

# Committee on National Security Systems



## **FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) PLANNING GUIDANCE FOR THE SECRET FABRIC 21 November 2013**

This document has been sanctioned to incorporate the CNSS registered logo based on content approval by the CNSS Subcommittee Tri-Chairs as accepted by the CNSS Subcommittee – Date 01/14/2014.

Jan. 14, 2014



**ENDORSEMENT MEMORANDUM  
FICAM PLANNING GUIDANCE FOR THE SECRET FABRIC**

1. (U) The *Federal Identity, Credential, and Access Management (FICAM) Planning Guidance for the Secret Fabric* defines a set of activities to be implemented by departments and agencies that operate on the Secret Fabric to promote secure information sharing and safeguarding. These activities are divided into four sequential stages. Although individual departments and agencies may complete different activities at different times, the goal of interoperable information sharing requires that all departments and agencies complete all of the activities in each stage prior to the end date for that stage.
2. (U) Priority objective four in the *National Strategy for Information Sharing and Safeguarding*<sup>1</sup> is to “Extend and implement the FICAM Roadmap across all security domains.” The planning guidance provides a framework and timelines for achieving this priority objective on the Secret Fabric.
3. (U) The members of the Committee on National Security Systems (CNSS) Subcommittee have reviewed the *Federal Identity, Credential, and Access Management (FICAM) Planning Guidance for the Secret Fabric*. Based on their review, the Tri-Chairs of the CNSS Subcommittee endorse the planning guidance.

/s/

  
Richard Tannich  
CNSS Tri-Chair

  
Dominic Cussatt  
CNSS Tri-Chair

  
Jeffrey Wilk  
CNSS Tri-Chair

---

<sup>1</sup> *National Policy for Information Sharing and Safeguarding*, December 2012,  
[http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy\\_1.pdf](http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf)

## ABSTRACT

Priority objective four in the National Strategy for Information Sharing and Safeguarding (NSISS) is to “Extend and implement the FICAM Roadmap across all security domains.” This planning guidance document provides the framework and timelines for achieving this priority objective on the Secret Fabric.

The guidance also supports the priorities identified by the Senior Information Sharing and Safeguarding Steering Committee (SISS SC) established by Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.” The guidance identifies specific activities to meet two of the five Initial Operating Capability (IOC)/Full Operating Capability (FOC) near-term priorities: reduce anonymity and access control. It also identifies activities that support a third priority, enterprise audit.

## ACKNOWLEDGEMENTS

This planning guidance was developed as a result of the Program Manager for the Information Sharing Environment (PM-ISE) taking the initiative to provide funding for this effort, and the PM-ISE and Department of Homeland Security (DHS) for providing the leadership to ensure this document met the goals of promoting improved information sharing for the Secret Fabric.

The PM-ISE and DHS would like to acknowledge the contributions of Booz Allen Hamilton and PKH Enterprises for their work in drafting the guidance, and the contributions of reviewers from the joint Committee on National Security Systems (CNSS) and Identity, Credential and Access Management Steering Committee (ICAMSC) Identity Management Working Group, including representatives from DHS, the Department of Defense (DoD), the Department of Energy, and the Department of State.

---

**FEDERAL IDENTITY, CREDENTIAL, AND ACCESS  
MANAGEMENT (FICAM)  
PLANNING GUIDANCE FOR THE SECRET FABRIC**

**21 NOVEMBER 2013**

---

## EXECUTIVE SUMMARY

The National Strategy for Information Sharing and Safeguarding (NSISS) outlines a vision for “a future in which information supports national security decision-making by providing the right information, at any time, to any authorized user, restricted only by law or policy, not technology; and where safeguarding measures, to include a comprehensive regimen of accountability, and prevent the misuse of information.” Effective Identity, Credential, and Access Management (ICAM) supports this vision by providing the underlying capabilities to enable an authorized user to securely access the right information at the right time. As a result, the “National Strategy for Information Sharing and Safeguarding” (NSISS) identified the implementation of the Federal Identity, Credential, and Access Management (FICAM) Roadmap to all security domains as one of its top five priorities. This planning guidance document provides the framework and timelines for achieving this priority objective on the Secret Fabric.

Implementation of interoperable ICAM capabilities on the Secret Fabric demands a clear governance structure that supports collaboration within and among departments and agencies that participate in the Secret Fabric. Governance allows for the stand-up and long term maintenance and modernization of ICAM technologies and processes. The following four components have been identified to implement effective governance across the activities in this guidance:

- **Resource Alignment and Implementation Management** to define a coordinated approach for the allocation of federal resources to ICAM efforts and aligning current and out-year (strategic) ICAM budget requests;
- **Development of Policy and Standards** that are shared across all departments and agencies using the Secret Fabric are required to ensure that technology and process solutions are interoperable across agencies;
- **Interagency Coordination, De-confliction, Synchronization, and Interoperability** of policies and standards among the various working groups developing solutions to ICAM on the Secret Fabric; and
- **Department and Agency Governance** at individual agencies that operate large Secret networks or that have a significant number of users on Secret networks to execute and coordinate agency-specific planning guidance for ICAM capabilities on individual portions of the Secret Fabric.

This planning guidance centers around an overall approach of implementing an Attribute-Based Access Control (ABAC) model on the Secret Fabric. This model was selected for its robust approach to identifying, verifying, and controlling access based upon relevant attributes applied to subjects, resources, and environmental factors. Implementing FICAM on the Secret Fabric will require a combination of deploying new capabilities specific to elements of the ABAC model; modifying and upgrading existing Secret Fabric infrastructure such as network architecture and interconnection mechanisms; instituting governance mechanisms; and operating and maintaining required capabilities.

This document identifies governance- and technology-related activities necessary to implement the ABAC model and groups them into four stages:

Stage	Focus	Target Date
<b>Stage 1</b>	Develop and implement a common authentication capability leveraging the NSS PKI. Lay the groundwork in identifying architecture standards, technologies, processes, and interfaces that will be used in future stages.	<b>Q3 FY14 (JUN 2014)</b>
<b>Stage 2</b>	Complete the rollout of a common authentication capability. Identify subject and resource attributes that are needed to implement digital policies. Finalize and test interfaces for sharing attributes and making access control decisions.	<b>Q3 FY15 (JUN 2015)</b>
<b>Stage 3</b>	Begin implementation of ABAC to include establishing and performing operational testing for the full ABAC capability set.	<b>Q4 FY16 (SEP 2016)</b>
<b>Stage 4</b>	Achieve ABAC across the Secret Fabric, supporting secure information sharing, attribution, and data protection.	<b>Q4 FY18 (SEP 2018)</b>

Although individual departments and agencies may complete different activities at different times, the goal of interoperable information sharing requires that all departments and agencies complete all of the activities in each stage by the target date for the stage. In support of implementing the stages, this document provides an overview of infrastructure and agency specific costs elements that are needed, along with a tool that departments and agencies can use to assist them with developing their cost estimates.

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	BACKGROUND.....	1
1.2	SCOPE.....	3
<b>2</b>	<b>STRATEGIC VISION.....</b>	<b>4</b>
2.1	APPROACH.....	4
2.2	IMPLEMENTATION STAGES.....	6
<b>3</b>	<b>GOVERNANCE.....</b>	<b>8</b>
3.1	KEY ELEMENTS OF ICAM GOVERNANCE.....	8
3.2	GOVERNANCE MODEL AND KEY ACTIVITIES.....	9
3.2.1	<i>Resource Alignment and Implementation Management.....</i>	<i>10</i>
3.2.2	<i>Policy and Standards Development.....</i>	<i>10</i>
3.2.3	<i>Interagency Coordination, De-confliction, Synchronization, and Interoperability.....</i>	<i>11</i>
3.2.4	<i>Department and Agency Governance.....</i>	<i>11</i>
<b>4</b>	<b>KEY IMPLEMENTATION ACTIVITIES.....</b>	<b>13</b>
4.1	STAGE 1.....	14
4.1.1	<i>Stage 1 Secret Fabric FICAM Capabilities.....</i>	<i>14</i>
4.1.2	<i>Stage 1 Goal State.....</i>	<i>15</i>
4.1.3	<i>Stage 1 Goal State Activities.....</i>	<i>15</i>
4.1.4	<i>Activities to Support Future Stages.....</i>	<i>16</i>
4.2	STAGE 2.....	18
4.2.1	<i>Stage 2 Secret Fabric FICAM Capabilities.....</i>	<i>18</i>
4.2.2	<i>Stage 2 Goal State.....</i>	<i>18</i>
4.2.3	<i>Stage 2 Goal State Activities.....</i>	<i>19</i>
4.2.4	<i>Activities to Support Future Stages.....</i>	<i>20</i>
4.3	STAGE 3.....	21
4.3.1	<i>Stage 3 Secret Fabric FICAM Capabilities.....</i>	<i>21</i>
4.3.2	<i>Stage 3 Goal State.....</i>	<i>21</i>
4.3.3	<i>Stage 3 Goal State Activities.....</i>	<i>22</i>
4.3.4	<i>Activities to Support Future Stages.....</i>	<i>23</i>
4.4	STAGE 4.....	23
4.4.1	<i>Stage 4 Secret Fabric FICAM Capabilities.....</i>	<i>23</i>
4.4.2	<i>Stage 4 Goal State.....</i>	<i>24</i>
4.4.3	<i>Stage 4 Goal State Activities.....</i>	<i>24</i>
<b>5</b>	<b>COST ASSESSMENT.....</b>	<b>26</b>
5.1	INFRASTRUCTURE COSTS.....	26
5.2	AGENCY COSTS.....	27
5.3	OTHER COSTS.....	32
<b>APPENDIX A</b>	<b>PROCESS FLOW.....</b>	<b>33</b>
<b>APPENDIX B</b>	<b>ORGANIZATION RELATIONSHIP MAP.....</b>	<b>34</b>
<b>APPENDIX C</b>	<b>ACTIVITIES AND INTERDEPENDENCIES.....</b>	<b>40</b>
C.1	GOVERNANCE ACTIVITIES.....	40
C.2	POLICY ACTIVITIES.....	41
C.3	BUSINESS ACTIVITIES.....	42
C.4	CREDENTIALING ACTIVITIES.....	44
C.5	SUBJECT ATTRIBUTE ACTIVITIES.....	45
C.6	RESOURCE ATTRIBUTE ACTIVITIES.....	47
C.7	ENVIRONMENT ATTRIBUTE ACTIVITIES.....	48

C.8	DIGITAL POLICY ACTIVITIES.....	48
C.9	ENABLING ACTIVITIES .....	49
<b>APPENDIX D PROGRESS AND PERFORMANCE METRICS.....</b>		<b>52</b>
D.1	CAPABILITY: CERTIFICATE-BASED AUTHENTICATION TO APPLICATIONS ACROSS THE SECRET FABRIC, INCLUDING EMPLOYEES, AFFILIATES, AND INTERNATIONAL PARTNERS .....	52
D.2	CAPABILITY: ACCESS TO ENABLED APPLICATIONS LOGGED USING UNIQUE IDENTIFIER CONTAINED IN DIGITAL CERTIFICATES WHICH IS LINKED TO SUBJECT ATTRIBUTES .....	54
D.3	CAPABILITY: CERTIFICATE-BASED NETWORK LOGON .....	54
D.4	CAPABILITY: NETWORK ACCESS LOGGED USING UNIQUE IDENTIFIER CONTAINED IN DIGITAL CERTIFICATES 54	
D.5	CAPABILITY: AUTOMATED ABAC BASED ON SUBJECT ATTRIBUTES, RESOURCE ATTRIBUTES, ENVIRONMENT ATTRIBUTES, AND DIGITAL POLICY RULES .....	54
D.6	CAPABILITY: SHARED DIGITAL POLICY RULES USED TO CONTROL ACCESS TO RESOURCES ACROSS THE SECRET FABRIC .....	56
D.7	CAPABILITY: ABILITY TO EXCHANGE USER ACTIVITY RECORDS ACROSS THE SECRET FABRIC TO SUPPORT AUDIT LOG REVIEW AND INSIDER THREAT PROFILING .....	57
D.8	SUPPORTING OR ENABLING ACTIVITIES – METRICS .....	57
<b>APPENDIX E COST MODEL TOOL FOR IMPLEMENTATION COSTS.....</b>		<b>61</b>
<b>APPENDIX F COST MODEL TOOL FOR AGENCY COSTS.....</b>		<b>62</b>
<b>APPENDIX G REFERENCES.....</b>		<b>63</b>
<b>APPENDIX H ACRONYMS.....</b>		<b>65</b>



## 1 INTRODUCTION

This Federal Identity, Credential, and Access Management (FICAM) Planning Guidance for the Secret Fabric provides a plan for assisting departments and agencies to implement specific governance, technical, and business model activities on the Secret Fabric to protect resources while achieving interoperability and controlled information sharing. The Secret Fabric includes Secret level networks operated by federal departments and agencies that interconnect with other department and agency classified networks as well as closed operational networks that do not interconnect. This document focuses on requirements for interconnected networks to support the critical capability of information sharing. However, activities identified in this planning guide may also be used on closed networks to enhance standardization and overall assurance on the Secret Fabric at the discretion of the agency operating the closed network.

### 1.1 BACKGROUND

Over the past ten years, the Federal Government has made concerted advances in the development and implementation of ICAM. In 2009, the Identity, Credential and Access Management Subcommittee (ICAMSC)<sup>1</sup> published Version 1.0 of the “Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance” (FICAM Roadmap) providing a common segment architecture and implementation guidance for use by federal agencies on unclassified networks. Version 2.0 of the FICAM Roadmap was published in 2011.

Also in 2009, the Committee on National Security Systems (CNSS) published CNSS Policy Number 25, “National Policy for Public Key Infrastructure in National Security Systems” (CNSSP 25), developed by the Public Key Infrastructure (PKI) working group (WG) of the CNSS. CNSSP 25 established the National Security Systems (NSS) PKI as a mechanism for issuing and managing PKI credentials to support interoperable authentication across the Secret Fabric. In 2010, the Identity and Access Management (IdAM) WG, a joint working group of the CNSS and the ICAMSC, developed the “ICAM Lexicon” (ICAM Lexicon), a common set of terms and definitions for ICAM, compiled using the FICAM Roadmap as the baseline.

Also in 2010, efforts to improve interoperability across the Secret Fabric were initiated by the Information Sharing and Access Interagency Policy Committee (ISA IPC)<sup>2</sup> by forming the Assured Secret Network Interoperability (ASNI) WG. A chartering goal of this working group was to develop concurrence on a shared ICAM solution for the federal Secret Fabric.

As a result of security events in 2010 focusing attention on the development and implementation of ICAM solutions for federal and classified systems, Executive Order (EO) 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” was published in 2011. EO 13587 directed structural

---

<sup>1</sup> The ICAMSC is a subcommittee of the Information Security and Identity Management Committee (ISIMC) of the Federal Chief Information Officer (CIO) Council. Additional information about ICAM Governance is provided in Section 3.

<sup>2</sup> Additional information about ICAM Governance is provided in Section 3.

reforms for responsible sharing and safeguarding of classified information including the coordinated interagency development and implementation of policies and minimum standards.

- EO 13587 established the Senior Information Sharing and Safeguarding Steering Committee (SISS SC) to exercise overall responsibility and senior-level accountability for interagency development and implementation of policies and standards.
- In July 2012, the SISS SC established five near-term priorities for departments and agencies and defined Initial Operational Capability (IOC) and Full Operational Capability (FOC) goals for each priority to measure implementation progress.<sup>3</sup>

In 2011, the Program Manager for the Information Sharing Environment (PM-ISE) issued FY13 Implementation Guidance for the ISE (PM-ISE FY2013 Guidance) as a companion document to the Office of Management and Budget (OMB) fiscal year (FY) 13 Programmatic Guidance (OMB Cir A-11 85) outlining the resource priorities and policies for all executive branch departments and agencies. In this memorandum, departments and agencies are directed to do the following by 30 September 2013.

- Program funds to align Secret network identity management solutions to the FICAM Framework to support interoperability among Secret networks
- Implement CNSSP 25, or an interoperable identity management solution, for individual networks and enclaves that access or transit the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNET)

In 2012, the CNSS published CNSS Directive Number 506, “National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks” (CNSSD 506), drafted by the NSS PKI Member Governing Body (MGB) in response to EO 13587. CNSSD 506 requires all departments and agencies that operate systems on or use the Secret Fabric to implement the NSS PKI and leverage NSS PKI certificates for network logon and application authentication. Also in 2012, after conducting a study on federated attribute sharing on the Secret Fabric as assigned by the DNI CIO, the National Geospatial-Intelligence Agency (NGA) published a concept of operations, an architecture document, and an implementation plan.

In response to these and other drivers, the IdAM WG and the ASNI WG collaborated to evaluate the applicability of the FICAM Roadmap to the current and envisioned future state of ICAM capabilities for the Secret Fabric. The resulting “Gap Analysis Between the FICAM and U.S. Secret Networks” (Gap Analysis) was based on the analysis of the ICAM capabilities of six predominant Secret networks in use within the Federal Government and outlines gaps in the current implementation of FICAM on the Secret networks and the FICAM Roadmap.

Subsequently, the IdAM WG developed “Recommendations for Implementing FICAM on U.S. Secret Networks” (Gap Analysis Recommendations). The Gap Analysis Recommendations identified the development of planning guidance that outlines a comprehensive and coordinated approach to implement robust and interoperable ICAM capabilities for the federal Secret Fabric as a critical step. The recommendations laid the foundation for implementing guidance that aligns with the FICAM Roadmap. While departments and agencies have begun efforts to respond

---

<sup>3</sup> A crosswalk of the IOC/FOC goals and this implementation planning guidance is included in Appendix D.

to the drivers outlined above, this document will provide a mechanism for harmonizing department and agency implementation while maximizing interoperability as well as information sharing and safeguarding.

Further, the “National Strategy for Information Sharing and Safeguarding” (NSISS) provides guidance for the effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible information sharing. One of the five goals identified in NSISS is to “Improve information discovery and access through common standards” and is reflected in NSISS Priority Objective 4, “Extend and implement the FICAM Roadmap across all security domains.” This document will act as the baseline for implementing the FICAM Roadmap on the Secret Fabric.<sup>4</sup>

## 1.2 SCOPE

This document applies to all departments and agencies of the United States Government who own, operate, or maintain systems operating on the Secret Fabric. Departments and agencies are expected to implement and enforce the activities identified in this planning guide for all of their affiliates including state government, local government, tribal government, territorial government, international, and private sector partners that they sponsor as users of the Secret Fabric. This document is not intended to alter or supersede the authorities of the Director of National Intelligence (DNI).

Since departments and agencies are at varying degrees of maturity regarding FICAM processes, this document proposes a phased approach for implementation to allow for appropriate resource allocation in a fiscally-constrained environment and acquisition process. The goal of achieving interagency interoperability and information sharing requires that all departments and agencies complete the required activities in each defined stage to achieve the capabilities of that stage.

The remaining sections of this planning guidance define the overarching strategic vision for FICAM on the Secret Fabric, identify gaps in the current governance structure and activities needed to address those gaps, define the four stages of implementation, and provide a business model for the implementation. The appendices provide additional descriptions and resources for the various items discussed and referenced throughout the planning guidance.

---

<sup>4</sup> This document was completed for review in March, 2013. Since then, there have been significant decisions related to governance and responsibilities for implementation of NSISS Priority Objective #4 that are not reflected herein. Since this document will be incorporated into the overall NSISS Priority Objective #4 Implementation Plan, which will take into account more recent developments, no effort is planned to update this document to reflect them.

## 2 STRATEGIC VISION

The strategic vision for FICAM implementation across the Secret Fabric is based on the vision of the NSISS, “a future in which information supports national security decision-making by providing the right information, at any time, to any authorized user, restricted only by law or policy, not technology; and where safeguarding measures, to include a comprehensive regimen of accountability, and prevent the misuse of information.” This planning guidance provides governance, technology, and process activities to achieve this vision, extending and implementing the FICAM Roadmap across all security domains as identified as one of the top five priority objectives in the NSISS. This future vision requires all agencies that manage Secret Fabric networks, maintain applications on the Secret Fabric, or have users who require access to information resources on the Secret Fabric to work together to establish common priorities, collaborate on common processes and standards, and implement capabilities along a single timeline. Continuing to minimize duplication of effort between agencies and ensuring that operational decisions made by each agency reinforce interoperability across the Secret Fabric.

### 2.1 APPROACH

This document is not intended to specify the technologies and standards needed to implement the vision but rather to provide an overall approach of an attribute based access control (ABAC) model on the Secret Fabric. ABAC is a method of Dynamic Access Control that can facilitate interoperable access control and information sharing across agency resources. At a high level, this approach incorporates the following.

- Verifying the identities of individuals who are authorized to access the Secret Fabric
- Providing person and non-person entities (subjects) with strong credentials that assert verified identities
- Authenticating subjects to network and information resources using these credentials
- Determining requirements that govern access to resources on the Secret Fabric and developing digital policy rules that describe these requirements
- Verifying values of attributes applied to subjects, resources, and environmental factors and strongly linking these values to the appropriate entity
- Using digital policy rules to compare attribute values with access rules to determine whether a subject is authorized to access a resource

Figure 2-1 shows the high level elements operated by individual agencies and operated as a shared service to enable a functioning ABAC model. In this model, each agency operates one or more internal authoritative attribute stores, a digital policy store, and a PKI directory. These internal stores are accessed by the agency’s attribute exchange service, which provides requested attribute values both within the agency and to other agencies. Each agency also operates one or more authorization services, which leverage digital policy rules and attribute values to support access control decisions. In addition, some agencies operate their own Certification Authority (CA) under the NSS PKI. Interagency information sharing is supported by shared services, including a digital policy store for those policies which apply across the full Secret Fabric; an attribute map indicating where agency authorization services can go to obtain attributes for users

external to that agency; the Common Service Provider (CSP) CA, which supports all agencies that are not operating their own NSS PKI CAs; and a PKI validation service that provides information about the validity status of all NSS PKI certificates.

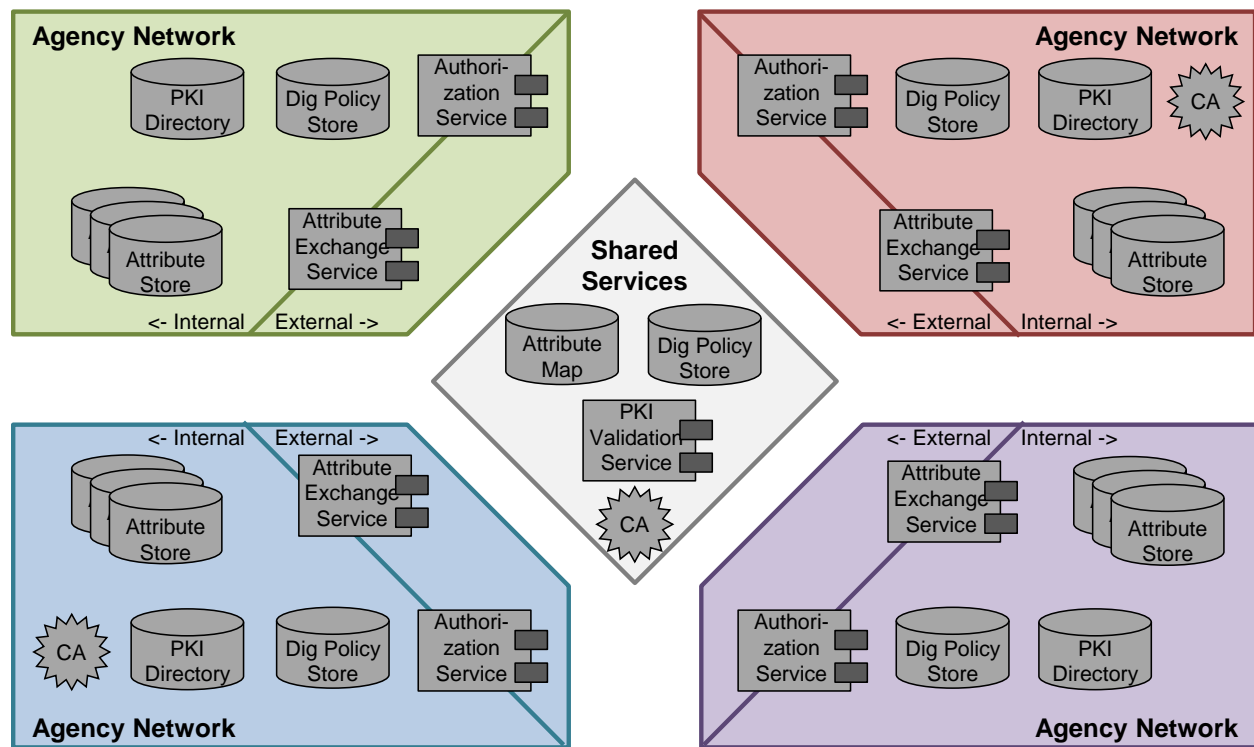


Figure 2-1: Elements of an ABAC Model for Secure Information Sharing

Throughout this document, attributes are divided into three types – subject attributes, environment attributes, and resource attributes. In all cases, the language of existing laws, policies, regulations, and business rules translated into digital policies should establish what attributes are needed to support the ABAC model. The following table provides a high level description of how these terms are used in the document.

Attribute Type	Attribute Description	Attribute Examples
<b>Subject Attribute</b>	Subject attributes are information about the entity requesting access. Entities may be individuals or may be a system or web service that is requesting access on behalf of an individual or as part of performing a process within that service. Subject attributes are linked to the identifier of the subject and are generally maintained in an attribute store. Changes to the values of subject attributes require the implementation of manual or automated processes.	<ul style="list-style-type: none"> <li>• Clearance level</li> <li>• Agency affiliation</li> <li>• Affiliation type (e.g., employee, contractor, state government employee)</li> <li>• Position</li> </ul>
<b>Resource Attribute</b>	Resource attributes are information about the resource being requested. Resources include data, applications, and services. Resource attributes are used to determine which digital policies apply when making an access control decision. Resources can be assigned attributes at multiple levels. Initially, resource attributes may be defined for all resources that are accessible from a single application. Over time, however, resources should be bound to	<ul style="list-style-type: none"> <li>• Resource owner</li> <li>• Resource type</li> <li>• Security categorization of information within the resource</li> <li>• Facts about the resource that relate to the dissemination of the data</li> </ul>

Attribute Type	Attribute Description	Attribute Examples
	attributes at a much more fine-grained level, allowing for enhanced support for information sharing and safeguarding.	
<b>Environment Attribute</b>	Environment attributes are attributes, not specifically about the subject or the resource, but about the current environment at the time of the transaction itself. Environment attributes are key to fine-grained access control because many of the policies that are enforced on information are conditional on some outside environmental factor rather than just the attributes of the subject requesting access.	<ul style="list-style-type: none"> <li>• Type of connection</li> <li>• Time of day</li> <li>• Physical location of subject</li> <li>• Current threat level</li> <li>• Emergency situation</li> </ul>

This document only addresses the use of subject, resource, and environment attributes for the purpose of authentication, authorization, and auditing. Attributes used for authentication are the attributes needed to authenticate to the network such as the credential, the attributes on the credential, and any other information used for authentication. Attributes used for authorization are the attributes that are used in the access rules implemented by the resource providers. Subject, environment, and resource attributes used for authentication and authorization must come from authoritative sources and not be self-asserted and be used for auditing as they provide information that is needed to record the identity and behavior of a user in audit logs. Attributes that are used to control information flow by the user, sometimes called subscription attributes, are not addressed in this document. A detailed process flow for an access control transaction using ABAC has been provided in Appendix A.

## 2.2 IMPLEMENTATION STAGES

Developing and populating these entities will require significant focus and effort from all agencies that participate in the Secret Fabric, both individually to address requirements for the agency's own users and resources and collectively to ensure interoperability across the Secret Fabric. To assist agencies in developing and coordinating their agency implementation plans, this

overall planning guidance provides a list of activities divided into four stages as shown in

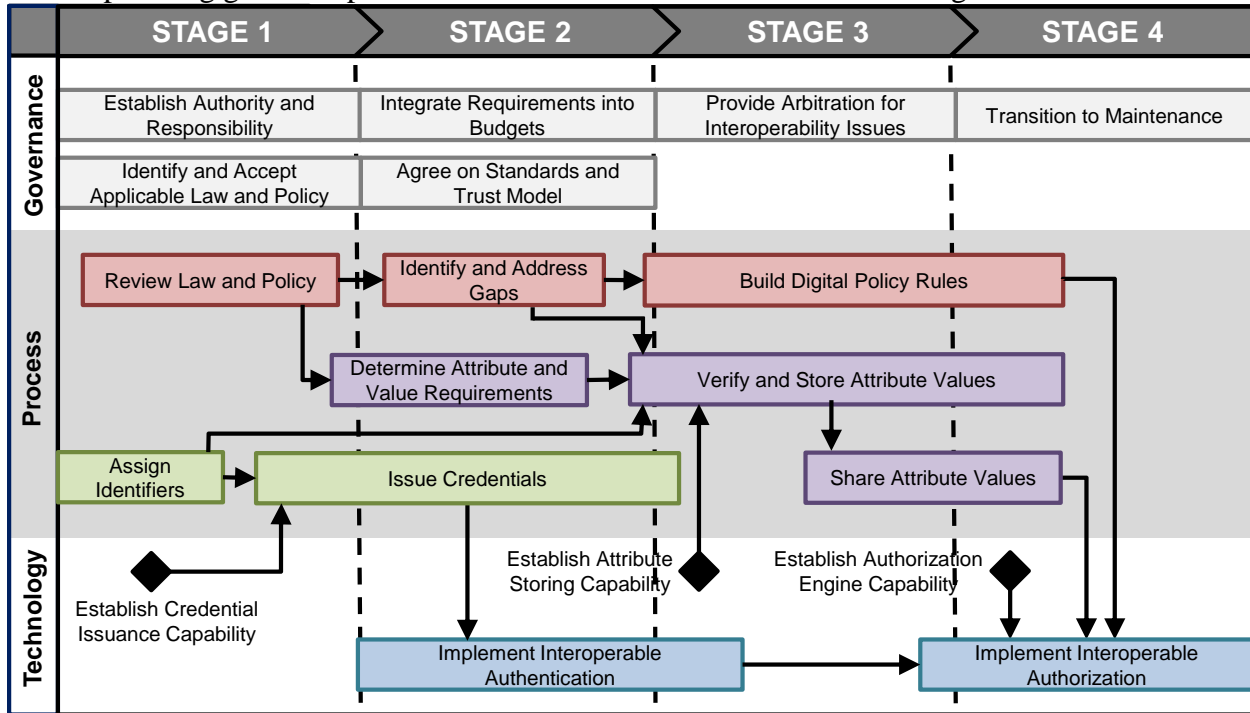


Figure 2-2. Significant effort has already been performed on unclassified networks and by the IC to analyze, prototype, or implement interoperable ICAM capabilities on their respective fabrics. Where possible, these efforts should be leveraged in developing and implementing the overarching FICAM capability for the Secret Fabric.

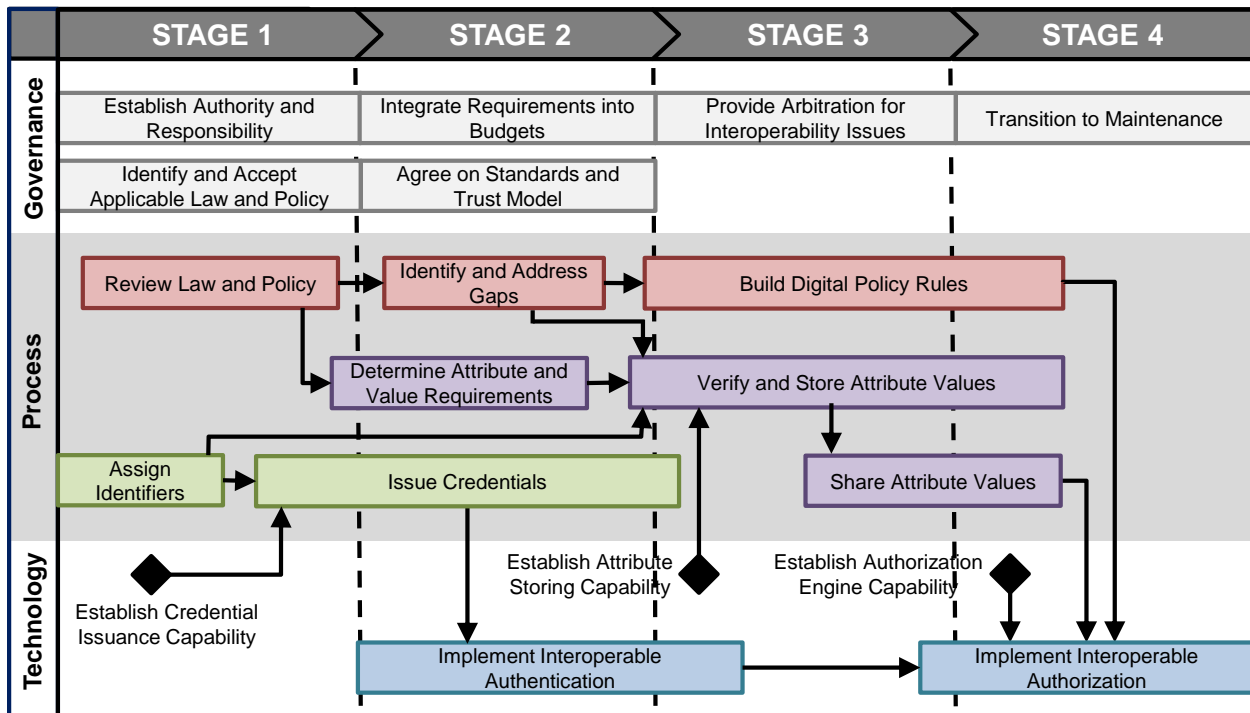


Figure 2-2: High Level Activities and Dependencies for Implementing FICAM on the Secret Fabric

### 3 GOVERNANCE

Governance across the Secret Fabric is critical for defining technical and management standards for credentials, attributes, and digital policies and provides a sustained approach to decision making and resource alignment. Implementation requires a clear governance structure that supports collaboration within and among departments and agencies that participate in the Secret Fabric and integrates stakeholder input for policy and standards development, strategic alignment, decision making, and resource prioritization for the initial stand-up of the ICAM solution over the next few years and its longer-term maintenance and modernization.

#### 3.1 KEY ELEMENTS OF ICAM GOVERNANCE

The following figure introduces the three key elements that comprise a successful ICAM governance program for extending FICAM across the Secret Fabric.

Element	Description
<b>Resource Alignment and Implementation Management</b>	<ul style="list-style-type: none"> <li>• Departments and agencies should identify and reuse best solutions currently available and develop standards-based technologies</li> <li>• Departments and agencies must strategically align acquisition requirements, invest in using shared services and bulk purchase solutions, and employ service provider methods.</li> <li>• Leveraging the forum and authority of the governance bodies, departments and agencies can discuss the allocation of federal resources to ICAM efforts based on prioritized needs or to address observed gaps.</li> </ul>
<b>Policy and Standards Development</b>	<ul style="list-style-type: none"> <li>• Departments and agencies will identify any gaps associated with extending the FICAM Roadmap across the Secret Fabric (e.g., addressing unique concepts like controls on compartmented data and services, cross domain transfer and discovery, and hardware token use that are specific to classified networks)</li> <li>• Departments and agencies will develop common policies and standards to address those gaps and extend and implement FICAM across the Secret Fabric.</li> <li>• Governance will enable department and agencies to make decisions within a formalized structure, providing a solid foundation for developing and approving ICAM policy, guidance, and standards.</li> </ul>
<b>Interagency Coordination, De-confliction, Synchronization, and Interoperability</b>	<ul style="list-style-type: none"> <li>• Secret Fabric owners, operators, and users need a forum to discuss ICAM policies and standards, to align budget requests, and to discuss and de-conflict interagency issues to support interoperability, shared services and efficiency, and shared risk management.</li> <li>• Participating departments and agencies will need a forum within their agency to discuss agency-specific requirements that will be communicated to the federal-wide body and to interpret federal-wide policy for implementation within their agencies.</li> <li>• Agencies will need to synchronize on-going efforts and harmonize them under this planning guide; a robust governance structure will provide the venues to coordinate and synchronize ICAM-related activities and to discuss how these activities should align to other associated or interdependent efforts.</li> </ul>



### 3.2 GOVERNANCE MODEL AND KEY ACTIVITIES

Discussions on ICAM policies and standards currently occur across four major interagency bodies and numerous working groups and subcommittees with varying authorities and responsibilities. The following table outlines these four bodies and the major subcommittees and working groups that are relevant to this planning guidance.

Governance Body	Description
<b>Senior Information Sharing and Safeguarding Steering Committee (SISS SC)</b>	Co-chaired by OMB and the National Security Staff, exercises overall responsibility and ensures senior-level accountability for interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks. <sup>5</sup> In this role, the SISS SC established five information sharing and safeguarding priorities for departments and agencies and established a set of IOC and FOC initiatives for each priority. <sup>6</sup>
<b>Information Sharing and Access Interagency Policy Committee (ISA IPC)</b>	Co-chaired by the National Security Staff and the PM-ISE, is the day-to-day forum for interagency coordination on and development of policies, processes, standards, and technologies to promote secure and responsible national security information sharing. Among its duties, the ISA IPC oversees the implementation of the NSISS. In response to NSISS Priority Objective 4, the ISA IPC designated the Government Accountability Office (GAO) to coordinate federal-wide implementation of Priority Objective 4 and plans to establish an Identity Federation Coordination Working Group (IFC WG) to collaborate on ICAM-related issues and solutions
<b>Federal Chief Information Officer (CIO) Council</b>	Chaired by OMB, is the principal interagency forum to improve agency practices related to the design, acquisition, development, modernization, sustainment, use, sharing, and performance of Federal Government information technology. <sup>7</sup> In support of ICAM efforts, the Federal CIO Council established the ISIMC, under which falls the ICAMSC. The ICAMSC established the Access Control Attribute Governance (ACAG) WG, the IdAM WG (created jointly with CNSS), and the FICAM Roadmap Alignment Working Group (FRAWG).
<b>Committee on National Security Systems (CNSS)</b>	Provides a forum for the discussion of National Security System policy issues and is responsible for setting national-level information assurance policies, directives, instructions, operational procedures, guidance, and advisories for the security of National Security Systems. <sup>8</sup> In support of ICAM efforts, the CNSS established the Architecture Panel, under which falls the IdAM WG (established jointly with the ICAMSC) and the PKI MGB.

A mapping of the relationships between these organizations and other relevant stakeholders has been provided in Appendix B.

<sup>5</sup> EO 13587.

<sup>6</sup> A detailed crosswalk of the activities in this planning guidance and the SISS SC five priorities can be found in Appendix D.

<sup>7</sup> EO 13011 “Federal Information Technology”; E-Government Act of 2002

<sup>8</sup> National Security Directive (NSD)-42 “National Policy for the Security of National Security Telecommunications and Information Systems”; EO 13284 “Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security”; EO 13231 “Critical Infrastructure Protection in the Information Age”.

This section identifies an ICAM governance model that supports each stage of implementation by leveraging these existing bodies and devising a structure that includes the elements of governance described in Section 3.1, namely resource alignment and implementation management; policy and standards development; and interagency coordination, de-confliction, synchronization, and interoperability.<sup>9</sup>

### 3.2.1 Resource Alignment and Implementation Management

The SISS SC and ISA IPC will work together to prioritize resources for implementation of ICAM on the Secret Fabric, leveraging the programmatic processes of both bodies to communicate these priorities to departments and agencies. They will define a coordinated approach for the allocation of federal resources to ICAM efforts as well as align current and out-year (strategic) ICAM budget requests. To support these resource decisions, the SISS SC will monitor implementation of this planning guidance by annually collecting metrics via the Key Information Sharing and Safeguarding Indicators (KISSI)<sup>10</sup> process that demonstrate progress against the IOC and FOC established for the five information sharing and safeguarding priorities. Similarly, the ISA IPC will monitor implementation of this planning guidance as it relates and supports the implementation of the NSISS. Per its role described in EO 13587, the Office of the PM-ISE and the Classified Information Sharing and Safeguarding Office within the Office of the PM-ISE will coordinate activities between the SSIS SC and the ISA IPC on this planning guidance.

### 3.2.2 Policy and Standards Development

The Federal CIO Council and the CNSS will be responsible for developing and approving the majority of policy and standards to support implementation. The various bodies described above perform a unique function in developing and implementing this ICAM solution. Note that the specific responsibilities (activities) of each body in support of this planning guidance are detailed in Section 4.0.

- The **PKI MGB** is responsible for the governance and operations of the NSS PKI, including governance of the NSS PKI CSP. In this role, it will develop PKI-related policies and standards required for implementation.
- The **IdAM WG** will develop identity and access policies and standards required for implementation, integrating insights from the CNSS and ICAMSC.
- The **CNSS** will task and oversee activities of the IdAM WG to develop identity and access policies and standards required for implementation.

---

<sup>9</sup> Appendix A provides an overview of the various organizations, committees, and working groups that will support the implementation of FICAM on the Secret Fabric.

<sup>10</sup> The KISSI process is currently managed by the Office of the PM-ISE on behalf of the SISS SC but is expected to transition from the Office of the PM-ISE to CNSS in the coming months. When this transition occurs, the CNSS will be responsible for collecting the metrics and the SISS SC will continue to monitor implementation

- The **ACAG WG** will develop attribute policies and standards required for implementation.<sup>11</sup>
- The **FRAWG** will investigate and identify gaps in FICAM, based on the work performed under this plan, and develop solutions for integration back into the FICAM Roadmap.

The policies and standards developed in the five bodies above will be published through their respective parent governance body, either the Federal CIO Council or the CNSS.

### **3.2.3 Interagency Coordination, De-confliction, Synchronization, and Interoperability**

The coordination, de-confliction, and synchronization of policies and standards to create durable, interoperable solutions will be the roles of the SISS SC and ISA IPC. Disputes among agencies on ICAM policies and standards should be resolved at the lowest level possible. In the event that the dispute cannot be resolved, the SISS SC will make a final decision. The dispute could be the result of conflicting policies or standards, could be a lack of interoperability between ICAM solutions, or could be related differences among agencies on how to implement a certain ICAM solution.

While coordination and synchronization of policies and standards can occur naturally among the various working groups and sub-committees, the IFC WG, established under the ISA IPC, will facilitate this coordination among the various ICAM elements. ICAM issues that require cross-committee or cross-working group coordination will be brought to the IFC WG for discussion. The IFC WG will also ensure alignment with related interagency efforts (e.g., Comprehensive National Cybersecurity Initiative (CNCI) as well as with other relevant associated programs, initiatives, and priorities). It will also be a mechanism to garner input and feedback on policies and standards from affiliates.

### **3.2.4 Department and Agency Governance**

Once federal-wide ICAM policy and standards exist for the Secret Fabric, each agency will need a similar internal decision-making structure to analyze and prioritize the policies and standards as well as determine how to implement them to support their specific mission set.

The agency body will include those agency components that have a role in the implementation of this planning guidance. The body should be chaired by the department or agency CIO or their designee to ensure the proper agency leadership and oversight of these activities. The agency body will need to perform the following functions.

- Determine the agency strategy for reaching compliance
- Interpret federal-wide policy for implementation within their agencies and develop policies at the enterprise level to govern ICAM capabilities
- Communicate ICAM budget priorities to their agency's Chief Financial Officer or through the appropriate budgetary channels

---

<sup>11</sup> The ACAG WG's work currently focuses on the unclassified environment so their charter may have to be amended to address the activities recommended in this planning guidance.

- Monitor agency implementation of ICAM capabilities and report to the interagency body on implementation progress
- Discuss agency-specific requirements and communicate those requirements to the interagency body (or bodies).

## 4 KEY IMPLEMENTATION ACTIVITIES

The key implementation activities have been grouped into four stages to provide interim milestones. Although individual departments and agencies may complete different activities at different times, the goal of interoperable information sharing requires that all departments and agencies complete all of the activities in each stage. Agencies are encouraged not to require authentication and authorization as described in this document prior to the stage gate deadlines. However, failure to complete required stage activities by one agency may result in that agency's users not being able to access resources hosted by other agencies that have completed stage gate activities.

Each stage begins with a target date and a description of the focus for that stage and then provides a bulleted list of capabilities that are available and a description of the goal state of ICAM on the Secret Fabric at the end of the stage. Goal states are defined along the following axes.

### Governance

- **Governance Process** is defined as the establishment and maturing of a governance process for FICAM on the Secret Fabric.
- **Policy** is defined as establishing interagency and agency policy that ensures compliance with an integrated enterprise approach to FICAM on the Secret Fabric.
- **Business** is defined as accomplishing the business activities that lead to an efficient and effective management implementation and maintenance of FICAM on the Secret Fabric.

### Technical

- **Credentialing** is defined as the issuance and management of credentials to all person entities and non-person entities (such as web servers or other applications) who have a need and are authorized to access resources on the Secret Fabric. Credentials must contain an identifier that is unique to the entity across the Secret Fabric.
- **Subject Attributes** are attributes that are linked to entities that have a need to access resources on the Secret Fabric. Subject attributes include identity and role attributes. Attributes must be linked to the entity through the use of the entity's unique identifier.
- **Resource Attributes** are attributes that are linked to resources available on the Secret Fabric.
- **Environment Attributes** are attributes that describe environmental factors that are relevant to access rules.
- **Digital Policies** refers to the digital representation of policy rules that govern access to resources. Digital policies must be expressed in terms of required subject attributes and linked to resources through resource attributes and linked to the environment through environment attributes.

Each stage contains a set of activities that must be performed to achieve the goal state for the stage. Activities are associated with one of nine activity types. Eight of these types are directly

related to the stage axes described above. The remaining activity type is enabling. Enabling activities enable networks and systems on the Secret Fabric to leverage credentialing, subject attribute, resource attribute, environment attribute, and digital policy capabilities to implement ICAM. Activity numbers indicate the activity type as follows.

- **GOV** Governance Process
- **POL** Policy
- **BUS** Business
- **CRED** Credentialing
- **SATT** Subject Attribute
- **RATT** Resource Attribute
- **EATT** Environment Attribute
- **DPOL** Digital Policy
- **ENAB** Enabling

Activities are grouped into two sets within each stage. The first set contains activities that are needed to achieve the goal state for that stage. The second set contains activities that must be completed in that stage in order to achieve the goal state for future stages. Where possible, activities are ordered sequentially; later activities may depend on earlier activities. Appendix C provides a listing of all of the activities listed by activity type and identifies specific dependency relationships. Appendix D provides target metrics associated with the capabilities to be implemented across the stages.

## 4.1 STAGE 1

*The target date for achieving Stage 1 is June 30, 2014.*

The primary focus for Stage 1 is developing and implementing a common authentication capability by ensuring that agencies are able to begin issuing NSS PKI credentials to their employees and affiliates, either through operating their own CA or by using the CSP. In addition, Stage 1 activities lay the groundwork to solidify governance for interagency coordination and to identify architecture standards, technologies, processes, and interfaces that will be used in future stages. Agencies are also required to identify applicable laws, policies, and other regulations that govern access to resources as the first step in developing the ABAC model.

### 4.1.1 Stage 1 Secret Fabric FICAM Capabilities

The following FICAM capabilities will be available on the Secret Fabric at the conclusion of Stage 1.

- Certificate-based authentication to high sensitivity<sup>12</sup> applications.

---

<sup>12</sup> As defined by the SISS SC for IOC and FOC - High Impact from FIPS 199 & CNSSI 1253. The potential impact is High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic

- Access to enabled high sensitivity systems logged using unique identifier contained in digital certificates.

#### 4.1.2 Stage 1 Goal State

##### Governance

- **Governance Process:** Designated interagency governance bodies and their responsibilities are defined.
- **Policy:** Interagency policy has been established requiring implementation of FICAM on the Secret Fabric.
- **Business:** Initial acquisition guidance, cost model, and risk sharing approaches defined.

##### Technical

- **Credentialing:** NSS PKI certificates are issued to individuals who require access to shared information.
- **Subject Attributes:** No formal attribute exchange mechanism in place.
- **Resource Attributes:** Although some data owners may have identified resource attributes relevant to their data, no formal attribute association mechanism in place.
- **Environment Attributes:** No environment attributes have been defined.
- **Digital Policies:** Catalog of Authorities defining laws, policies, and other regulations that define requirements for controlling access to resources on the Secret Fabric is assembled.

#### 4.1.3 Stage 1 Goal State Activities

The following activities are required to achieve Stage 1 goals.

Number	Activity	Responsible Party
<b>GOV-01</b>	Establish the IFC WG as the facilitator for coordination among the various identity federations that exist in the Federal Government on all classifications and between federal agencies and their affiliates.	ISA IPC
<b>POL-01</b>	Develop interagency policy guidance to require adherence to FICAM Planning Guidance for the Secret Fabric.	SISS SC, ISA IPC
<b>BUS-01</b>	Identify the cost model for participating agencies and shared service providers for the CSP.	SISS SC, ISA IPC
<b>CRED-01</b>	Establish the NSS PKI CSP capability to issue certificates to	PKI MGB

---

adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals exceeding mission expectations.

Number	Activity	Responsible Party
	entities from agencies that are not operating their own NSS PKI CA.	
<b>CRED-02</b>	Establish agency NSS PKI CAs for those agencies that will not be obtaining certificates from the NSS PKI CSP.	Departments and Agencies
<b>CRED-03</b>	Establish registration infrastructure needed to support issuing certificates to entities within the department or agency.	Departments and Agencies
<b>CRED-04</b>	Issue certificates to a minimum of 10% of employees and affiliates, focusing on those who require access to resources hosted by other departments and agencies.	Departments and Agencies
<b>CRED-05</b>	Install smart card readers and middleware on a minimum of 10% of Secret Fabric workstations, including thin clients, that will be used by employees and affiliates who receive NSS PKI hardware certificates on smart cards.	Departments and Agencies
<b>CRED-06</b>	Issue certificates to web servers or other applications that host high sensitivity resources that are currently shared with other departments and agencies.	Departments and Agencies
<b>ENAB-01</b>	Enable high sensitivity applications that are currently shared with other departments and agencies to ensure the subject has authenticated using a PKI certificate.	Departments and Agencies
<b>ENAB-02</b>	Implement mandatory certificate-based network logon to Secret Fabric networks for at least 10% of users.	Departments and Agencies
<b>ENAB-03</b>	Ensure enabled applications generate logs <sup>13</sup> indicating the identifier used to authenticate the user.	Departments and Agencies
<b>DPOL-01</b>	Develop a Catalog of Authorities defining laws, policies, and other regulations that define requirements for controlling access to resources on the Secret Fabric.	Department and Agency Governance Bodies

#### 4.1.4 Activities to Support Future Stages

The following additional activities are required to be completed during Stage 1 to support future stages.

Number	Activity	Responsible Party
<b>GOV-02</b>	Develop department and agency implementation plans for implementing FICAM on the Secret Fabric based on this planning guidance.	Departments and Agencies
<b>GOV-03</b>	Establish department or agency organizational and policy requirements to implement agency implementation plans for FICAM on the Secret Fabric.	Departments and Agencies
<b>GOV-04</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of PKI policies and standards for the Secret Fabric).	PKI MGB
<b>GOV-05</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of identity and access policies and standards for the Secret Fabric).	ICAMSC

<sup>13</sup> This activity will be aligned to the federal-wide efforts to achieve the IOCs and FOCs established by the SISS SC.



Number	Activity	Responsible Party
<b>GOV-06</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of identity and access policies and standards for the Secret Fabric).	IdAM WG
<b>GOV-07</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of attribute policies and standards for the Secret Fabric).	ACAG WG
<b>POL-02</b>	Publish policy that requires departments and agencies to implement FICAM on the Secret Fabric and sets target dates for achieving implementation.	CNSS, ICAMSC
<b>BUS-02</b>	Designate a governance body responsible for assessing and addressing the overall risk management for FICAM on the Secret Fabric to enable departments and agencies to rely on attribute values asserted by other departments and agencies as part of access decisions.	SISS SC, ISA IPC
<b>BUS-03</b>	Identify a framework for individual agencies to manage the risk of trusting credentials and attribute values issued and managed by a third party and ensure it is consistent with their mission and with the overall Secret Fabric risk management governance and technical implementations.	SISS SC, ISA IPC
<b>BUS-04</b>	Integrate requirements for hardware and software upgrades needed to implement FICAM on the Secret Fabric into overall information technology acquisition planning and investment activities.	Departments and Agencies
<b>BUS-05</b>	Coordinate and distribute budget guidance for implementing FICAM on the Secret Fabric.	SISS SC, OMB
<b>BUS-06</b>	Incorporate budget guidance for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies
<b>ENAB-04</b>	Define a target network architecture that defines the level of required interoperability of Secret Fabric networks for information sharing and safeguarding and identifies the interfaces necessary for departments and agencies to use Secret Fabric shared services (such as PKI or Identity Providers).	ICAMSC Architecture Group
<b>ENAB-05</b>	Identify standards and protocols for performing authentication; obtaining subject, environment, and resource attributes; and applying digital policy rules to make access control decisions. Standards and protocols identified must ensure interoperability across the Secret Fabric and, to the extent possible, also provide interoperability with those standards and protocols used by the IC and unclassified communities.	ICAMSC Architecture Group
<b>SATT-01</b>	Identify standards, interfaces, and models for sharing subject attribute information, including identifier, attribute name, attribute value, and availability.	ACAG WG, ICAMSC
<b>EATT-01</b>	Identify standards, interfaces, and models for sharing environment attribute information, including identifier, attribute name, attribute value, and availability.	ACAG WG, ICAMSC
<b>RATT-01</b>	Identify mechanisms for binding resource attributes to resources.	Departments and Agencies
<b>RATT-02</b>	Identify standards, interfaces, and models for registering, binding,	ACAG WG,

Number	Activity	Responsible Party
	and sharing resource attribute information including availability information.	ICAMSC
<b>ENAB-06</b>	Develop prototype of attribute exchange capability on the Secret Fabric as a reference implementation for attribute sharing.	PM-ISE and Partnering Agency Provider(s)

## 4.2 STAGE 2

*The target date for achieving Stage 2 is June 30, 2015.*

The primary focus for Stage 2 is in completing the rollout of a common authentication capability leveraging the NSS PKI. In addition, Stage 2 activities include identifying subject and resource attributes that are needed to implement digital policies so that these attributes can be collected and shared in future stages, and finalizing and testing interfaces for sharing attributes and making access control decisions.

### 4.2.1 Stage 2 Secret Fabric FICAM Capabilities

The following Secret Fabric ICAM capabilities will be available at the conclusion of Stage 2.

- Certificate-based authentication to high and medium sensitivity<sup>14</sup> applications.
- Access to enabled high and medium sensitivity systems logged using unique identifier contained in digital certificates.
- Certificate-based network logon.
- Network access logged using unique identifier contained in digital certificates.

### 4.2.2 Stage 2 Goal State

#### Governance

- **Governance Process:** Department and agency governance is integrated with interagency governance.
- **Policy:** Governance approval of the policy authorities defined in the Catalog of Authorities.
- **Business:** Cost model for developing and maintaining shared services is defined; funding requirements for implementing FICAM is integrated into budget submissions and information technology budgets.

<sup>14</sup> As defined by the SISS SC for IOC and FOC - Moderate impact from FIPS 199. The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interested of the United States (i.e., 1) causes a signification degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries).

## Technical

- **Credentialing:** NSS PKI certificates are issued to 90% of employees and affiliates who require access to the Secret Fabric. Users have the capability to exchange digitally signed and encrypted email (with the NSS PKI hardware token).
- **Subject Attributes:** Subject attributes needed to implement digital policy rules are defined, but no formal attribute exchange mechanism is yet in place.
- **Resource Attributes:** Resource attributes needed to apply digital policy rules to resources are defined.
- **Environment Attributes:** Environment attributes needed to implement digital policy rules are defined.
- **Digital Policies:** Subject, resource, and environment attributes needed to apply digital policies are defined; registration for context information is initiated; prototype digital policy engine is implemented.

### 4.2.3 Stage 2 Goal State Activities

The following activities are required to achieve Stage 2 goals.

Number	Activity	Responsible Party
<b>GOV-08</b>	Incorporate technology requirements for implementing FICAM capabilities into agency implementation plans. Include an ongoing process for evaluating further appropriate technological enhancements to improve agency alignment with FICAM capabilities.	Department and Agency Governance Bodies
<b>DPOL-02</b>	Identify shared digital policies that apply across the Secret Fabric.	ACAG WG
<b>POL-03</b>	Review the Catalog of Authorities, developed per DPOL-01, including legal review and approval.	ICAMSC, IdAM WG
<b>BUS-07</b>	Identify the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB
<b>BUS-08</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC
<b>BUS-09</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies
<b>CRED-07</b>	Issue certificates to at least 90% of employees and affiliates who have fully-provisioned network accounts on the Secret Fabric.	Departments and Agencies
<b>CRED-08</b>	Install smart card readers and middleware on all Secret Fabric workstations, including thin clients, that will be used by employees and affiliates who receive NSS PKI hardware certificates on smart cards.	Departments and Agencies
<b>CRED-09</b>	Issue certificates to web servers or other applications that host high and medium sensitivity resources that are currently shared with other departments and agencies.	Departments and Agencies
<b>CRED-10</b>	Issue certificates to network domain controllers.	Departments and Agencies

Number	Activity	Responsible Party
<b>ENAB-07</b>	Enable high and medium sensitivity applications that are currently shared with other departments and agencies to ensure the subject has authenticated using a PKI certificate.	Departments and Agencies
<b>ENAB-08</b>	Implement mandatory certificate-based network logon to Secret Fabric networks.	Departments and Agencies
<b>ENAB-09</b>	Ensure network logon generates activity logs <sup>15</sup> that include the identifier of the entity that logged on.	Departments and Agencies

#### 4.2.4 Activities to Support Future Stages

The following additional activities are required to be completed during Stage 2 to support future stages.

Number	Activity	Responsible Party
<b>POL-04</b>	Identify any gaps and overlaps in the Catalog of Authorities, developed per DPOL-01, and develop an action plan to address.	ICAMSC, CNSS
<b>POL-05</b>	Draft new policies or propose changes to existing policies to address identified policy gaps and overlaps.	CNSS, ICAMSC
<b>DPOL-03</b>	Perform a compliance office review of the set of shared digital policies.	OMB
<b>DPOL-04</b>	Identify initial set of digital policies that will be used to govern access to resources intended to be shared across the Secret Fabric.	Department and Agency Governance Bodies
<b>DPOL-05</b>	Develop agency-specific digital policy rules governing access control to department or agency resources.	Departments and Agencies
<b>SATT-02</b>	Determine subject attributes that will be needed to support ABAC decisions based on the Catalog of Authorities.	Department and Agency Governance Bodies
<b>SATT-03</b>	Identify and establish authoritative attribute stores for subject attributes.	Departments and Agencies
<b>EATT-02</b>	Determine environment attributes that will be needed to support ABAC decisions based on the Catalog of Authorities.	Department and Agency Governance Bodies
<b>RATT-03</b>	Determine resource attributes that will be needed to link resources to applicable requirements based on the Catalog of Authorities.	Department and Agency Governance Bodies
<b>ENAB-10</b>	Implement prototype of authorization service that implements digital policy rules based on resource attributes and includes discovery and use of subject and environment attributes.	PM-ISE and Partnering Agency Provider(s)
<b>ENAB-11</b>	Develop attribute exchange services and link them with agency attribute stores.	Departments and Agencies
<b>ENAB-12</b>	Test attribute exchange service interfaces with Stage 1 prototype implementation to measure interoperability.	Departments and Agencies

<sup>15</sup> This activity will be aligned to the federal-wide efforts to achieve the IOCs and FOCs established by the SISS SC.

### 4.3 STAGE 3

*The target date for achieving Stage 3 is September 30, 2016.*

The primary focus for Stage 3 is to begin implementing ABAC. Although Stage 3 implementation will be limited by the ability of agencies to populate attribute information and by the ability to link resources to attributes and appropriate policy rules, agencies should be able to establish and perform operational testing for the full ABAC capability set during this stage.

#### 4.3.1 Stage 3 Secret Fabric FICAM Capabilities

The following Secret Fabric ICAM capabilities will be available at the conclusion of Stage 3.

- Certificate-based authentication to applications.
- Access to all PKI-enabled systems logged using unique identifier contained in digital certificates.
- Certificate-based network logon.
- Network access logged using unique identifier contained in digital certificates.
- Limited ABAC based on digital policy rules and attribute exchange capability for access control for department's or agency's own employees and affiliates.

#### 4.3.2 Stage 3 Goal State

##### Governance

- **Governance Process:** Subject, resource, and environment attribute set is approved by interagency governance body.
- **Policy:** Policy addresses subject attributes, attribute sources, and levels of confidence for attribute values for federal and affiliates.
- **Business:** Cost sharing is initiated on policy based access management.

##### Technical

- **Credentialing:** NSS PKI certificates are issued to all employees and affiliates who require access to the Secret Fabric.
- **Subject Attributes:** Attribute exchange systems and interfaces are operational and tested; however, attribute values for employees and affiliates are not fully populated.
- **Resource Attributes:** Resource attributes are bound to data, resources, and systems.
- **Environment Attributes:** Mechanisms for determining values of environment attributes are defined and implemented.
- **Digital Policies:** Requirements for access to resources are defined in digital policy format.

### 4.3.3 Stage 3 Goal State Activities

The following activities are required to achieve Stage 3 goals.

Number	Activity	Responsible Party
<b>GOV-09</b>	Develop guidelines and requirements for sharing network and application activity logs <sup>16</sup> across the Secret Fabric to applicable agencies to support audit review.	ICAMSC, IFC WG
<b>BUS-10</b>	Review trust model assumptions for management of attribute values for employees and affiliates for all subject attributes to ensure ability of all departments and agencies to accept attribute values from other departments and agencies and update as required.	SISS SC, ISA IPC
<b>CRED-11</b>	Issue certificates to all employees, affiliates, and non-person entities (such as web servers or other applications) that require certificates to support authentication on the Secret Fabric.	Departments and Agencies
<b>SATT-04</b>	Establish attribute mapping capability to allow agencies to identify the location of subject attributes that are not locally managed.	ICAMSC Architecture Group
<b>SATT-05</b>	Determine whether values for attributes identified in Stage 2 currently exist in a format that supports migration to an existing attribute store for agency employees and affiliates.	Departments and Agencies
<b>SATT-06</b>	For attributes that exist in a usable format, identify authoritative source and develop processes and interfaces for making attribute values available to attribute exchange services.	Departments and Agencies
<b>SATT-07</b>	For attributes that do not currently exist in a usable format, identify processes for determining and managing the values of the attribute for employees and affiliates and identify a mechanism for provisioning attribute values that will be available to attribute exchange services.	Departments and Agencies
<b>SATT-08</b>	Populate attribute values for users of high sensitivity applications.	Departments and Agencies
<b>SATT-09</b>	Modify on-boarding and provisioning processes to include provisioning and maintenance of defined subject attributes for employees and affiliates.	Departments and Agencies
<b>SATT-10</b>	Modify out-board and de-provisioning processes to include update and deletion of defined subject attributes for employees and affiliates.	Departments and Agencies
<b>EATT-03</b>	Identify environment attribute sources and establish connections to attribute exchange services.	Departments and Agencies
<b>RATT-04</b>	Implement binding of resource attributes to resources for resources that are intended to be shared.	Departments and Agencies
<b>ENAB-13</b>	Ensure that all applications that manage resources that are intended to be shared with other departments and agencies require certificate-based authentication of all authorized users.	Departments and Agencies
<b>ENAB-14</b>	Ensure that applications log all resource access using identifiers contained in certificates.	Departments and Agencies

<sup>16</sup> This activity will be aligned to the federal-wide efforts to achieve the IOCs and FOCs established by the SISS SC.

Number	Activity	Responsible Party
<b>ENAB-15</b>	Implement agency authorization services that perform access control based on digital policies linked to resources and values of associated subject and environment attributes.	Departments and Agencies
<b>ENAB-16</b>	Enable 25% of high sensitivity applications to use authorization services for access control.	Department and Agency Governance

#### 4.3.4 Activities to Support Future Stages

The following additional activities are required to be completed during Stage 3 to support future stages.

Number	Activity	Responsible Party
<b>BUS-11</b>	Review and update, as required, the on-going cost model for shared services including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB
<b>BUS-12</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC
<b>BUS-13</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies
<b>GOV-10</b>	Review interagency governance structures, including working group charters, and modify them, as required, to support on-going maintenance activities for operating FICAM on the Secret Fabric.	ICAMSC, CNSS
<b>GOV-11</b>	Review department or agency organizational and policy requirements and modify them, as required, to support on-going maintenance activities for operating on the Secret Fabric.	Departments and Agencies

#### 4.4 STAGE 4

***The target date for achieving Stage 4 is September 30, 2018.***

The focus for Stage 4 is to achieve ABAC across the Secret Fabric, supporting secure information sharing, attribution, and data protection.

##### 4.4.1 Stage 4 Secret Fabric FICAM Capabilities

The following Secret Fabric ICAM capabilities will be available at the conclusion of Stage 4.

- Certificate-based authentication to all applications across the Secret Fabric, including employees, affiliates, and international partners.
- Access to all PKI-enabled systems logged using unique identifier contained in digital certificates that is linked to subject attributes.
- Certificate-based network logon.
- Access to networks and applications logged using unique identifier contained in digital certificates along with attribute values used in access decision and the source of those attributes.

- Automated ABAC capability based on subject attributes, resource attributes, environment attributes, and digital policy rules.
- Shared digital policy rules used to control access to resources across the Secret Fabric.

#### 4.4.2 Stage 4 Goal State

##### Governance

- **Governance Process:** The governance body is effective at continued management of FICAM activities across the Secret Fabric and is transparent to users of the Secret Fabric.
- **Policy:** Policies are established and implemented that clearly and concisely address requirements for access to resources on the Secret Fabric.
- **Business:** Processes and technologies are implemented and maintained to support secure information sharing.

##### Technical

- **Credentialing:** NSS PKI certificates are issued to all employees and affiliates who require access to the Secret Fabric. External (e.g., international) partners may authenticate for access to appropriate resources using PKI certificates that have been approved by the NSS PKI Program Management Authority (PMA).
- **Subject Attributes:** Attribute exchange systems and interfaces are operational and tested; attribute values for employees and affiliates are fully populated.
- **Resource Attributes:** Resource attributes, including classification, are bound to resources at the data element level.
- **Environment Attributes:** Environment attributes are standardized and used across the Secret Fabric as needed to determine access to resources.
- **Digital Policies:** Standardized digital policies are used across the Secret Fabric where appropriate to govern access to resources.

#### 4.4.3 Stage 4 Goal State Activities

The following activities are required to achieve Stage 4 goals.

Number	Activity	Responsible Party
<b>GOV-12</b>	Identify and implement processes for maintaining and updating identified subject, resource, and environment attributes.	ACAG WG
<b>GOV-13</b>	Define governance processes to manage digital policies that apply to the full Secret Fabric.	CNSS, ICAMSC
<b>GOV-14</b>	Define governance processes to manage agency specific digital policies.	Department and Agency Governance Bodies
<b>BUS-14</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC



Number	Activity	Responsible Party
<b>BUS-15</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies
<b>BUS-16</b>	Review and update, as required, the on-going cost model for shared services including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB
<b>DPOL-06</b>	Identify full set of common digital policy rules that apply across the Secret Fabric.	ICAMSC, IdAM WG
<b>DPOL-07</b>	Ensure digital policy stores are fully populated with digital policy rules.	Departments and Agencies
<b>CRED-12</b>	Implement trust agreements to facilitate certificate validation processing with international partners to facilitate authentication of non-NSS PKI certificates.	PKI MGB
<b>SATT-11</b>	Complete the population of attribute values for employees and affiliates used in digital policy rules in authoritative data stores.	Departments and Agencies
<b>SATT-12</b>	Ensure that attribute values for employees and affiliates used in digital policy rules are accessible via agency attribute exchange services.	Departments and Agencies
<b>SATT-13</b>	Ensure all attribute values used in digital policy rules are identified in the shared attribute map so other agencies can locate them.	Departments and Agencies
<b>SATT-14</b>	Identify attribute stores maintained by affiliates or alternative sources of affiliate attributes that rise to the authoritative level necessary to satisfy the FICAM trust framework.	Departments and Agencies
<b>SATT-15</b>	Ensure that agency attribute exchange services have access to affiliate attribute stores.	Departments and Agencies
<b>RATT-05</b>	Ensure resource attributes are defined, validated, and bound to associated resources.	Departments and Agencies
<b>ENAB-17</b>	Enable all high and medium sensitivity to use authorization services for access control.	Departments and Agencies
<b>ENAB-18</b>	Ensure applications generate logs <sup>17</sup> indicating the identifier used to authenticate to the system, the values of attributes used in the access control decision, and the source of those attribute values.	Departments and Agencies

<sup>17</sup> This activity will be aligned to the federal-wide efforts to achieve the IOCs and FOCs established by the SISS SC.

## 5 COST ASSESSMENT

Implementing FICAM on the Secret Fabric will require a combination of deploying new capabilities specific to elements of the ABAC model; modifying and upgrading existing Secret Fabric infrastructure such as network architecture and interconnection mechanisms; and instituting governance mechanisms. In addition, departments and agencies will need to provide for operations and maintenance of required capabilities.

Cost savings can be achieved through the use of shared services, where one lead department or agency develops the capability, which is then either implemented by that department or agency for the entire Secret Fabric or which is provided to other departments and agencies as a reference implementation.

This section provides a description of shared infrastructure and agency specific cost elements that will be needed for ABAC implementation and a cost model tool, along with a listing of assumptions for each cost element. The cost element descriptions in this document identify the projected stages, and the cost model tool provides an ability to allocate costs for these elements across the different stages so an agency can estimate its cost for achieving each stage. The cost model tool can be used by departments and agencies as preliminary guidance in planning. Current values are broad estimates, and as efforts pursuant to this planning guidance mature, the cost values for the model can be determined more precisely based on experience. The numbers in the cost model tool should not be considered prescriptive for budgeting purposes.

### 5.1 INFRASTRUCTURE COSTS

Infrastructure costs are cost elements that will be provided by a single agency but leveraged by multiple departments and agencies. The funding model for infrastructure costs will be developed during stage 1 of implementation. This model may be a combination of participating agencies providing funds to agencies operating shared infrastructure services as well as agencies requesting and receiving specific budget allocations for providing shared services. The cost estimation tool provides an estimated total cost for each infrastructure element and allows agencies to identify what, if any, their portion of the cost will be for agency budgeting purposes.

The cost model tool for infrastructure costs is provided in Appendix F.

Number	Cost Element	Cost Element Description	Assumptions
<b>INF-01</b>	<b>Operate the CSP</b>	The CSP is a capability under the NSS PKI Root Certification Authority to provide issuance, maintenance, publication, and revocation status checking for PKI certificates. The Defense Information Systems Agency (DISA) is the provider of the CSP. The CSP is required to be operational at Stage 1.	<ul style="list-style-type: none"> <li>All agencies except for the DoD, Department of State, and Federal Bureau of Investigation (FBI) will use the CSP for their certificates and will provide funding to DISA to support CSP operations.</li> <li>CSP capabilities that are desired by a single agency must be fully funded by that agency and should be added by that agency to their cost assessment.</li> </ul>
<b>INF-02</b>	<b>Provide a test capability for performing</b>	Agencies require the ability to test certificate issuance, certificate revocation, and certificate status	<ul style="list-style-type: none"> <li>The test capability will be provided as part of the overall service by the CSP. Costs are included in the cost for</li> </ul>

Number	Cost Element	Cost Element Description	Assumptions
	<b>certificate-based authentication</b>	checking leveraging a test infrastructure. In addition, agencies require test certificates that can be issued to developers and applications to support enabling these systems to perform PKI-based authentication. The certificate test capability must be operational at Stage 1.	INF-01 with no additional cost for the test capability.
<b>INF-03</b>	<b>Create and operate an attribute map</b>	An attribute map service will be necessary as part of the enterprise infrastructure to enable agency authorization services to determine the location of attribute values. The attribute map must be operational at Stage 3.	<ul style="list-style-type: none"> <li>• Agencies will primarily rely on their agency attribute exchange services to obtain attributes.</li> <li>• The attribute map will be a fairly simple data store that agencies can use when they require access to attribute values they have not yet mapped.</li> </ul>
<b>INF-04</b>	<b>Create and operate a digital policy store</b>	The digital policy store contains digital policies that are common across the Secret Fabric. The digital policy store must be operational at Stage 3.	<ul style="list-style-type: none"> <li>• Digital policy rules specific to a single department or agency are not included in the infrastructure digital policy store.</li> </ul>
<b>INF-05</b>	<b>Provide a test capability for authorization services</b>	Agencies require the ability to test PKI-based authentication combined with attribute discovery and application of digital policy rules through an authorization service. The authorization test capability must be operational at Stage 3.	<ul style="list-style-type: none"> <li>• Estimating costs for the operation of a test authorization service will be provided at a future time once standards and technologies have been determined.</li> </ul>

## 5.2 AGENCY COSTS

Agency cost elements must be implemented by each department or agency to support FICAM on the Secret Fabric. These cost elements are dependent on agency specific information, such as the number of users or the number and complexity of applications that require enabling. The cost model for agency costs does not include costs to maintain FICAM on the Secret Fabric. However, those items that should be considered as Operation and Maintenance (O&M) costs are noted in the assumptions column of the following table.

The cost model tool for agency costs is provided in Appendix G.

#	Cost Element	Cost Element Description	Assumptions	Applicable Stage(s)	Cost Unit
A-01	<b>Establish registration infrastructure (Registration Authority Officers, Trusted Agents)</b>	Establishing an infrastructure with a qualified workforce and workstations with the same platform is necessary to register users into the Secret Fabric. The workforce infrastructure is comprised of Registration Authority (RA) Officers and Trusted Agents (TAs). The number of RA Officers and TAs is directly related to the total number and the geographical distribution of agency users.	<ul style="list-style-type: none"> <li>The cost metric includes the establishment of dedicated RA Officer workstations and tokens as well as training costs for RA Officers.</li> <li>The cost model is based on CSP estimated costs. Agencies not using the CSP may need to modify the model to more accurately reflect their agency costs.</li> <li>Because TAs can use their NSS PKI token credentials, TA workstation costs are not included in this assessment.</li> <li>Any configuration costs to ensure connectivity between RA Officer workstations and the CSP are not included in this assessment.</li> <li>O&amp;M costs not included: workstation refresh; training required as a result of staff turnover.</li> </ul>	Stage 1 (50%) Stage 2 (50%)	Number of RA Officers
A-02	<b>Issue Tokens to Users</b>	This cost element accounts for the cost associated with issuing PKI certificates on hardware tokens to users.	<ul style="list-style-type: none"> <li>The cost model includes the cost of the tokens and the time needed for RA Officers and TAs to issue a certificate. It does not include the user's time.</li> <li>The cost model is based on CSP estimated costs. Agencies not using the CSP may need to modify the model to more accurately reflect their agency costs.</li> <li>O&amp;M costs not included: cost for new tokens as a result of lost tokens, failed tokens, or technology refresh; labor cost for certificate reissuance as a result of expiration, loss, or staff turnover.</li> </ul>	Stage 1 (10%) Stage 2 (90%) Stage 3 (remaining)	Number of users
A-03	<b>Configure user workstations with card reader and middleware</b>	This cost element includes the costs associated with configuring end user workstations connected to the Secret Fabric to support hardware PKI certificates.	<ul style="list-style-type: none"> <li>The cost model includes a fixed cost for developing the workstation configuration.</li> <li>The cost model also incorporates the cost of rolling out the configuration installation to each workstation, the licensing fees for the middleware, and the time required for the install.</li> <li>Middleware cost is an annual cost across</li> </ul>	Stage 1 (10%) Stage 2 (90%) Stage 3 (remaining)	Number of workstations

#	Cost Element	Cost Element Description	Assumptions	Applicable Stage(s)	Cost Unit
			<p>workstations and is not calculated per workstation.</p> <ul style="list-style-type: none"> <li>The cost model does not include the cost of the end user's time during the install.</li> <li>O&amp;M costs not included: workstation refresh.</li> </ul>		
<b>A-04</b>	<b>Enable applications to perform certificate-based authentication</b>	This cost element accounts for the costs to configure applications such as web servers to perform certificate-based authentication.	<ul style="list-style-type: none"> <li>Enabling individual applications is dependent on the architecture and design of the application as well as the capabilities provided by any commercial-off-the-shelf software used within the application.</li> <li>The cost model provides different costs for low, medium, and high complexity applications.</li> <li>Costs related to network configuration changes that may be needed to support interoperable PKI-based authentication are not included in the cost model.</li> <li>O&amp;M costs not included: configuration changes as a result of technology refresh; enabling requirement for new applications.</li> </ul>	<p>Stage 1 (high sensitivity)</p> <p>Stage 2 (medium and high)</p> <p>Stage 3 (remaining)</p>	Number of applications
<b>A-05</b>	<b>Configure networks to perform certificate-based authentication</b>	This cost element accounts for the costs to configure network logon to require hardware token certificate-based authentication.	<ul style="list-style-type: none"> <li>The cost model assumes that network resources and end user workstations are using operating systems that natively support certificate-based authentication. Costs for upgrading the operating system on user workstations are not included in this model.</li> <li>O&amp;M costs not included: configuration changes as a result of technology refresh.</li> </ul>	Stage 2	Number of network domains
<b>A-06</b>	<b>Establish and operate an externally-facing attribute exchange service</b>	This cost element accounts for the costs to develop an externally-facing attribute exchange service that provides attribute values to internal and interagency authorization services.	<ul style="list-style-type: none"> <li>The cost model assumes that agencies do not desire to provide direct access to internal databases on their network but instead provide an externally facing service for attribute values needed to support interoperable access control.</li> <li>Each agency provides subject attributes for their own employees and affiliates and may also provide attribute values for external entities that are managed by that agency.</li> </ul>	Stage 3	Agency

#	Cost Element	Cost Element Description	Assumptions	Applicable Stage(s)	Cost Unit
			<ul style="list-style-type: none"> <li>O&amp;M costs not included: maintenance labor and software licensing fees.</li> </ul>		
A-07	<b>Establish and operate a digital policy store</b>	This cost element accounts for the costs to develop and operate a digital policy store that contains agency specific digital policies for access to that agency's resources.	<ul style="list-style-type: none"> <li>Digital policy rules that are common across the Secret Fabric and are included in the infrastructure digital policy store are not included in agency digital policy stores.</li> <li>O&amp;M costs not included: maintenance labor.</li> </ul>	Stage 3	Agency
A-08	<b>Create and populate digital policy rules</b>	This cost element accounts for the analysis and validation of policies identified based in law, regulation, or government-wide policy. It also includes creating digital policies based on the Catalog of Authorities.	<ul style="list-style-type: none"> <li>This cost element includes the translation of identified policy requirements into digital policy language and entering them into the digital policy store.</li> <li>This cost element does not include the cost of reviewing existing laws and policies to determine what the policy rules are.</li> <li>O&amp;M costs not included: maintenance labor and software licensing fees.</li> </ul>	Stage 3 (high sensitivity) Stage 4 (remaining)	Number of digital policy rules
A-09	<b>Populate subject attribute values and link to attribute exchange service</b>	It is expected that many of the subject attribute values needed to implement digital policies are not currently available for agency users and must be verified and recorded. In addition, interfaces must be developed to ensure attribute values are accessible to the attribute exchange service.	<ul style="list-style-type: none"> <li>As the number of attributes is not yet known, the cost model provides a basic estimate for verifying the value of a single attribute for a single subject.</li> <li>For subject attributes that are already defined and maintained in existing attribute stores, the cost to populate values is limited to the cost to develop an interface between the existing attribute store and the attribute exchange service.</li> <li>O&amp;M costs not included: maintenance labor and software licensing fees; requirements to populate new attributes for existing users or attributes for new users.</li> </ul>	Stage 3 (10%) Stage 4 (remaining)	Number of entities and number of attributes for each entity
A-10	<b>Populate resource attribute values and bind them to resources</b>	Resource attributes are needed to determine which digital policies apply to which resources. Because digital policies are not yet defined, the full scope of resource attribute identification and binding is not yet	<ul style="list-style-type: none"> <li>The cost model assumes a standard methodology for binding resource attributes to resources. Because this methodology is not yet defined, the cost for populating resource attributes may change.</li> <li>O&amp;M costs not included: maintenance labor</li> </ul>	Stage 3 (10%) Stage 4 (remaining)	Number of resources and number of associated resource attributes

#	Cost Element	Cost Element Description	Assumptions	Applicable Stage(s)	Cost Unit
		known. As a result, resource attributes will likely start with coarse-grained attributes applied at the application level and migrate to fine-grained resource attributes bound directly to resources.	and software licensing fees; requirements to populate attributes for new resources.		
A-11	<b>Identify sources for environment attribute values and link to attribute exchange service</b>	Environment attributes provide information about a specific transaction. Defining environment attributes and identifying interfaces for providing the values of environment attributes real-time to an authorization service allows for incorporation of these factors into access decisions.	<ul style="list-style-type: none"> <li>Environment attributes already exist but may not be properly recorded or made available.</li> <li>O&amp;M costs not included: maintenance labor and software licensing fees; requirements to identify and link new environment attributes.</li> <li>Costs for assuring the integrity of environment attributes throughout their measurement, collection, storage, and distribution are not included.</li> </ul>	Stage 3 (10%) Stage 4 (remaining)	Number of environment attributes
A-12	<b>Establish and operate an authorization service that uses digital policies and attributes to make authorization decisions</b>	The authorization service capability acts as the integrator of the digital policy store and attribute stores to determine whether a subject is authorized to access the requested resource.	<ul style="list-style-type: none"> <li>The cost element accounts for the implementation of a single authorization service. If an agency requires multiple authorization services to support its architecture, each service should be treated as an independent cost.</li> <li>O&amp;M costs not included: maintenance labor and software licensing fees.</li> </ul>	Stage 3	Number of authorization services
A-13	<b>Link applications to authorization service for access control</b>	Once the authorization service is available, existing authentication and authorization performed by applications must be replaced with a link to the authorization service to implement ABAC.	<ul style="list-style-type: none"> <li>Linking individual applications is dependent on the architecture and design of the application as well as the capabilities provided by any commercial-off-the-shelf software used within the application.</li> <li>O&amp;M costs not included: configuration changes as a result of technology refresh; requirement to configure new applications.</li> </ul>	Stage 3 (high sensitivity) Stage 4 (remaining)	Number of applications

### 5.3 OTHER COSTS

Departments and agencies will incur costs beyond those defined in the infrastructure and agency sections above, including the following.

- **Costs for agency specific implementations where agencies choose not to use shared services:** Although shared services can provide significant cost savings, some departments or agencies may choose not to leverage shared services, either because of existing capabilities or because of a need for capabilities not supported by the shared service provider. Departments and agencies must include these costs in their individual cost models.
- **Costs to implement governance activities:** Implementing a governance model for developing baseline digital policy rules, a set of attributes and acceptable values, and minimum verification procedures for determining attribute values across the departments and agencies that comprise the Secret Fabric is a critical success factor for secure information sharing and safeguarding. Although governance activities are generally performed using existing resources, departments and agencies should determine if additional resources will be necessary to support FICAM rollout and maintenance.
- **Costs to update Secret Fabric architecture or other elements:** Updates to current Secret Fabric architecture capabilities that may be required to support FICAM should be incorporated into standard technology upgrade cycles and achieved through recapitalizing existing capabilities. Departments and agencies should assess whether FICAM implementation timelines can be coordinated with currently planned network updates to determine if additional budget planning is needed.
- **Operations and Maintenance costs:** Operations and maintenance costs are out of scope for this planning guidance. However, departments and agencies should understand the impact that the rollout of FICAM capabilities to current O&M budgets to ensure appropriate planning and budgeting is performed for FICAM support.



## APPENDIX A      PROCESS FLOW

The following steps provide a process flow for an access control decision using credentials, digital policy rules, and attributes.

- Step 1.** User attempts to access resource.
- Step 2.** User authenticates, using a PKI-based digital certificate issued under the NSS PKI, to authorization engine that governs access to the desired resource.
- Step 3.** Authorization service determines the digital policy or policies that apply to the requested resource.
- Step 4.** Authorization service determines any additional subject and environment attributes needed by the digital policies.
- Step 5.** Authorization service obtains required attribute values for the authenticated user and the current environment leveraging the attribute map to obtain attribute values for attributes not available from its own attribute exchange service.
- Step 6.** Authorization service compares values of attributes against digital policies and grants or denies access based on the result.

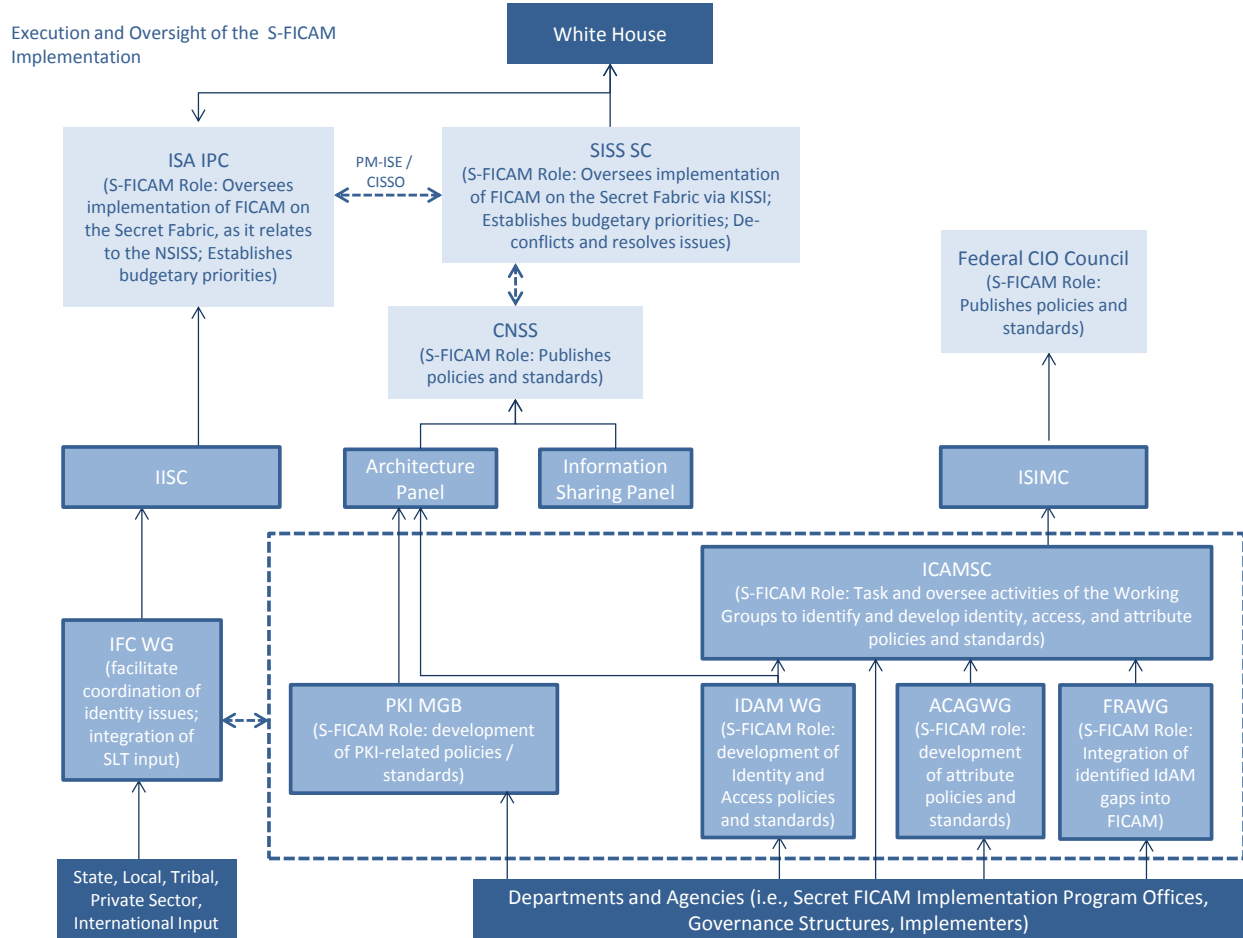
A key element in transitioning from direct individual management of access control of information to automated ABAC is ensuring that the information used for the access decision is trustworthy to the data steward. The first step is to develop a Catalog of Authorities that defines the laws, policies, and other regulations that define requirements for controlling access to resources on the Secret Fabric. Governance and Policy activities relating to the review and approval of the Catalog of Authorities and associated attributes ensure that departments, agencies, and the government as a whole can trust the system to base access control on the rules that are applicable to the information. As subject attribute, environment attribute, and resource attribute definition and validation activities are undertaken, the responsible parties must ensure that (1) the definition of each attribute is clear, (2) that the level of confidence expected to set the value of the attribute is clear, and (3) that the offices or roles within a department have the authority to set the value are defined.

The framework of trust for access control is thus established because:

- The digital policy rules correctly implement the scope of access control that is expected under the Governance and Policy activities
- The attributes and their values are clearly defined so that data stewards know exactly what characteristics of the users, environments, and resources they are using to control access
- The management of attribute values are determined and assigned for each user, environment, and resource attribute by the persons or offices that are authoritative for the relevant attribute

## APPENDIX B ORGANIZATION RELATIONSHIP MAP

Figure A-1 provides a high level overview of the various organizations, committees, and working groups that will support the implementation of FICAM on the Secret Fabric as discussed in Section 3.



**Figure A-1: Organizations Supporting Activities Related to FICAM on the Secret Fabric**

Additional information about each of these groups - including its full name, the authority under which it operates, the purpose of the group, and recent activities performed by the group that are relevant to implementing FICAM on the Secret Fabric - is provided in the following table.

Name	Authority	Purpose	Recent Activity related to FICAM on the Secret Fabric
<b>ISA IPC Information Sharing and Access Interagency Policy Committee</b>	<ul style="list-style-type: none"> <li>• Presidential Policy Directive (PPD)-1, Organization of the National Security Council System.</li> <li>• Successor to the Information Sharing Council established by section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.</li> </ul>	<p>Serve as main day-to-day forum for interagency coordination of national security policy; provide policy analysis for consideration by the more senior committees of the National Security Staff system and ensure timely responses to decisions made by the President. Specifically, the ISA IPC is responsible for the integration and implementation of policies, processes, standards, and technologies to promote secure and responsible national security information sharing.</p>	<p>Includes the following Sub-committees and Working Groups, as described below.</p> <ul style="list-style-type: none"> <li>• Information Integration Sub-Committee (IISC)</li> <li>• Identity Federation Coordination (IFC) WG (proposed), under the IISC</li> </ul>
<b>IISC Information Integration Sub- Committee</b>	<ul style="list-style-type: none"> <li>• Authorized by the ISA IPC, consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended.</li> </ul>	<p>Advise and support the ISA IPC by addressing of issues related to (1) assured interoperability across Sensitive But Unclassified (SBU) networks; (2) assured interoperability and governance across all Secret networks, data-related processes, and standards, and (3) interagency architecture guidance that supports data aggregation capabilities in support of non-traditional screening for terrorism.</p> <p>Its Working Groups include: Data Aggregation Working Group; SBU Working Group; Standards Working Group; and Standards Coordinating Council (which includes outside standards development organizations).</p>	<ul style="list-style-type: none"> <li>• Proposed establishment of the Identity Federation Coordination (IFC) Working Group to ensure representation from affiliates.</li> </ul>
<b>IFC WG Identity Federation Coordination Working Group (proposed)</b>	<ul style="list-style-type: none"> <li>• Authorized by the ISA IPC, consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended.</li> <li>• Assists the Classified Information Sharing and Safeguarding Office (CISSO) in its support of the SISS SC established by EO 13587.</li> </ul>	<p>Serve as the facilitator for coordination among the various identity federations that exist in the Federal Government on all classifications and within the state, local, tribal, territorial, and private sector affiliate environments to ensure support of the ISE; advise the SISS SC by addressing interoperability and consistency between identity federations; and leverage the federal IC, CNSS, affiliate processes and other forums to capture best practices and lessons learned from ICAM efforts.</p>	<ul style="list-style-type: none"> <li>• Established to also address Priority Objective #4, Implementation of FICAM on all Fabrics, from the NSISS.</li> <li>• Coordinating federal-wide identity body.</li> </ul>

Name	Authority	Purpose	Recent Activity related to FICAM on the Secret Fabric
<b>SISS SC Senior Information Sharing and Safeguarding Steering Committee</b>	<ul style="list-style-type: none"> <li>EO 13587 “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.”</li> </ul>	<p>Exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.</p>	<ul style="list-style-type: none"> <li>Established five priorities and corresponding IOC and FOC goals aligned to each of five information sharing and safeguarding priorities to measure implementation progress: Removable Media, Reduce Anonymity, Insider Threat Program, Access Control, and Enterprise Audit.</li> <li>Currently considering a proposal from the Classified Shared Services Committee for the establishment of an Identity and Access Management Line of Business to coordinate the creation and delivery of shared services on the sensitive but unclassified and Secret fabrics.</li> </ul>
<b>CNSS Committee on National Security Systems</b>	<ul style="list-style-type: none"> <li>National Security Directive (NSD)-42 “National Policy for the Security of National Security Telecommunications and Applications.”</li> <li>EO 13284 “Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security.”</li> <li>EO 13231 (Critical Infrastructure Protection in the Information Age).</li> <li>EO 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information).</li> </ul>	<p>Provide a forum for the discussion of policy issues and is responsible for setting national-level information assurance policies, directives, instructions, operational procedures, guidance, and advisories for United States Government departments and agencies for the security of National Security Systems through the CNSS Issuance System.</p>	<ul style="list-style-type: none"> <li>Established the PKI WG which Developed CNSSP 25 and CNSSI 1300.</li> <li>Co-established the IdAM WG with the ICAMSC.</li> </ul>

Name	Authority	Purpose	Recent Activity related to FICAM on the Secret Fabric
<b>Information Sharing Panel</b>	<ul style="list-style-type: none"> <li>• CNSS Governing and Operating Procedures</li> </ul>	<p>Ensure that the priority of effective information sharing is represented in all CNSS activities and is integrated with security and other considerations in the issuances, decisions, and recommendations of the Subcommittee. Promote coordination, consistency, and leveraging of efforts between CNSS and other organizations with information-sharing authorities or a major stake in the effective information sharing of classified network fabrics. Make recommendations for processes to assure that coordination of CNSS issuances with other information-sharing stakeholders is efficient and results in guidance that meets the needs of information custodians and system operators.</p>	<ul style="list-style-type: none"> <li>• N/A</li> </ul>
<b>Architecture Panel</b>	<ul style="list-style-type: none"> <li>• CNSS Governing and Operating Procedures.</li> </ul>	<p>Oversee development of an architecture framework and standards for NSS and associated shared/common services across the Federal Government. Coordinate with organizations across the Federal Government on issues that may affect NSS architectural development and leverage their architectural efforts with particular emphasis on the Department of Defense and the IC, which between them operate the majority of NSS.</p>	<ul style="list-style-type: none"> <li>• N/A</li> </ul>
<b>PKI MGB PKI Member Governing Body</b>	<ul style="list-style-type: none"> <li>• Established by CNSS.</li> </ul>	<p>Assist the NSS PKI Policy Management Authority (PMA) in managing the NSS PKI. Conduct policy, management, operational, security, and administrative reviews of all aspects of NSS PKI and make recommendations to the PMA for implementation approval. Responsible for policy management, operational direction, internal audit (including corrective action approval and monitoring), external cross certification review and acceptance, and governance over the NSS PKI CSP.</p>	<ul style="list-style-type: none"> <li>• Developed the Concept of Operations for the PKI Common Service Provider.</li> <li>• Developed CNSSD 506.</li> </ul>

Name	Authority	Purpose	Recent Activity related to FICAM on the Secret Fabric
<b>CSP Governance Board</b>	<ul style="list-style-type: none"> <li>Established by the PKI MGB.</li> </ul>	Facilitate and coordinate developmental and operational activities of the CSP.	<ul style="list-style-type: none"> <li>Finalized the requirements for initial operating capability of the CSP.</li> </ul>
<b>IdAM WG Identity and Access Management Working Group—established jointly with ICAMSC, under the Federal CIO Council</b>	<ul style="list-style-type: none"> <li>Joint working group formed by the CNSS and the ICAMSC.</li> </ul>	Collaborate on IdAM related issues and solutions across both unclassified and Secret Fabrics.	<ul style="list-style-type: none"> <li>Published the ICAM Lexicon</li> <li>Published the Gap Analysis Between the FICAM and U.S. Secret Networks.</li> <li>Published the Secret FICAM Recommendations Paper.</li> </ul>
<b>Federal CIO Council Federal Chief Information Officer Council</b>	<ul style="list-style-type: none"> <li>EO 13011 “Federal Information Technology.”</li> <li>E-Government Act of 2002.</li> </ul>	Serve as principal interagency forum to improve agency practices related to the design, acquisition, development, modernization, sustainment, use, sharing, and performance of Federal Government IT.	<ul style="list-style-type: none"> <li>Published the Federal Identity, Credential, and Access Management (FICAM) Roadmap for unclassified networks.</li> </ul>
<b>ISIMC Information Security and Identity Management Committee</b>	<ul style="list-style-type: none"> <li>Established by the Federal CIO Council.</li> </ul>	Identify and recommend information security and identity management enhancements to policies, processes, and solutions that address the strategies and improve upon identification management solutions; Identify high priority security and identity management initiatives; Develop recommendations for policies, procedures, and standards to address those initiatives that enhance the security posture and protection afforded to Federal Government networks, information, and applications.	<ul style="list-style-type: none"> <li>Established the ICAMSC.</li> </ul>
<b>ICAMSC Identity, Credential, and Access Management Sub-Committee</b>	<ul style="list-style-type: none"> <li>Chartered under the ISIMC.</li> </ul>	Align the identity management activities of federal executive branch agencies.	<ul style="list-style-type: none"> <li>Established the ACAG WG, the FRAWG, and co-established the CNSS IdAM WG.</li> </ul>
<b>ACAG WG</b>	<ul style="list-style-type: none"> <li>Established by the ICAMSC.</li> </ul>	Focus on governance, coordination of semantics,	<ul style="list-style-type: none"> <li>Released the Attribute</li> </ul>

Name	Authority	Purpose	Recent Activity related to FICAM on the Secret Fabric
<b>Access Control Attribute Governance</b>		syntax, and protocol work. Coordinate a common language and understanding of access control attributes across the Federal Government.	Management Roadmap.
<b>FRAWG FICAM Roadmap Alignment Working Group</b>	<ul style="list-style-type: none"> <li>Established by the ICAMSC.</li> </ul>	Review and identify gaps in the FICAM; Assigns the identified gap to the appropriate working group or create a Tiger Team to address the issue.	<ul style="list-style-type: none"> <li>N/A This working group just began operations.</li> </ul>

## APPENDIX C ACTIVITIES AND INTERDEPENDENCIES

This section provides a summary list of activities grouped by activity type and identifies dependency relationships between the activities. The embedded object contains a graphical representation of these relationships in a Microsoft Visio format.



FICAM Planning Guidance Dependencies 25SEP2013.vsd

### C.1 GOVERNANCE ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>GOV-01</b>	Establish the IFC WG as the facilitator for coordination among the various identity federations that exist in the Federal Government on all classifications and between federal agencies and their affiliates.	ISA IPC	Stage 1 Goal Predecessor Activities: None Successor Activities: GOV-09, GOV-10
<b>GOV-02</b>	Develop department and agency implementation plans for implementing FICAM on the Secret Fabric based on this planning guidance.	Departments and Agencies	Stage 1 Future Predecessor Activities: POL-02 Successor Activities: GOV-03
<b>GOV-03</b>	Establish department or agency organizational and policy requirements to implement agency implementation plans for FICAM on the Secret Fabric.	Departments and Agencies	Stage 1 Future Predecessor Activities: GOV-02 Successor Activities: GOV-11
<b>GOV-04</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of PKI policies and standards for the Secret Fabric).	PKI MGB	Stage 1 Future Predecessor Activities: None Successor Activities: None
<b>GOV-05</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of identity and access policies and standards for the Secret Fabric).	ICAMSC	Stage 1 Future Predecessor Activities: None Successor Activities: None
<b>GOV-06</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of identity and access policies and standards for the Secret Fabric).	IdAM WG	Stage 1 Future Predecessor Activities: None Successor Activities: None
<b>GOV-07</b>	Incorporate activities from this planning guidance into work plans as appropriate (e.g., development and publishing of attribute policies and standards for the Secret Fabric).	ACAG WG	Stage 1 Future Predecessor Activities: None Successor Activities: None
<b>GOV-08</b>	Incorporate technology requirements for	Department and	Stage 2 Goal



Number	Activity	Responsible Party	Dependencies
	implementing FICAM capabilities into agency implementation plans. Include an ongoing process for evaluating further appropriate technological enhancements to improve agency alignment with FICAM capabilities.	Agency Governance Bodies	Predecessor Activities: ENAB-04 Successor Activities: None
<b>GOV-09</b>	Develop guidelines and requirements for sharing network and application activity logs across the Secret Fabric to applicable agencies to support audit review.	ICAMSC, IFC WG	Stage 3 Goal Predecessor Activities: GOV-01, ENAB-04 Successor Activities: ENAB-18
<b>GOV-10</b>	Review interagency governance structures, including working group charters, and modify them, as required, to support on-going maintenance activities for operating FICAM on the Secret Fabric.	ICAMSC, CNSS	Stage 3 Future Predecessor Activities: GOV-01 Successor Activities: None
<b>GOV-11</b>	Review department or agency organizational and policy requirements and modify them, as required, to support on-going maintenance activities for operating on the Secret Fabric.	Departments and Agencies	Stage 3 Future Predecessor Activities: GOV-03 Successor Activities: None
<b>GOV-12</b>	Identify and implement processes for maintaining and updating identified subject, resource, and environment attributes.	ACAG WG	Stage 4 Goal Predecessor Activities: SATT-09, SATT-10, SATT-12, EATT-03 Successor Activities: None
<b>GOV-13</b>	Define governance processes to manage digital policies that apply to the full Secret Fabric.	CNSS, ICAMSC	Stage 4 Goal Predecessor Activities: DPOL-06 Successor Activities: None
<b>GOV-14</b>	Define governance processes to manage agency specific digital policies.	Department and Agency Governance Bodies	Stage 4 Goal Predecessor Activities: DPOL-07 Successor Activities: None

## C.2 POLICY ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>POL-01</b>	Develop interagency policy guidance to require adherence to FICAM Planning Guidance for the Secret Fabric.	SISS SC, ISA IPC	Stage 1 Goal Predecessor Activities: None Successor Activities: None
<b>POL-02</b>	Publish policy that requires departments and agencies to implement FICAM on the Secret Fabric and sets target dates for achieving	CNSS, ICAMSC	Stage 1 Future Predecessor Activities: GOV-02

Number	Activity	Responsible Party	Dependencies
	implementation.		Successor Activities: None
<b>POL-03</b>	Review the Catalog of Authorities, developed per DPOL-01, including legal review and approval.	ICAMSC, IdAM WG	Stage 2 Goal Predecessor Activities: DPOL-01, DPOL-02 Successor Activities: POL-04
<b>POL-04</b>	Identify any gaps and overlaps in the Catalog of Authorities, developed per DPOL-01, and develop an action plan to address.	ICAMSC, CNSS	Stage 2 Future Predecessor Activities: POL-03 Successor Activities: POL-05
<b>POL-05</b>	Draft new policies or propose changes to existing policies to address identified policy gaps and overlaps.	CNSS, ICAMSC	Stage 2 Future Predecessor Activities: POL-04 Successor Activities: None

### C.3 BUSINESS ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>BUS-01</b>	Identify the cost model for participating agencies and shared service providers for the CSP.	SISS SC, ISA IPC	Stage 1 Goal Predecessor Activities: None Successor Activities: BUS-06
<b>BUS-02</b>	Designate a governance body responsible for assessing and addressing the overall risk management for FICAM on the Secret Fabric to enable departments and agencies to rely on attribute values asserted by other departments and agencies as part of access decisions.	SISS SC, ISA IPC	Stage 1 Future Predecessor Activities: None Successor Activities: BUS-03
<b>BUS-03</b>	Identify a framework for individual agencies to manage the risk of trusting credentials and attribute values issued and managed by a third party and ensure it is consistent with their mission and with the overall Secret Fabric risk management governance and technical implementations.	SISS SC, ISA IPC	Stage 1 Future Predecessor Activities: BUS-02 Successor Activities: BUS-10
<b>BUS-04</b>	Integrate requirements for hardware and software upgrades needed to implement FICAM on the Secret Fabric into overall information technology acquisition planning and investment activities.	Departments and Agencies	Stage 1 Future Predecessor Activities: ENAB-04 Successor Activities: CRED-05, BUS-08
<b>BUS-05</b>	Coordinate and distribute budget guidance for implementing FICAM on the Secret Fabric.	SISS SC, OMB	Stage 1 Future Predecessor Activities: None

Number	Activity	Responsible Party	Dependencies
			Successor Activities: BUS-06
<b>BUS-06</b>	Incorporate budget guidance for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies	Stage 1 Future Predecessor Activities: BUS-01, BUS-05 Successor Activities: BUS-07
<b>BUS-07</b>	Identify the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB	Stage 2 Goal Predecessor Activities: BUS-06 Successor Activities: BUS-08, BUS-11
<b>BUS-08</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC	Stage 2 Goal Predecessor Activities: BUS-04, BUS-07 Successor Activities: BUS-09
<b>BUS-09</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies	Stage 2 Goal Predecessor Activities: BUS-08 Successor Activities: BUS-12
<b>BUS-10</b>	Review trust model assumptions for management of attribute values for employees and affiliates for all subject attributes to ensure ability of all departments and agencies to accept attribute values from other departments and agencies and update as required.	SISS SC, ISA IPC	Stage 3 Goal Predecessor Activities: BUS-03 Successor Activities: CRED-12
<b>BUS-11</b>	Review and update, as required, the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB	Stage 3 Future Predecessor Activities: BUS-07 Successor Activities: BUS-16
<b>BUS-12</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC	Stage 3 Future Predecessor Activities: BUS-09 Successor Activities: BUS-13
<b>BUS-13</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies	Stage 3 Future Predecessor Activities: BUS-12 Successor Activities: BUS-14
<b>BUS-14</b>	Refine agency budget estimates based on implementation and maintenance costs defined in agency implementation plans.	SISS SC, ISA IPC	Stage 4 Goal Predecessor Activities: BUS-13

Number	Activity	Responsible Party	Dependencies
			Successor Activities: BUS-15
<b>BUS-15</b>	Incorporate funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric.	Departments and Agencies	Stage 4 Goal Predecessor Activities: BUS-14 Successor Activities: None
<b>BUS-16</b>	Review and update, as required, the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies that will rely on shared services.	SISS SC, ISA IPC, OMB	Stage 4 Goal Predecessor Activities: BUS-11 Successor Activities: None

#### C.4 CREDENTIALING ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>CRED-01</b>	Establish the NSS PKI CSP capability to issue certificates to entities from agencies that are not operating their own NSS PKI CA.	PKI MGB	Stage 1 Goal Predecessor Activities: None Successor Activities: CRED-03
<b>CRED-02</b>	Establish agency NSS PKI CAs for those agencies that will not be obtaining certificates from the NSS PKI CSP.	Departments and Agencies	Stage 1 Goal Predecessor Activities: None Successor Activities: CRED-03
<b>CRED-03</b>	Establish registration infrastructure needed to support issuing certificates to entities within the department or agency.	Departments and Agencies	Stage 1 Goal Predecessor Activities: CRED-01, CRED-02 Successor Activities: CRED-04, CRED-06, CRED-10
<b>CRED-04</b>	Issue certificates to a minimum of 10% of employees and affiliates, focusing on those who require access to resources hosted by other departments and agencies.	Departments and Agencies	Stage 1 Goal Predecessor Activities: CRED-03 Successor Activities: CRED-07, ENAB-01, ENAB-02
<b>CRED-05</b>	Install smart card readers and middleware on a minimum of 10% of Secret Fabric workstations, including thin clients, that will be used by employees and affiliates who receive NSS PKI hardware certificates on smart cards.	Departments and Agencies	Stage 1 Goal Predecessor Activities: BUS-04, ENAB-05 Successor Activities: CRED-08, ENAB-01, ENAB-02
<b>CRED-06</b>	Issue certificates to web servers or other applications that host high sensitivity resources that are currently shared with other departments and agencies.	Departments and Agencies	Stage 1 Goal Predecessor Activities: CRED-03 Successor Activities:

Number	Activity	Responsible Party	Dependencies
			CRED-09, ENAB-01
<b>CRED-07</b>	Issue certificates to at least 90% of employees and affiliates who have fully provisioned network accounts on the Secret Fabric.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-04 Successor Activities: ENAB-07, ENAB-08, CRED-11
<b>CRED-08</b>	Install smart card readers and middleware on all Secret Fabric workstations, including thin clients, that will be used by employees and affiliates who receive NSS PKI hardware certificates on smart cards.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-05 Successor Activities: ENAB-07, ENAB-08
<b>CRED-09</b>	Issue certificates to web servers or other applications that host high and medium sensitivity resources that are currently shared with other departments and agencies.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-06 Successor Activities: CRED-11, ENAB-07
<b>CRED-10</b>	Issue certificates to network domain controllers.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-03 Successor Activities: ENAB-08
<b>CRED-11</b>	Issue certificates to all employees, affiliates, and non-person entities (such as web servers or other applications) that require certificates to support authentication on the Secret Fabric.	Departments and Agencies	Stage 3 Goal Predecessor Activities: CRED-07, CRED-09 Successor Activities: ENAB-13
<b>CRED-12</b>	Implement trust agreements to facilitate certificate validation processing with international partners to facilitate authentication of non-NSS PKI certificates.	PKI MGB	Stage 4 Goal Predecessor Activities: BUS-10, SATT-14, ENAB-13 Successor Activities: None

### C.5 SUBJECT ATTRIBUTE ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>SATT-01</b>	Identify standards, interfaces, and models for sharing subject attribute information, including identifier, attribute name, attribute value, and availability.	ACAG WG, ICAMSC	Stage 1 Future Predecessor Activities: ENAB-05 Successor Activities: ENAB-10, SATT-03
<b>SATT-02</b>	Determine subject attributes that will be needed to support ABAC decisions based on the Catalog of Authorities.	Department and Agency Governance Bodies	Stage 2 Future Predecessor Activities: DPOL-05 Successor Activities: SATT-03, SATT-05 SATT-09, SATT-10

Number	Activity	Responsible Party	Dependencies
<b>SATT-03</b>	Identify and establish authoritative attribute stores for subject attributes.	Departments and Agencies	Stage 2 Future Predecessor Activities: SATT-01, SATT-02 Successor Activities: SATT-04, SATT-12
<b>SATT-04</b>	Establish attribute mapping capability to allow agencies to identify the location of subject attributes that are not locally managed.	ICAMSC Architecture Group	Stage 3 Goal Predecessor Activities: SATT-03 Successor Activities: SATT-13
<b>SATT-05</b>	Determine whether values for attributes identified in Stage 2 currently exist in a format that supports migration to an existing attribute store for agency employees and affiliates.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-02 Successor Activities: SATT-06, SATT-07 SATT-14
<b>SATT-06</b>	For attributes that exist in a usable format, identify authoritative source and develop processes and interfaces for making attribute values available to attribute exchange services.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-05 Successor Activities: SATT-08
<b>SATT-07</b>	For attributes that do not currently exist in a usable format, identify processes for determining and managing the values of the attribute for employees and affiliates and identify a mechanism for provisioning attribute values that will be available to attribute exchange services.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-05 Successor Activities: SATT-08
<b>SATT-08</b>	Populate attribute values in authoritative data stores for users of high sensitivity applications.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-06, SATT-07 Successor Activities: SATT-11, ENAB-15
<b>SATT-09</b>	Modify on-boarding and provisioning processes to include provisioning and maintenance of defined subject attributes for employees and affiliates.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-02 Successor Activities: GOV-12
<b>SATT-10</b>	Modify out-board and de-provisioning processes to include update and deletion of defined subject attributes for employees and affiliates.	Departments and Agencies	Stage 3 Goal Predecessor Activities: SATT-02 Successor Activities: GOV-12
<b>SATT-11</b>	Complete the population of attribute values for employees and affiliates used in digital policy rules in authoritative data stores.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-08 Successor Activities: SATT-12

Number	Activity	Responsible Party	Dependencies
<b>SATT-12</b>	Ensure that attribute values for employees and affiliates used in digital policy rules are accessible via agency attribute exchange services.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-03, SATT-11 Successor Activities: GOV-12, SATT-13
<b>SATT-13</b>	Ensure all attribute values used in digital policy rules are identified in the shared attribute map so other agencies can locate them.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-04, SATT-12, ENAB-12 Successor Activities: ENAB-17
<b>SATT-14</b>	Identify attribute stores maintained by affiliates or alternative sources of affiliate attributes that rise to the authoritative level necessary to satisfy the FICAM trust framework.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-05 Successor Activities: SATT-15, CRED-12
<b>SATT-15</b>	Ensure that agency attribute exchange services have access to affiliate attribute stores.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-14 Successor Activities: None

## C.6 RESOURCE ATTRIBUTE ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>RATT-01</b>	Identify mechanisms for binding resource attributes to resources.	Departments and Agencies	Stage 1 Future Predecessor Activities: ENAB-04 Successor Activities: RATT-04
<b>RATT-02</b>	Identify standards, interfaces, and models for registering, binding, and sharing resource attribute information including availability information.	ACAG WG, ICAMSC	Stage 1 Future Predecessor Activities: ENAB-05 Successor Activities: RATT-04, ENAB-10
<b>RATT-03</b>	Determine resource attributes that will be needed to link resources to applicable requirements based on the Catalog of Authorities.	Department and Agency Governance Bodies	Stage 2 Future Predecessor Activities: DPOL-05 Successor Activities: RATT-04
<b>RATT-04</b>	Implement binding of resource attributes to resources for resources that are intended to be shared.	Departments and Agencies	Stage 3 Goal Predecessor Activities: RATT-01, RATT-02 RATT-03 Successor Activities: ENAB-15, RATT-05
<b>RATT-05</b>	Ensure resource attributes are defined, validated, and bound to associated	Departments and Agencies	Stage 4 Goal Predecessor Activities:

Number	Activity	Responsible Party	Dependencies
	resources.		RATT-04 Successor Activities: ENAB-17

### C.7 ENVIRONMENT ATTRIBUTE ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>EATT-01</b>	Identify standards, interfaces, and models for sharing environment attribute information, including identifier, attribute name, attribute value, and availability.	ACAG WG, ICAMSC	Stage 1 Future Predecessor Activities: ENAB-04 Successor Activities: ENAB-10
<b>EATT-02</b>	Determine environment attributes that will be needed to support ABAC decisions based on the Catalog of Authorities.	Department and Agency Governance Bodies	Stage 2 Future Predecessor Activities: DPOL-05 Successor Activities: EATT-03
<b>EATT-03</b>	Identify environment attribute sources and establish connections to attribute exchange services.	Departments and Agencies	Stage 3 Goal Predecessor Activities: EATT-02 Successor Activities: ENAB-15, GOV-12

### C.8 DIGITAL POLICY ACTIVITIES

Number	Activity	Responsible Party	Dependencies
<b>DPOL-01</b>	Develop a Catalog of Authorities defining laws, policies, and other regulations that define requirements for controlling access to resources on the Secret Fabric.	Department and Agency Governance Bodies	Stage 1 Goal Predecessor Activities: None Successor Activities: DPOL-02, DPOL-04,
<b>DPOL-02</b>	Identify shared digital policies that apply across the Secret Fabric.	ACAG WG	Stage 2 Goal Predecessor Activities: DPOL-01 Successor Activities: DPOL-03, POL-03
<b>DPOL-03</b>	Perform a compliance office review of the set of shared digital policies.	OMB	Stage 2 Future Predecessor Activities: DPOL-02 Successor Activities: DPOL-06
<b>DPOL-04</b>	Identify initial set of digital policies that will be used to govern access to resources intended to be shared across the Secret Fabric	Department and Agency Governance Bodies	Stage 2 Future Predecessor Activities: DPOL-01 Successor Activities: DPOL-05
<b>DPOL-05</b>	Develop agency specific digital policy rules governing access control to department or	Departments and Agencies	Stage 2 Future Predecessor Activities:



Number	Activity	Responsible Party	Dependencies
	agency resources.		DPOL-04 Successor Activities: DPOL-07, EATT-02, RATT-03, SATT-02
<b>DPOL-06</b>	Identify full set of common digital policy rules that apply across the Secret Fabric.	ICAMSC, IdAM WG	Stage 4 Goal Predecessor Activities: DPOL-03 Successor Activities: DPOL-07, GOV-13
<b>DPOL-07</b>	Ensure digital policy stores are fully populated with digital policy rules.	Departments and Agencies	Stage 4 Goal Predecessor Activities: DPOL-05, DPOL-06 Successor Activities: ENAB-17, GOV-14

### C.9 ENABLING ACTIVITIES

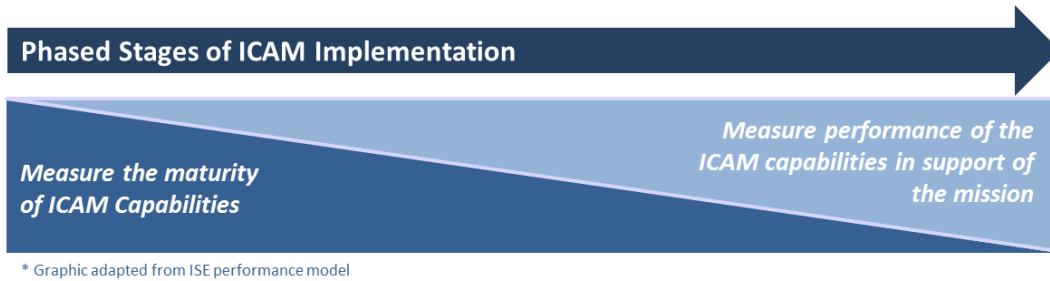
Number	Activity	Responsible Party	Dependencies
<b>ENAB-01</b>	Enable high sensitivity applications that are currently shared with other departments and agencies to ensure the subject has authenticated using a PKI certificate.	Departments and Agencies	Stage 1 Goal Predecessor Activities: CRED-04, CRED-05, CRED-06 Successor Activities: ENAB-03, ENAB-16
<b>ENAB-02</b>	Implement mandatory certificate-based network logon to Secret Fabric networks for at least 10% of users.	Departments and Agencies	Stage 1 Goal Predecessor Activities: CRED-04, CRED-05 Successor Activities: None
<b>ENAB-03</b>	Ensure enabled applications generate logs indicating the identifier used to authenticate the user.	Departments and Agencies	Stage 1 Goal Predecessor Activities: ENAB-01 Successor Activities: None
<b>ENAB-04</b>	Define a target network architecture that defines the level of required interoperability of Secret Fabric networks for information sharing and safeguarding and identifies the interfaces necessary for departments and agencies to use Secret Fabric shared services (such as PKI or Identity Providers).	ICAMSC Architecture Group	Stage 1 Future Predecessor Activities: None Successor Activities: GOV-08, GOV-09, RATT-01, BUS-04, EATT-01, ENAB-05
<b>ENAB-05</b>	Identify standards and protocols for performing authentication; obtaining subject, environment, and resource attributes; and applying digital policy rules to make access control decisions. Standards and protocols identified must ensure interoperability across the Secret	ICAMSC Architecture Group	Stage 1 Future Predecessor Activities: ENAB-04 Successor Activities: RATT-02, ENAB-06, SATT-01, CRED-05

Number	Activity	Responsible Party	Dependencies
	Fabric and, to the extent possible, also provide interoperability with those standards and protocols used by the IC and unclassified communities.		
<b>ENAB-06</b>	Develop prototype of attribute exchange capability on the Secret Fabric as a reference implementation for attribute sharing.	PM-ISE and Partnering Agency Provider(s)	Stage 1 Future Predecessor Activities: ENAB-05 Successor Activities: ENAB-11
<b>ENAB-07</b>	Enable high and medium sensitivity applications that are currently shared with other departments and agencies to ensure the subject has authenticated using a PKI certificate.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-07, CRED-08, CRED-09 Successor Activities: ENAB-13
<b>ENAB-08</b>	Implement mandatory certificate-based network logon to Secret Fabric networks.	Departments and Agencies	Stage 2 Goal Predecessor Activities: CRED-07, CRED-10, CRED-08 Successor Activities: ENAB-09
<b>ENAB-09</b>	Ensure network logon generates activity logs that include the identifier of the entity that logged on.	Departments and Agencies	Stage 2 Goal Predecessor Activities: ENAB-08 Successor Activities: None
<b>ENAB-10</b>	Implement prototype of authorization service that implements digital policy rules based on resource attributes and includes discovery and use of subject and environment attributes.	PM-ISE and Partnering Agency Provider(s)	Stage 2 Future Predecessor Activities:SATT-01, EATT-01, RATT-02 Successor Activities: ENAB-15
<b>ENAB-11</b>	Develop attribute exchange services and link them with agency attribute stores.	Departments and Agencies	Stage 2 Future Predecessor Activities: ENAB-06 Successor Activities: ENAB-12
<b>ENAB-12</b>	Test attribute exchange service interfaces with Stage 1 prototype implementation to measure interoperability.	Departments and Agencies	Stage 2 Future Predecessor Activities: ENAB-11 Successor Activities: ENAB-15, SATT-13
<b>ENAB-13</b>	Ensure that all applications that manage resources that are intended to be shared with other departments and agencies require certificate-based authentication of all authorized users.	Departments and Agencies	Stage 3 Goal Predecessor Activities: CRED-11, ENAB-07 Successor Activities: ENAB-14, CRED-12, ENAB-17

Number	Activity	Responsible Party	Dependencies
<b>ENAB-14</b>	Ensure that applications log all resource access using identifiers contained in certificates	Departments and Agencies	Stage 3 Goal Predecessor Activities: ENAB-13 Successor Activities: None
<b>ENAB-15</b>	Implement agency authorization services that perform access control based on digital policies linked to resources and values of associated subject and environment attributes.	Departments and Agencies	Stage 3 Goal Predecessor Activities: ENAB-10, ENAB-12, RATT-04, EATT-03, SATT-08 Successor Activities: ENAB-16
<b>ENAB-16</b>	Enable 25% high sensitivity applications to use authorization services for access control.	Department and Agency Governance	Stage 3 Goal Predecessor Activities: ENAB-15, ENAB-01 Successor Activities: None
<b>ENAB-17</b>	Enable all high and medium sensitivity applications to use authorization services for access control.	Departments and Agencies	Stage 4 Goal Predecessor Activities: SATT-13, RATT-05, DPOL-07, ENAB-13 Successor Activities: ENAB-18
<b>ENAB-18</b>	Ensure applications generate logs indicating the identifier used to authenticate to the system, the values of attributes used in the access control decision, and the source of those attribute values.	Departments and Agencies	Stage 4 Goal Predecessor Activities: ENAB-17, GOV-09 Successor Activities: None

## APPENDIX D PROGRESS AND PERFORMANCE METRICS

Successful implementation of this document requires a management approach that assesses progress towards achieving the capabilities at each stage in addition to the overall goal of a coordinated ICAM implementation on the Secret Fabric. The phased approach in Section 4 of this document means that the activities at one stage of implementation build upon the activities and capabilities achieved in the previous stages. As these capabilities mature, the metrics associated with these capabilities should also mature, as shown in **Error! Reference source not found.**



**Figure C-1: Measuring Capabilities to Measuring Performance**

Progress measures are organized by the seven capabilities and divided into agency metrics (i.e., agency-specific implementation activities) and interagency metrics (i.e., shared implementation activities via governance). Performance measures associated should be developed through the ICAM governance process, based on the overall goals for information sharing and safeguarding established in NSISS and the strategic vision defined in Section 2. The resulting reports should be used by departments and agencies to compare their progress to the goals and timelines established in this document. Accordingly, such performance measures are not defined in this document.

### D.1 CAPABILITY: CERTIFICATE-BASED AUTHENTICATION TO APPLICATIONS ACROSS THE SECRET FABRIC, INCLUDING EMPLOYEES, AFFILIATES, AND INTERNATIONAL PARTNERS

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency established NSS PKI CAs for those agencies that will not be obtaining certificates from the NSS PKI CSP?	Stage 1	Yes
Has your agency established registration infrastructure to support issuing certificates to entities with your department or agency?	Stage 1	Yes
Number of certificates issued.	Stage 1	[Agency provided number]
	Stage 2	[Agency provided number]
	Stage 3	[Agency provided number]
Percentage of employees and non-federal affiliates who have been issued a certificate (number of certificates issued divided by total number of employees and non-federal affiliates with network accounts).	Stage 1	10%
	Stage 2	90%
	Stage 3	100%

Metric	Stage	Target
Number of high sensitivity applications.	Stage 1	[Agency provided number]
	Stage 2	[Agency provided number]
	Stage 3	[Agency provided number]
	Stage 4	[Agency provided number]
Has your agency enabled high sensitivity applications to ensure the subject has authenticated using a PKI certificate?	Stage 1	Yes
Number of medium sensitivity applications.	Stage 1	[Agency provided number]
	Stage 2	[Agency provided number]
	Stage 3	[Agency provided number]
	Stage 4	[Agency provided number]
Has your agency enabled medium sensitivity applications to ensure the subject has authenticated using a PKI certificate?	Stage 2	Yes
Number of applicable Secret Fabric workstations.	Stage 1	[Agency provided number]
Number of Secret Fabric workstations, including thin clients, that will be used by employees and non-federal affiliates who receive NSS PKI hardware certificates on smart cards.	Stage 1	[Agency provided number]
	Stage 2	[Agency provided number]
Percentage of Secret Fabric workstations, including thin clients, used by employees and affiliates who receive NSS PKI hardware certificates on smart cards (counted above) that have been installed with smart card readers and middleware (number of workstations installed with smart card readers divided by the total number of Secret Fabric workstations, including thin clients, used by employees and affiliates who receive NSS PKI hardware certificates on smart cards (counted above)).	Stage 1	10%
	Stage 2	100%
Has your agency issued certificates to web servers or other applications that host high sensitivity resources and that are currently shared with other departments and agencies?	Stage 1	Yes
Has your agency issued certificates to web servers or other applications that host medium sensitivity resources and that are currently shared with other departments and agencies?	Stage 2	Yes
Has your agency issued certificates to all network domain controllers?	Stage 2	Yes
Has your agency implemented mandatory certificate-based network logon to Secret Fabric networks?	Stage 1	10%
	Stage 2	100%
Has your agency issued certificates to all employees, affiliates, and non-	Stage 3	Yes

Metric	Stage	Target
person entities (such as web servers or other applications) that require certificates to support authentication and have fully provisioned network accounts on the Secret Fabric?		
Has the PKI MGB implemented trust agreements to facilitate certificate validation processing with international partners to facilitate authentication of non-NSS PKI certificates?	Stage 4	Yes
<b>Interagency Metrics</b>		
Has the PKI MGB established the NSS PKI CSP capability to issue certificates to entities from any agencies that are not operating their own NSS PKI CA?	Stage 1	Yes

**D.2 CAPABILITY: ACCESS TO ENABLED APPLICATIONS LOGGED USING UNIQUE IDENTIFIER CONTAINED IN DIGITAL CERTIFICATES WHICH IS LINKED TO SUBJECT ATTRIBUTES**

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency enabled applications to generate logs that indicate the identifier used to authenticate the user?	Stage 1	Yes
<b>Interagency Metrics</b>		
No associated metrics.		

**D.3 CAPABILITY: CERTIFICATE-BASED NETWORK LOGON**

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency ensured that the network logon generates activity logs that include the identifier of the entity that logged on?	Stage 2	Yes
<b>Interagency Metrics</b>		
No associated metrics.		

**D.4 CAPABILITY: NETWORK ACCESS LOGGED USING UNIQUE IDENTIFIER CONTAINED IN DIGITAL CERTIFICATES**

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency ensured that applications log all resource access using identifiers contained in certificates?	Stage 3	Yes
<b>Interagency Metrics</b>		
Has the ICAM SC and IFC WG developed guidelines and requirements for sharing network and application activity logs across the Secret Fabric to applicable agencies to support audit review?	Stage 3	Yes

**D.5 CAPABILITY: AUTOMATED ABAC BASED ON SUBJECT ATTRIBUTES, RESOURCE ATTRIBUTES, ENVIRONMENT ATTRIBUTES, AND DIGITAL POLICY RULES**

Metric	Stage	Target
--------	-------	--------

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency identified mechanisms for binding resource attributes to resources?	Stage 1	Yes
Has your agency governance bodies determined subject attributes that will be needed to support ABAC decisions based on the Catalog of Authorities?	Stage 2	Yes
Has your agency identified and established authoritative attribute stores for subject attributes?	Stage 2	Yes
Has your agency governance body determined environment attributes that will be needed to support ABAC decisions based on the Catalog of Authorities?	Stage 2	Yes
Has your agency developed attribute exchange services and linked them with agency attribute stores?	Stage 2	Yes
Has your agency tested attribute exchange service interfaces with Stage 1 prototype implementation to measure interoperability?	Stage 2	Yes
Has your agency governance body determined resource attributes that will be needed to link resources to applicable requirements based on the Catalog of Authorities?	Stage 2	Yes
Has your agency modified on-boarding/provisioning processes to include provisioning and maintenance of defined subject attributes for employees and affiliates?	Stage 3	Yes
Has your agency modified out-boarding and de-provisioning processes to include update and deletion of defined subject attributes for employees and affiliates?	Stage 3	Yes
Has your agency enabled high sensitivity applications to use authorization services for access control?	Stage 3	25%
	Stage 4	100%
Has your agency enabled medium sensitivity applications to use authorization services for access control?	Stage 4	Yes
Has your agency determined whether or not the values for attributes identified in Stage 2 exist in a format that supports migration to an existing attribute store for agency employees and affiliates?	Stage 3	Yes
For subject attributes that exist in a useable format, has your agency identified the authoritative source and developed processes and interfaces for making attribute values available to attribute exchange services?	Stage 3	Yes
For attributes that do not currently exist in a usable format, has your agency identified processes for determining and managing the values of the attribute for employees and affiliates and identify a mechanism for provisioning attribute values that will be available to attribute exchange services?	Stage 3	Yes
Has your agency identified attribute stores maintained by affiliates or alternative sources of affiliate attributes that rise to the authoritative level necessary to satisfy the FICAM trust framework?	Stage 4	Yes
Has your agency ensured that agency attribute exchange services have access to affiliate attribute stores?	Stage 4	Yes
Has your agency ensured that all attribute values used in digital policy rules are identified in the shared attribute map?	Stage 4	Yes

Metric	Stage	Target
Has your agency bound resource attributes to resources for resources which are intended to be shared? <sup>18</sup>	Stage 3	Yes
Has your agency ensured all applications that manage resources that are intended to be shared with other departments and agencies require certificate-based authentication of all authorized users?	Stage 3	Yes
Has your agency implemented authorization services that perform access control based on digital policies linked to resources and values of associated subject and environment attributes?	Stage 3	Yes
Has your agency identified environment attribute sources and established connections to attribute exchange services?	Stage 3	Yes
Has your agency populated attribute values for users of high sensitivity applications?	Stage 3	Yes
Has your agency completed the population of attribute values for employees and affiliates used in digital policy rules in authoritative data sources?	Stage 4	Yes
Has your agency ensured that attribute values for employees and affiliates used in digital policy rules are accessible via agency attribute exchange services?	Stage 4	Yes
Has your agency ensured that resource attributes are defined, validated, and bound to associated resources? <sup>19</sup>	Stage 4	Yes
Has your agency ensured that digital policy stores are fully populated with digital policy rules?	Stage 4	Yes
<b>Interagency Metrics</b>		
Has the ACAG WG and ICAM SC identified standards, interfaces, and models for sharing subject attribute information, including identifier, attribute name, and attribute value, and availability?	Stage 1	Yes
Has the ACAG WG and ICAM SC identified standards, interfaces, and models for registering and sharing resource attribute information including availability information?	Stage 1	Yes
Have the ACAG WG and ICAM SC identified standards, interfaces, and models for sharing environment attribute information, including identifier, attribute name, attribute value, and availability?	Stage 1	Yes
Has the ICAMSC Architecture Group established an attribute mapping capability that allows agencies to identify the location of subject attributes that are not locally managed?	Stage 3	Yes

#### D.6 CAPABILITY: SHARED DIGITAL POLICY RULES USED TO CONTROL ACCESS TO RESOURCES ACROSS THE SECRET FABRIC

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Has your agency, in coordination with the appropriate governance	Stage 1	Yes



Metric	Stage	Target
bodies, developed a Catalog of Authorities defining laws, policies, and other regulations that define requirements for controlling access to resources on the Secret Fabric?		
Has your agency identified an initial set of digital policies that will be used to govern access to resources intended to be shared across the Secret Fabric?	Stage 2	Yes
Has your agency developed specific digital policy rules governing access control to department or agency resources?	Stage 2	Yes
Has your agency enabled all applications that host resources intended to be shared to use authorization services for access control?	Stage 4	Yes
<b>Interagency Metrics</b>		
Have the ICAM SC and IdAM WG reviewed and approved the Catalog of Authorities?	Stage 2	Yes
Have the CNSS and the ICAM SC identified any gaps and overlaps in the Catalog of Authorities and developed an action plan to address them?	Stage 2	Yes
Has the ACAG WG identified digital policies that apply across the Secret Fabric (i.e., shared digital policies)?	Stage 2	Yes
Has OMB performed a compliance office review of the set of shared digital policies?	Stage 2	Yes
Have the ICAM SC and IdAM WG identified a set of common digital policy rules that apply across the Secret Fabric?	Stage 4	Yes

#### D.7 CAPABILITY: ABILITY TO EXCHANGE USER ACTIVITY RECORDS ACROSS THE SECRET FABRIC TO SUPPORT AUDIT LOG REVIEW AND INSIDER THREAT PROFILING

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
Does your agency ensure applications generate logs indicating the identifier used to authenticate to the system, the values of attributes used in the access control decision, and the source of those attribute values?	Stage 4	Yes
<b>Interagency Metrics</b>		
Has the ICAM SC and IFC WG developed guidelines and requirements for sharing network and application activity logs across the Secret Fabric to applicable agencies to support audit review?	Stage 3	Yes

#### D.8 SUPPORTING OR ENABLING ACTIVITIES – METRICS

Metric	Stage	Target
<b>Department or Agency Metrics</b>		
<b>Governance</b>		
Has your agency developed an implementation plan for implementing FICAM on the Secret Fabric within your agency based on this FICAM Planning Guidance for the Secret Fabric?	Stage 1	Yes
Has your agency established organizational (e.g., designated a Secret FICAM Implementation Program Office) and policy (e.g., authoritative body to govern ICAM on Secret Networks within your agency)	Stage 1	Yes

Metric	Stage	Target
requirements to implement your agency's implementation plan for FICAM on the Secret Fabric?		
Has your agency governance body incorporated the technology requirements for implementing FICAM capabilities into agency implementation plans?	Stage 2	Yes
Has your agency governance body included an ongoing process for evaluating further appropriate technological enhancements to improve agency alignment with FICAM capabilities?	Stage 2	Yes
Has your agency reviewed its organizational and policy requirements and modified them as required to support on-going maintenance activities for operating on the Secret Fabric?	Stage 3	Yes
Has your agency governance body defined governance processes to manage agency specific digital policies?	Stage 4	Yes
<b>Business</b>		
Has your agency integrated requirements for hardware and software upgrades needed to implement FICAM on the Secret Fabric into overall information technology acquisition planning and investment activities?	Stage 1	Yes
Has your agency incorporated budget guidance for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric?	Stage 1	Yes
Has your agency incorporated funding requirements for implementing FICAM on the Secret Fabric into annual budget submission to fund the implementation of FICAM on the Secret Fabric?	Stage 2	Yes
	Stage 3	Yes
	Stage 4	Yes
Has your agency implemented the first year of cost sharing for policy authority and access management?	Stage 3	Yes
<b>Interagency Metrics</b>		
<b>Policy</b>		
Has the SISS SC and/or ISA IPC developed interagency policy guidance to require adherence to FICAM Planning Guidance for the Secret Fabric?	Stage 1	Yes
Has the Architecture WG defined the level of required interoperability of Secret Fabric networks for information sharing and safeguarding and identified the interfaces necessary for departments and agencies to use Secret Fabric shared services (such as PKI or Identity Providers)?	Stage 1	Yes
Have the CNSS and ICAM SC published policy that requires departments and agencies to implement FICAM on the Secret Fabric and sets target dates for achieving implementation?	Stage 1	Yes
Have the CNSS and ICAM SC drafted new policies or proposed changes to existing policies to address identified policy gaps and overlaps?	Stage 2	Yes
Has the Architecture WG identified standards and protocols for performing authentication; obtaining subject, environment, and resource attributes; and applying digital policy rules to make access control decisions?	Stage 1	Yes
Have the PM-ISE and partnering agencies providers developed a prototype of attribute exchange capability on the Secret Fabric as a reference implementation for attribute sharing?	Stage 1	Yes

Metric	Stage	Target
Have the PM-ISE and partnering agencies implemented a prototype of authorization service which implements digital policy rules based on resource attributes and includes discovery and use of subject and environment attributes?	Stage 2	Yes
<b>Business</b>		
Have the SISS SC and/or ISA IPC identified a framework for individual agencies to manage the risk of trusting credentials and attribute values issued and managed by a third party and ensure it is consistent with their mission and with the overall Secret Fabric risk management governance and technical implementations?	Stage 1	Yes
Has the SISS SC and ISA IPC reviewed the trust model assumptions for management of attribute values for employees and affiliates for all subject attributes to ensure ability of all departments and agencies to accept attribute values from other departments and agencies?	Stage 3	Yes
Have the SISS SC and OMB coordinated and distributed budget guidance for implementing FICAM on the Secret Fabric?	Stage 1	Yes
Have the SISS SC and/or ISA IPC identified the cost model for participating agencies and shared service providers for the CSP?	Stage 1	Yes
Have the SISS SC and/or ISA IPC refined agency budget estimates based on implementation and maintenance costs defined in agency implementation plans?	Stage 2	Yes
	Stage 3	Yes
	Stage 4	Yes
Have the SISS SC and/or ISA IPC identified the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies that will rely on shared services?	Stage 2	Yes
Has the SISS SC, ISA IPC, and OMB reviewed and updated the on-going cost model for shared services, including budget language for agencies providing shared services and for agencies who will rely on shared services?	Stage 3	Yes
	Stage 4	Yes
<b>Governance</b>		
Has the ISA IPC established the IFC WG as the facilitator for coordination among the various identity federations that exist in the Federal Government on all classifications and between federal agencies and their affiliates?	Stage 1	Yes
Has the PKI MGB incorporated the activities of this planning guidance into their work plan, as appropriate?	Stage 1	Yes
Has the ICAM SC incorporated the activities of this planning guidance into their work plan, as appropriate?	Stage 1	Yes
Has the IdAM WG incorporated the activities of this planning guidance into their work plan, as appropriate?	Stage 1	Yes
Has the ACAG WG incorporated the activities of this planning guidance into their work plan, as appropriate?	Stage 1	Yes
Have the SISS SC and and/or ISA IPC designated a governance body responsible for assessing and addressing the overall risk management for FICAM on the Secret Fabric to enable departments and agencies to rely on attribute values asserted by other departments and agencies as part of access decisions?	Stage 1	Yes
Has the CNSS and ICAM SC reviewed the interagency governance	Stage 3	Yes

Metric	Stage	Target
structures, including working group charters, and modified them as required to support on-going maintenance activities for operating FICAM on the Secret Fabric?		
Has the ACAG WG identified and implemented processes for maintaining and updating identified subject, resource, and environment attributes?	Stage 4	Yes
Have the CNSS and ICAM SC defined governance processes to manage digital policies that apply to the full Secret Fabric?	Stage 4	Yes

## **APPENDIX E            COST MODEL TOOL FOR IMPLEMENTATION COSTS**

The embedded object contains the cost model tool for infrastructure costs.



FICAM Planning  
Guidance for the Secr

## **APPENDIX F            COST MODEL TOOL FOR AGENCY COSTS**

The embedded object contains the cost model tool for agency costs, which consists of a set of questions that will assist agencies in determining their cost estimate.



FiCAM Planning  
Guidance for the Secr

## APPENDIX G REFERENCES

Number	Title	Date
CNSSP 25	Committee on National Security Systems Policy Number 25, “National Policy for Public Key Infrastructure in National Security Systems” <a href="http://www.cnss.gov/Assets/pdf/CNSSP-25.pdf">http://www.cnss.gov/Assets/pdf/CNSSP-25.pdf</a>	March 2009
CNSSD 506	Committee on National Security Systems Directive Number 506, “National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks” <a href="http://www.cnss.gov/Assets/pdf/CNSSD-506.pdf">http://www.cnss.gov/Assets/pdf/CNSSD-506.pdf</a>	October 2012
E-Government Act	“E-Government Act of 2002”	December 2001
EO 13011	Executive Order 13011 “Federal Information Technology”	July 1996
EO 13231	Executive Order 13231 “Critical Infrastructure Protection in the Information Age”	October 2001
EO 13284	Executive Order 13284 “Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security”	January 2003
EO 13587	Executive Order 13587 “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” <a href="http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-">http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-</a>	October 2011
FICAM Roadmap	“Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance,” Version 2.0 <a href="http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf">http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf</a>	December 2011
Gap Analysis	CNSS Identity Management Working Group White Paper, “Gap Analysis Between the FICAM and U.S. Secret Networks”	May 2012
Gap Analysis Recommendations	CNSS Identity Management Working Group White Paper, “Recommendations for Implementing FICAM on U.S. Secret Networks”	January 2013
ICAM Lexicon	CNSS “NSS Identity, Credential and Access Management Lexicon, Version 0.5”	March 2011
IRTPA	“Intelligence Reform and Terrorism Prevention Act of 2004” <a href="http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf">http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf</a>	December 2004
NSD-42	National Security Directive (NSD)-42 “National Policy for the Security of National Security Telecommunications and Information Systems”	October 2001
NSISS	“National Strategy for Information Sharing and Safeguarding” <a href="http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf">http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf</a>	December 2012
OMB Cir A-11 85	OMB Circular No. A-11 Memorandum No. 85--August 2011 <a href="http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2011.pdf">http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a_11_2011.pdf</a>	August 2011
PM-ISE FY2013 Guidance	PM-ISE Memorandum, “FY2013 Implementation Guidance for the ISE”	August 2011
PPD-1	Presidential Policy Directive (PPD)-1, “Organization of the National	February 2009

Number	Title	Date
	Security Council System”	



## APPENDIX H                      ACRONYMS

ACAG	Access Control Attribute Governance
ASNI	Assured Secret Network Interoperability
BUS	Business (activity type)
CIO	Chief Information Officer
CISSO	Classified Information Sharing and Safeguarding Office
CNCI	Comprehensive National Cybersecurity Initiative
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CRED	Credentialing (activity type)
CSP	Common Service Provider
DISA	Defense Information Systems Agency
DoD	Department of Defense
DPOL	Digital Policy (activity type)
EATT	Environment Attribute (activity type)
ENAB	Enabling (activity type)
EO	Executive Order
FBI	Federal Bureau of Investigation
FICAM	Federal Identity, Credential, and Access Management
FOC	Full Operational Capability
FRAWG	FICAM Roadmap Alignment Working Group
GAO	Government Accountability Office
GOV	Governance Process (activity type)
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
IdAM	Identity and Access Management
IFC	Identity Federation Coordination
IISC	Information Integration Sub-Committee
INF	Infrastructure (cost element type)

IOC	Initial Operational Capability
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISIMC	Information Security and Identity Management Committee
KISSI	Key Information Sharing and Safeguarding Indicators
MGB	Member Governing Body
NSD	National Security Directive
NSISS	National Strategy for Information Sharing and Safeguarding
NSS	National Security Systems
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PM-ISE	Program Manager for the Information Sharing Environment
POL	Policy (activity type)
PMA	Program Management Authority
PPD	Presidential Policy Directive
RA	Registration Authority
RATT	Resource Attribute (activity type)
ROM	Rough Order of Magnitude
SATT	Subject Attribute (activity type)
SBU	Sensitive but Unclassified
SIPRNET	Secret Internet Protocol Router Networks
SISS SC	Senior Information Sharing and Safeguarding Steering Committee
TA	Trusted Agent
WG	Working Group