degradation in the current state of interoperability rather than improvement and should be carefully managed to ensure no critical missions are impacted as a result of these mandates.

2.2.2.1 **Activity**: Identify dependencies and mission impacts of the PKI implementation timeline

Being a core enabling technology, PKI will have a significant impact on networks and applications and will have to have its implementation milestones carefully coordinated with other efforts in individual Agencies.

Artifacts. Input to *FICAM Implementation Plan for the Secret Fabric*

Responsibilities. All Governance Bodies, Departments, and Agencies.

Status. Departments and Agencies are currently assessing the dependencies and impacts of delays and complications inherent in the establishment of the CSP. An executive understanding of mission impacts related to the NSS PKI mandate needs to be developed.

Considerations. Without understanding the specific mission impacts of the NSS PKI mandate, unintended interoperability issues may lead to personnel and resource hazards due to mission necessity for connectivity and access to information resources. In an effort to reduce the occurrence and risks associated with these potential problems, an executive mission impact evaluation should be developed.

2.2.2.2 **Activity**: Provide technical implementation guidance for PKI and PK-enabled (PKE) systems

Having architectural and implementation reference models, sample deployments and tier 3 technical support will be critical to the success of implementing what will be unfamiliar technology to some organizations.

Artifacts. Architectural and implementation reference models, sample deployments, and prototypes.

Responsibilities. The CNSS PKI MGB has the responsibility for ensuring completion of this activity.

Status. The Defense Information Systems Agency (DISA) is currently developing technical implementation guidance for NSS PKI implementation under the direction of CNSS PKI MGB.

Considerations. Implementation support could include reference architectures and implementations, pilots, and downloadable prototypes for evaluation and use by Departments and Agencies.

2.2.3 *Objective:* Have an architecture and requirements that support interoperable information sharing and protection capability

Beyond the basic network logon capability, a short-term and medium-term objective is to be able to securely expose, protect, and share information that needs to be shared across the enterprise. The objective architecture will leverage an Attribute Based Access Control (ABAC) model to employ an interoperable identity attribute structure, a robust set of resource attributes or data tags to label resources for authorization decisions, and a comprehensive policy generation and enforcement capability that allows only authorized entities access to the authorized resources.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)section 1016 requires PM-ISE to do this and PM-ISE is creating an Interoperability Reference Architecture that will have an IdAM appendix based on the FICAM Segment architecture.

2.2.3.1 **Activity**: Identify information sharing requirements based on mission and business needs.

Not all applications and information need to be shared across organizational boundaries and it is important to focus time and resources on those requirements that directly impact mission needs and business necessities.

Artifacts. Information Sharing Registry. The Information Sharing Registry serves as a central repository for the types of information that need to be exposed by agencies and shared across the enterprise. As new information sharing requirements arise, organizations should register new types of information to be shared and provide information that will allow authorized users to access necessary systems or data.

Responsibilities. The IRTPA and NSISS define and mandate these requirements and charge the PM-ISE with establishing methods for managing information sharing needs.

Status. Currently, information sharing needs are managed on an ad-hoc basis between agencies. This activity provides for a more robust way of documenting and managing the information sharing interfaces across the Secret Fabric.

Considerations. None.

2.2.3.2 **Activity**: Identify digital policy requirements for authorization

Identify, document, and make machine-readable, the rules that govern authorization for access to enterprise shared information – as these digital policies define who may be allowed access to what resources.

Artifacts. Information protection policies, allowable digital policy models/mechanisms, trust models and trust arbitration methods.

Responsibilities. SISSSC is responsible for ensuring completion of this activity with inputs from Departments and Agencies. The National Security Agency (NSA), as the executive agent for Digital Policy, will play a significant role in defining the technical approach.

Status. SISSSC is currently identifying an approach to address this need with inputs from Departments and Agencies and will ensure a common methodology for all classified fabrics.

Considerations. None.

2.2.3.3 **Activity**: Identify common attributes needed to protect and share enterprise shared information

A set of commonly understood attributes for defining the user and attributes for defining the resource need to be identified to enable the establishment of attribute management and access control mechanisms that may be used to facilitate ABAC for shared information.

Artifacts. Lexicon of shared authorization attributes and Department/Agency-level attribute mapping.

Responsibilities. SISSSC is responsible for ensuring completion of this activity with inputs from Departments and Agencies.

Status. SISSSC is currently identifying an approach to address this need with inputs from Departments and Agencies and will ensure a common methodology for all classified fabrics.

Considerations. The focus of this activity should be identifying the required minimum set of shared attributes rather than a complete lexicon of all attributes thus minimizing the need to de-conflict synonyms and homonyms or map similar attributes across different organizations. The IC/DoD Attribute and Authorization Services Committee (AASC) and the ICAMSC Access Control Attribute Governance (ACAG) WG have made significant progress in defining and maintaining attributes needed for authorization decisions and their work should be significantly leveraged. This effort should also include metadata standards required for discovery and interoperability.

2.2.3.4 **Activity**: Mandate the provisioning/mapping of minimum attributes needed to satisfy enterprise information sharing requirements

Once a set of attributes is identified, it is necessary to mandate the use of those attributes or mandate the ability to map those attributes to Department- or Agency-specific attributes. This ensures that all resources may be protected in the same way using the same methods for authorization.

Artifacts. Policy for using attributes for authorization.

Responsibilities. The CNSS IdAM WG is responsible for establishing policy related to ICAM capabilities on the Secret Fabric.

Status. This activity has not started.

Considerations. None.

2.2.3.5 **Activity**: Establish information sharing architecture and interface requirements

As Departments and Agencies expose new information for information sharing, they will need a common architecture and set of agreed-upon interfaces to be able to interoperate with other Departments and Agencies.

Artifacts. Interoperability Reference Architecture.

Responsibilities. The PM-ISE is responsible for completing this activity.

Status. The CNSS Architecture and Information Sharing Panels are generating architecture and a set of information sharing and protection requirements for the Secret Fabric. The PM-ISE is creating an Interoperability Reference Architecture that will have an IdAM appendix based on the FICAM Segment architecture that will satisfy this activity.

Considerations. Special care needs to be taken to incorporate requirements for privacy, civil rights and civil liberties. These requirements need to be vetted with the appropriate authorities.

2.3 *Recommendation:* Transition to a Common Interoperable ICAM Architecture

NSISS defines FICAM as the target architecture on all fabrics from unclassified through Top Secret. The development and deployment of ICAM on the Secret Fabric capabilities should include spirals of development and deliverables in short delivery timeframes in order to begin to realize benefits as soon as possible and to build momentum for longer term goals. This requires coordinated efforts between government agencies to ensure interoperability between networks in the same fabric does not suffer from asymmetric development of identity management capabilities and sophistication.

2.3.1 *Objective:* Have a transition plan and identify the governance body to manage the transition across agencies

A new or existing governance body will be chartered to coordinate ICAM transition activities across the Secret Fabric and ensure a smooth transition to the target state of a fully secure and interoperable solution.

2.3.1.1 **Activity**: Assemble a project team charged with coordinating Department and Agency transition to the target end-state

The focus of this activity should be on identifying methods for addressing legacy and incompatible solutions within budget constraints. As Departments and Agencies develop their own transition plans, they will need to coordinate the transition of capabilities that have dependencies outside of their organizations.

Artifacts. Identity Federation Coordination Working Group.

Responsibilities. The ISA IPC is responsible for completing this activity.

Status. While there is a proposal before the ISA IPC to stand up the Identity Federations Coordination (IFC) WG, the work of managing the transition to a fully implemented set of ICAM capabilities compliant with FICAM has not yet begun.

Considerations. As new capabilities are planned, developed and deployed, an ongoing evaluation process will need to be performed that appraises the impact on interoperability with Departments and Agencies and can adjust deployment schedules in order to avoid any ruptures in critical interoperability operations.

2.3.2 *Objective:* Deploy a comprehensive interoperable identity management, authentication, authorization, and information sharing capability on the Secret Fabric

Once requirements, authorities, and transition planning is complete, the responsible Departments and Agencies must deploy capabilities to match the objective architecture. These activities will primarily be conducted individually by Departments and Agencies, but should periodically report status to the CNSS IdAM WG.

2.3.2.1 **Activity**: Implement interoperable authentication capabilities with PKI on the Secret Fabric

The first step to establishing an interoperable enterprise on the Secret Fabric is the establishment of interoperable authentication capabilities. This is mandated by CNSS Policy 25.

Artifacts. PKI implementations on the Secret Fabric.

Responsibilities. Mandated by CNSS Policy 25, ISA IPC has the authority to enforce the requirements supported by the Departments and Agencies.

Status. PKI is mandated by CNSS Policy 25 for secret networks and is a key enabling technology for other identity management functions and interoperability. NSS PKI is already implemented and the CSP is being established. Departments and Agencies are at varying degrees of adoption with regards to PKI and PKE. An integrated implementation plan accounting for the idiosyncrasies of each Department and Agency has not yet been developed.

Considerations. As a key enabling technology for specifying trust relationships and enabling secure interoperability between various secret networks, implementing PKI should occur in the early phases of the project plan. Some Departments and Agencies have made more progress than others. A key critical path item is the establishment and availability of services provided by the Common Service Provider. Testing and verification of PKI implementations should include verifying that other Departments and Agencies can authenticate to desired systems with PKI credentials.

2.3.2.2 **Activity**: Implement interoperable information sharing and protection capabilities on the Secret Fabric

Beyond just PKI, developing a secure information sharing architecture, authorization policies, and identifying attributes required for authorization is crucial to providing the ability to quickly and securely access and provide critical information to other organizations.

Artifacts. Interoperable identity and access management capabilities.

Responsibilities. The Federal CIO Council has the responsibility to operationalize FICAM on the Secret Fabric. However, the majority of the responsibility for completing this activity lies with the Departments and Agencies. Additionally, the ISA IPC will need to identify additional shared enterprise capabilities and owning service providers as well as enforcement mechanisms for meeting FICAM on the Secret Fabric requirements.

Status. Departments and Agencies are at various levels of completion across the Secret Fabric – most awaiting a set of definitive and authoritative requirements that establish the desired end-state for ICAM on the Secret Fabric.

Considerations. Development of these capabilities must be carefully coordinated between Departments and Agencies to ensure that critical operations now available do not suffer disruptions when one partner deploys advanced capabilities that the other does not have. Smaller Agencies may need to leverage shared enterprise services to enable full implementation of information sharing and protection capabilities. Note that SISSSC has responsibility for policies for removable media, audit, detecting insider threats, etc. which are narrower in scope than what is suggested by this activity.

2.3.2.3 **Activity**: Transition legacy ICAM systems to meet ICAM on the Secret Fabric and interoperability requirements

The impact to legacy systems must be considered as additional identity management infrastructure is developed along with how to include legacy systems in the infrastructure even if for a limited period of time.

Artifacts. Legacy system upgrade/shutdown schedule.

Responsibilities. Various Departments and Agencies coordinated by ISA IPC.

Status. Not started.

Considerations. The full range of options should be considered on a case-by-case basis for legacy systems including modernization, wrappers and front-ends, and early retirement of systems.

2.4 *Recommendation:* Prepare for the Evolution and Acquisition of ICAM on the Secret Fabric as New Technology Emerges and New Mission and Business Needs Arise

The rapid evolution of technology, mission requirements, threats, and organizational changes can overtake modernization efforts and limit the benefits of improved capabilities sooner than expected. Effort should be expended toavoid revisiting these activities as technologies change over time. A process should be established to incorporate evolving frameworks and technology into the the Secret Fabric architecture to take advantage of Commercial Off-The-Shelf (COTS) advances and to avoid early obsolescence of these capabilities.

2.4.1 *Objective:* Assign an existing governance body to survey technology and trends and evaluating against short-term and long-term architectural requirements

An organization should be assigned to focus on looking at developing technology trends in this space so that the government can incorporate new capabilities provided by new technology in a timely and effective manner.

2.4.1.1 **Activity**: Assign responsibilities dedicated to perform research on emerging technologies and updated policy

As ICAM capabilities evolve over time, it will be important to incorporate new technologies into existing architectures and requirements. Research and development organizations should be identified to help evolve existing ICAM architectures to meet the demands of the future and leverage the latest advances in ICAM technology.

Artifacts. Technology evaluations including readiness assessments.

Responsibilities. The ICAMSC will have the responsibility for ensuring that this activity is completed.

Status. The ICAMSC established the FICAM Roadmap Alignment Working Group (FRAWG) to meet this need. As the FICAM on the Secret Fabric architecture and requirements are established, the FRAWG will need to incorporate them into their technology alignment processes.

Considerations. In order to ensure that COTS vendors can provide new capabilities, consider incorporating a process where new requirements are fed back into the vendor community to enhance COTS capabilities.

2.4.2 *Objective:* Have an acquisition process that incorporates ICAM on the Secret Fabric and interoperability requirements into acquisition approvals

It is important that the acquisition community is provided with capability requirements to be included in new acquisitions. Driving enforcement mechanisms into development and acquisition processes ensures that new ICAM capabilities across the enterprise will be interoperable.

2.4.2.1 **Activity**: Establish acquisition criteria for new ICAM systems that ensure new systems meet ICAM on the Secret Fabric and interoperability requirements

ICAM on the Secret Fabric requirements should be incorporated into the requirements and SOWs of new acquisitions far enough ahead of time to ensure that new capabilities brought on-line will be compatible.

Artifacts. Standardized acquisition verbiage for inclusion in Statements of Work (SOWs).

Responsibilities. ICAMSC and various Departments and Agencies in coordination with ISA IPC.

Status. PM-ISE is working with the General Services Administration (GSA) Office of Government-wide Policy (GSA OGP) on a standards based acquisition initiative.

Considerations. None.

2.4.2.2 **Activity**: Engage acquisition process mechanisms to align and enforce ICAM on the Secret Fabric and interoperability requirements

As new acquisitions are reviewed, they should be evaluated for their ability to meet FICAM on the Secret Fabric requirements. Existing acquisition review mechanisms must be updated to incorporate these requirements.

Artifacts. Updates to Federal and Department and Agency acquisition systems

Responsibilities. ICAMSC and various Departments and Agencies in coordination with ISA IPC.

Status. Not started.

Considerations. There may be some significant complexity associated with this activity given the diversity of acquisition process in different components of the Federal Government. Having sample acquisition documents vetted by Departments and Agencies may help smooth adoption of the criteria.

2.4.3 *Objective:* Have a management plan for updating ICAM on the Secret Fabric architecture and project plans

As new requirements for to the target-state architecture are generated, there should be a method for vetting and approving changes to the target-state architecture and requirements.

2.4.3.1 **Activity**: Develop a management plan for approving and processing changes to approved ICAM on the Secret Fabric architecture and project plans

This plan will allow a governing body to properly evaluate and publish changes to the target-state architecture and requirements for ICAM capabilities on the Secret Fabric.

Artifacts. Updated architecture and capability revisions to the FICAM requirements.

Responsibilities. The ICAMSC FRAWG is responsible for performing this function.

Status. The FRAWG has not yet established a method for incorporating new changes into the ICAM architecture for the Secret Fabric.

Considerations. None.

3 SUMMARY

With the challenges facing federal agencies today, interoperability on the Secret Fabric is a necessity. This interoperability will enhance each Department and Agency's efficiencies by supporting information sharing across networks. Identity and access management are a vital part of this initiative and implementing ICAM capabilities in a consistent way across the government is critical not only to support information sharing but also to effectively protect each Department and Agency's data.

This document provides an initial set of recommendations for addressing gaps in the current state of ICAM capabilities on the Secret Fabric and serves as the foundation for the *FICAM Implementation Plan for the Secret Fabric.* Going forward, Departments and Agencies will need to work closely with capability stewards and ICAM governing bodies to ensure that their FICAM implementation plans and the transition of their ICAM capabilities is well coordinated and comprehensive. While the majority of the focus is on compliance with existing FICAM requirements, energy should be reserved for looking ahead to new capabilities and emerging technologies that may ease the burdens of interoperability, information sharing, and security of our nation's secrets.

Department and Agency CIOs responsible for the Secret Fabric are now called upon to begin planning for their part in achieving the vision of FICAM on the Secret Fabric. In order to realize the benefits of secure sharing of critical information, organizations must now plan for funding and acquisition activities to support deployment of interoperable ICAM capabilities on the Secret Fabric.

This page intentionally left blank

APPENDIX A **ACRONYMS**

AASC	Attribute and Authorization Services Committee
ABAC	Attribute Based Access Control
ACAG	Access Control Attribute Governance
ASNI	Assured Secret Network Interoperability
CERMB	CNSS Enterprise Risk Management Board
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off-The-Shelf
CSP	Common Service Provider
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOE-NNSA	Department of Energy-National Nuclear Security Administration
DOJ	Department of Justice
DOS	Department of State
EO	Executive Order
ESN	Enterprise Secure Network
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Network
FICAM	Federal Identity, Credential, and Access Management Roadmap and Implementation Plan
FY	Fiscal Year
FRAWG	FICAM Roadmap Alignment Working Group
FOC	Final Operating Capability
GSA	General Services Administration
GSA OGP	GSA Office of Government-wide Policy
HSDN	Homeland Secure Data Network
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICAMSC	ICAM Subcommittee

IdAM	Identity and Access Management
IFC	Identity Federations Coordination
IOC	Initial Operating Capability
IPC	Interagency Policy Committee
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Information Sharing and Access
ISE	Information Sharing Environment
ISIMC	Information Security and Identity. Management Committee
JCON-S	Justice Consolidated Office Network – Secret
MGB	Member Governing Body
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSISS	National Strategy for Information Sharing and Safeguarding
NSS	National Security Systems
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PKE	Public Key-Enabled
PKI	Public Key Infrastructure
PM-ISE	Program Manager for the Information Sharing Environment
SIPRNet	Secure Internet Protocol Router Network
SISSSC	Senior Information Sharing and Safeguarding Steering Committee
SOW	Statement of Work
U.S.	United States
WG	Working Group

APPENDIX B SENIOR INFORMATION SHARING AND SAFEGUARDING STEERING COMMITTEE (SISSSC) IOC/FOC DEFINITIONS

The SISSSC through the Office of Management and Budget (OMB) has a working group developing these definitions and they are still evolving. The definitions here are current as of 30 November 2012.

Initiative	Initial Operating Capability (IOC) Definition	Final Operating Capability (FOC) Definition
Removable Media	IOC is reached when write privileges are disabled and/or controlled using a hardware or software solution.	FOC includes IOC, and is achieved when a monitoring and alerting function is implemented for successful / unsuccessful "write" attempts to removable media devices.
Reduce Anonymity	IOC is reached when the PKI is established such that: • Certificates are issued (or a comparable solution) for identification for a minimum of 10 percent of users on classified networks (Secret and Top Secret): and • PKI tokens are used for authentication to high-sensitivity applications (software tokens are sufficient pursuant to Intelligence Community policy and with coordination with the Steering Committee).	FOC includes IOC, and is achieved when: • 90 percent of users have PKI certificates for identification (or a comparable solution)on classified networks (Secret and Top Secret); and • Hardware tokens are used for authentication to enable access to high and medium-sensitivity applications (software tokens are sufficient pursuant to Intelligence Community policy and with coordination with the Steering Committee).
Insider Threat Program[2]	IOC is reached when an agency has policies, procedures, and an organizational structure that identifies an accountable official(s) for the insider threat program, provides regular insider threat awareness training to agency personnel, and includes an integrated approach to gathering (electronically and/or manually) relevant sources of	FOC includes IOC, and is achieved when an agency has implemented the capabilities for: • Monitoring user network activities on all agency networks; • Inclusion of counterintelligence triggers for user-monitoring tailored to the agency

[2] National policy and standards for insider threat detection and prevention programs have not been written. Any IOC and FOC provided at this time for insider threat programs within agencies will be subject to modification when policy and standards are issued.

	insider threat information for analysis and response.	environment; • Establishing an integrated capability to monitor, audit, gather, and analyze information relevant to insider threat analysis from across the agency; and • There is a capability for integrated insider thereat analysis of current data on user actions collected from automated and/or manual information sources – such as audit data, foreign travel and contact reporting, financial disclosure, facility, access, phone records, and external databases.
Access Control	IOC is reached when an interoperable infrastructure for integrated access-control capability (PKI plus “attribute-based” authorization or a comparable solution) is operational (Secret and Top Secret) in accordance with the Federal Identity, Credential, and Access Management (FICAM) framework or equivalent guidance appropriate for the subject network fabric. • Establishes capability for user attribute provisioning to support attribute-based authorization on classified networks. • Requires this capability to be integrated with the PKI authentication capability. Scope: • Minimum of 10 percent of users on classified networks are provisioned with attributes for authorization-related access-control decisions. • Minimum of 25 percent of classified data	FOC includes IOC, and is achieved when an agency has implemented the capabilities for: • Federation (exchange) of standardized user authorization attributes on classified networks across organizations; • Consistent application of fabric-wide access control policy, with timely promulgation of policy changes; and • Tagging of information resources with access-relevant attributes on ingest, creation, or modification; as applicable. Scope: • All users of classified networks. • All high and medium-sensitivity classified network applications.

	repositories designated as highest sensitivity (as defined in NIST SP 800-53, CNSSI 1253, ICD 503 or equivalent guidance appropriate for the subject network fabric) are integrated to use the interoperable access-control infrastructure facilities (PKI integrated with attribute-based access control).	
Enterprise Audit	IOC is reached when an agency has the ability to: • Monitor user-attributable activities (defined as Auditable Events in ICS 500-27) on at least one community-shared information resource on at least one of the agency's classified networks; • Analyze identified anomalies (which includes correlating such anomalies with other data sources); • Report and respond to potential security incidents through collaboration with the appropriate CI, security, law enforcement, or Information Security (INFOSEC) offices; • Provide automated notifications of security incidents from a community-shared information resource on at least one of the agency's classified networks to the appropriate offices; • Deliver an automated flow of audit data from a community-shared information resource on at least one of the agency's classified networks into an agency-specific audit capability; and • Provide audit data to other affected organizations.	FOC includes IOC applied to all classified networks, and is achieved when an agency has implemented the ability to: • Share user-attributable audit information in a common format collected from high and medium-sensitivity information resources (both internal and community-shared) for users; • Analyze identified anomalies; and • Enable a timely response to incidents.

This page intentionally left blank

APPENDIX C REFERENCES

1. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, version 2.0, 02 December 2011 (http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

2. CNSS Policy 25: National Policy For Public Key Infrastructure In National Security Systems; March 2009.

3. EO 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; 07 October 2011.

4. CNSS IdAM Working Group Whitepaper, Gap Analysis Between the FICAM and United States (U.S.) Secret Networks, October 2012.

5. National Strategy for Information Sharing and Safeguarding, December 2012 (http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf).