# Gap Analysis Between the FICAM and U.S. Secret Networks

**23 May 2012**

This page intentionally left blank.

# MESSAGE FROM THE CO-CHAIRS

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

This report represents a first step towards meeting these interoperability goals. To take the first steps forward, we need to first evaluate our current state. This report's analysis and high level recommendations will pave the way to a unified ICAM solution which will support information sharing and interoperability across Secret networks. In turn, the work done on the Federal Secret Fabric can serve as an example and a foundation for other networks outside of the NSS community.

We'd like to thank the Department of Defense (DoD), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Department of Homeland Security (DHS), Department of Justice (DOJ), and Department of State (DOS) for playing a key role in this analysis by participating in interviews to give a snapshot of their current Secret networks. In addition, we'd like to acknowledge DoD, FBI, DOJ, Program Manager for the Information Sharing Environment (PM-ISE), DOS, the Director of National Intelligence, National Aeronautics and Space Administration, National Security Agency, United States Department of Agriculture, and Department of Treasury for participating in the CNSS Identity and Access Management Working Group. With the increased emphasis on responsible information sharing and safeguarding of classified and sensitive information, the support and contributions of the PM-ISE and the Identity, Credential, and Access Management Subcommittee (ICAMSC) were invaluable in the development of this report and recommendations. The CNSS, in partnership with the ICAMSC and PM-ISE, has identified systemic gaps between the FICAM and the Federal Secret Fabric in this report and has engaged in a collaborative effort among the groups to develop recommendations for closing these gaps. Additionally, the CNSS plans to publish NSS policy, and will coordinate with the Federal CIO Council, the Office of Management and Budget (OMB), and the Information Sharing community to develop and publish any Federal-level policy and guidance necessary to facilitate the movement towards greater interoperability.

Deborah Gallagher
NSS IdAM WG Co-Chair

Arthur R. Friedman
NSS IdAM WG Co-Chair

**CNSS Secretariat (IE32) National Security Agency * 9800 Savage Road * Suite 6716 * Ft Meade MD 20755-6716**
**cnss@radium.ncsc.mil**

This page intentionally left blank.

# EXECUTIVE SUMMARY

Over the past ten years, the Federal Government has made concerted advances in the development and implementation of Identity, Credential, and Access Management (ICAM). This progress includes capabilities designed to promote interoperability, assured information sharing, and efficiencies of scale across all agencies within the Federal Government. Recently, several high-visibility events have focused attention on classified networks with a renewed emphasis on information protection within the information sharing paradigm. Organizations must strive to ensure responsible sharing and safeguarding of classified information by employing advanced capabilities that enable a common level of assurance in information handling and sharing while ensuring the interoperability required to satisfy mission requirements.

In response to these and other drivers, the National Security Systems (NSS)'s Identity and Access Management (IdAM) Working Group, the Federal Chief Information Officer (CIO) Council / ICAM Subcommittee (ICAMSC), and the National Security Staff / Information Sharing and Access (ISA) Interagency Policy Committee (IPC)'s Assured Secret Network Interoperability (ASNI) Working Group collaborated to evaluate the applicability of the Federal ICAM Roadmap and Implementation Plan (FICAM) to U.S. Secret networks and identify obstacles to the future interoperability of the Federal Secret Fabric. This document is based on analysis of the ICAM capabilities of six predominant Secret networks in use within the Federal Government:

- Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNet)
- Federal Bureau of Investigation (FBI) Network (FBINet)
- Department of Energy-National Nuclear Security Administration (DOE-NNSA) Enterprise Secure Network (ESN) *Note: This analysis focuses on the DOE-NNSA ESN. Other networks at DOE were not included in this data.*
- Department of Homeland Security (DHS) Homeland Secure Data Network (HSDN)
- Department of Justice (DOJ) Justice Consolidated Office Network - Secret (JCON-S)
- Department of State (DOS) ClassNet

| | DoD | DOS | DHS | DOJ | FBI | DOE |
|---|---|---|---|---|---|---|
| **Network Name** | Secret Internet Protocol Router Network (SIPRNet) | ClassNet | Homeland Secure Data Network (HSDN) | Justice Consolidated Office Network – Secret (JCON-S) | FBINet | National Nuclear Security Administration (NNSA) Enterprise Secure Network (ESN) |
| **Approximate # of Users** | >800,000 | 25,000 | 7,000 | 3,000 | 50,000 | 1,500 |
| **Purpose of Network** | Tactical and Command and Control | Share diplomatic mission and intelligence data in support of national interests, international law enforcement, and counter-terrorism | Share intelligence and mission data primarily for counter-terrorism | Share intelligence and mission data primarily for prosecution and counter-terrorism | Primary corporate business network (HR and mission functions) | Support compartmented data sharing |

This document represents a snapshot of the state of governance, policies, and implementation status of Secret networks as of December 12, 2011. There were several key findings as a result of this analysis:

- FICAM is applicable to Secret networks with some changes in the technical implementation to account for the unique requirements of classified networks
- The agencies evaluated have different levels of maturity in the implementation and realization of the FICAM vision, but all agencies recognize the need to move toward that vision
- Lack of authoritative policy and governance structures has led to divergent ICAM implementation approaches among many agencies
- Most agencies lack a common technical approach to ICAM implementation illustrated by the following:
    - Currently, there is no common and interoperable credential employed on Secret networks
    - There is no common way to capture, compile, and evaluate identity or resource attributes on Secret networks
    - There is no common end-to-end approach (people, process, technology) to interoperability and information sharing between agencies – information sharing successes are mostly limited to mission-specific systems to meet specific mission needs
- There are ICAM requirements unique to classified networks that are not currently addressed in FICAM (i.e., physical protection of end points, cross-domain data transfer, etc.)
- In partnership with the Secret network community, additional work is needed to identify a viable roadmap and implementation plan for FICAM on Secret networks including provisions for:
    - Developing Implementation Best Practices
    - Incorporating Security and Privacy Needs within the ICAM Enterprise Architecture
    - Aligning ICAM Architectures from multiple organizations, enclaves, and security domains

Together, the CNSS, ICAMSC, and the Program Manager for the Information Sharing Environment (PM-ISE) will continue to work to identify solutions to these obstacles and forge a path for implementation of robust and interoperable ICAM capabilities on the Federal Secret Fabric.

The CNSS, Information Security & Identity Management Committee (ISIMC), ICAMSC, and ASNI Working Group reviewed and approve the release of this document.

# Table of Contents

*Message from the Co-Chairs* ..... *iv*

*Executive Summary* ..... *vi*

*1 Introduction* ..... *1*

**1.1 Background** ..... **1**

**1.2 Purpose** ..... **4**

**1.3 Scope** ..... **4**

**1.4 Approach** ..... **4**

**1.5 Requirements Derived from FICAM** ..... **5**

**1.6 Assumptions** ..... **9**

**1.7 Document Organization** ..... **9**

*2 Analysis of Secret Network ICAM Capabilities* ..... *11*

**2.1 Governance and Policy Framework** ..... **13**
2.1.1 Gaps ..... 14
2.1.2 Impact ..... 15

**2.2 Identity Management** ..... **15**
2.2.1 Gaps ..... 16
2.2.2 Impact ..... 17

**2.3 Credential Management** ..... **17**
2.3.1 Gaps ..... 19
2.3.2 Impact ..... 19

**2.4 Access Management** ..... **20**
2.4.1 Gaps ..... 21
2.4.2 Impact ..... 22

**2.5 Audit and Reporting** ..... **22**
2.5.1 Gaps ..... 23
2.5.2 Impact ..... 23

**2.6 Federation** ..... **23**
2.6.1 Gaps ..... 24
2.6.2 Impact ..... 25

*3 Summary and Recommendations* ..... *27*

This page intentionally left blank.

# 1 INTRODUCTION

Identity, Credential, and Access Management (ICAM) is fundamental to information protection and information sharing. To achieve assured information sharing among federal organizations and their networks and systems, interoperable ICAM solutions are required. Interoperable solutions not only assure that information is protected, accessed, and manipulated in a predictable, policy-driven manner as it traverses networks, but they are also a means to achieve efficiencies through reuse of shared services. In a time of constrained resources and concurrent mandates to increase protections, a greater urgency exists to achieve efficiencies by developing interoperable, shared solutions.

Incidents such as the WikiLeaks disclosures have recently reinforced the need for improved, interoperable ICAM solutions for federal classified systems. Changes being contemplated for improving the security of classified networks and information are predicated on the availability of interoperable ICAM solutions, creating a sense of urgency to begin the complicated task of developing, coordinating, and implementing these solutions as soon as possible in support of the National Strategy for Trusted Identities in Cyberspace (NSTIC).[1]

This report represents a first step towards developing and implementing an interoperable ICAM solution for the Federal Secret Fabric to achieve efficient, assured information sharing. This report achieves this first step by researching the current state of ICAM capabilities on Secret networks, comparing existing deployments with emerging common solutions and identifying existing capability gaps. This report will be followed by an implementation plan outlining the incremental recommendations for interoperable ICAM capabilities for the Federal Secret Fabric that align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Plan (FICAM).

## 1.1 Background

The need for interoperable ICAM solutions is not new. However, a number of driving events have taken place recently which has increased momentum on this issue, both for Federal systems in general, and for Classified systems in particular.

In September 2008, the Federal Chief Information Officer (CIO) Council established the Information Security & Identity Management Committee (ISIMC). The ISIMC was charged with overseeing the government-wide activities related to Cybersecurity and Identity Management. In turn, the ISIMC established four subcommittees. The Identity, Credential and Access Management Subcommittee (ICAMSC) is tasked with aligning the Identity Management activities of government, while the remaining three deal with the cybersecurity tasking.[2] In 2009, the ICAMSC released version 1.0 of the

[1] "The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions." (http://www.nist.gov/nstic/about-nstic.html)

[2] Identity, Credential, and Access Management, http://www.idmanagement.gov/pages.cfm/page/ICAM, 3 October 2011.

FICAM to provide a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs.[3]

The Committee on National Security Systems (CNSS) was established by National Security Directive (NSD)-42 to set national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government (USG) departments and agencies for the security of National Security Systems (NSS) through the CNSS Issuance System.[4] In March 2009, the CNSS provided guidance that all Federal agencies deploy a Public Key Infrastructure (PKI) to manage and support Secret and Unclassified NSS.[5] In July 2009, the CNSS PKI Working Group (WG) transitioned to the CNSS PKI Member Governing Body (MGB). Under CNSS Policy 25, the CNSS PKI MGB was established to: 1) maintain and enhance the NSS-PKI hierarchy and its governing policies, and 2) develop additional policy guidance to address PKI interoperability with non-Federal partners and establishment of trust relationships among Certificate Authorities (CAs) participating in the NSS-PKI.

In 2010, the Information Sharing and Access (ISA) Interagency Policy Committee (IPC) formed the Assured Secret Network Interoperability (ASNI) Working Group. One of the chartering goals of this working group was to develop concurrence on a shared ICAM solution for the Federal Secret Fabric to support information sharing among federal partners and with non-federal mission partners including State and Major Urban Area Fusion Centers.[6]

Shortly after the 2010 CNSS Conference, the newly formed Identity and Access Management (IdAM) WG identified the need for a common lexicon and gap analysis report to be jointly created by the Federal CIO Council and the CNSS, with the Identity Credential and Access Management Subcommittee (ICAMSC) providing ICAM policy recommendations.[7] The FICAM lexicon was compiled using the FICAM Roadmap as the baseline and augmented by relevant issuances within the Federal ICAM community. The lexicon was endorsed by the ICAMSC and the ISIMC member organizations and forwarded to the CNSS Glossary Working Group for adoption.[8]

On March 10, 2011, the Senate Select Committee on Intelligence held a hearing entitled, *Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration*. The hearing included senior executives from Department of Defense (DoD), Department of State (DOS), Office of the Director of National Intelligence (ODNI), and Program Manager (PM)-Information Sharing Environment (ISE). During this hearing, the Chief Information Officer of the Department of Defense addressed the ongoing need to both improve intra-governmental information sharing and access control:

> *Increased emphasis on user authentication, data tagging, development of user attributes, and implementation of advanced technologies such as Cloud implementations, consolidated*

[3] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, 10 November 2009.

[4] http://www.cnss.gov/history.html

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

[6] ASNI Working Group Charter; 17 November 2010.

[7] CNSS Conference 2010 Final Report.

[8] CNSS NSS Identity, Credential and Access Management Lexicon, Version 0.5, 24 March 2011.

> *discovery, and single-sign on will provide the foundational technology that will continue to improve sharing and data discovery while bringing protection up to the same level.*[9]

Additionally, during the same hearing, the Program Manager for the Information Sharing Environment (PM-ISE) stated:

> *We have several different identity management frameworks across the scope of federal government or state and local partners and so forth. Those frameworks are mostly aligned. But we need to make sure that as they get implemented, they're implemented in a way that's consistent across all the different partners. If that doesn't happen, then, you run into challenges when information moves across organizational boundaries.*[10]

On August 3, 2011, the Office of Management and Budget (OMB) issued its FY13 Programmatic Guidance outlining the resource priorities and policies for all executive branch departments and agencies. As a companion document the PM-ISE issued FY13 Implementation Guidance for the ISE. In this memorandum, ISE departments and agencies are directed to:

- *By **30 September 2013**, program funds to align Secret network identity management solutions to the Federal Identity, Credential, and Access Management (FICAM) Framework, such that these identity management solutions are interoperable among Secret networks and across security domains.*
- *By **30 September 2013**, establish and implement Committee on National Security Systems (CNSS) Policy 25, or an interoperable identity management solution, for individual networks and enclaves that access or transit SIPRNet.* [11]

Finally, as the culmination of the federal government's response to the WikiLeaks disclosures, Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, was published on October 7, 2011. This new executive order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks including the coordinated interagency development and reliable implementation of policies and minimum standards. Pointing to recent events as the driver for near-term action, the executive order highlights the partnership among the Federal CIO Council / ISIMC's ICAM Subcommittee, the National Security Staff / ISA IPC's Assured Secret Network Interoperability (ASNI) Working Group, and CNSS's Identity and Access Management (IdAM) Working Group as the mechanism for developing and implementing *a holistic solution for efficient, interoperable ICAM for the Federal Secret Fabric.*[12] This gap analysis represents the first in a series of steps these three organizations intend to pursue in response to EO 13587.

---

[9] Congressional Testimony; Teresa Takai; "Information Sharing in the Era of Wikileaks: Balancing Security and Collaboration"; 10 March 2011.

[10] Congressional Testimony; Kshemendra Paul; "Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"; 10 March 2011.

[11] PM-ISE Memorandum: FY2013 Implementation Guidance for the ISE; 4 August 2011.

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

## 1.2 Purpose

The purpose of this document is to compare the guidance found in the FICAM Roadmap and Implementation Plan with the current and envisioned future state of ICAM capabilities for U.S. Secret networks, and to determine applicability for implementing FICAM on these networks. This comparison outlines:

1) Gaps in the current implementation of the FICAM on the Secret networks, and
2) Gaps in the FICAM where it may not meet the specific needs of classified environments.

## 1.3 Scope

Interoperable ICAM solutions are critical to achieving assured information sharing for networks and systems at all classification levels, and are critical to support future assured sharing capabilities between security domains (i.e., cross domain solutions).

As illustrated in Figure 1, this gap analysis limits its focus to ICAM capabilities on network systems operating at the Secret classification level. There are several major Secret networks operated by federal departments and agencies, and a larger number of smaller Secret networks which are isolated and not connected to other networks. This gap analysis focuses on the interconnected networks for which information sharing represents a critical capability, comprising a Federal Secret inter-network or "Federal Secret Fabric". This document represents a snapshot of the state of governance, policies, and implementation status of Secret networks as of December 12, 2011. Conclusions regarding interoperability and FICAM implementation on Secret networks are based on information gathered on several of these networks, specifically on the following networks:

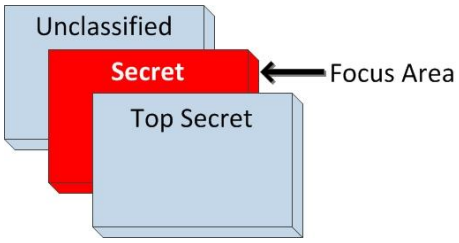


**Figure 1: Analysis Focus – ICAM Gaps in Secret Networks**

- DoD Secret Internet Protocol Router Network (SIPRnet)
- Federal Bureau of Investigation Network (FBINet)
- Department of Energy-National Nuclear Security Administration (DOE-NNSA) Enterprise Secure Network (ESN) *Note: This analysis focuses on the DOE-NNSA ESN. Other networks at DOE were not included in this data.*
- Department of Homeland Security (DHS) Homeland Secure Data Network (HSDN)
- Department of Justice (DOJ) Justice Consolidated Office Network - Secret (JCON-S)
- Department of State (DOS) ClassNet

## 1.4 Approach

The approach used for conducting the gap analysis was to derive requirements from the FICAM use cases and use these requirements as the foundation for a comparative analysis of ICAM capabilities on Secret networks. These requirements were used to conduct interviews with agency leaders and technical experts to explore the current state and future plans of the different ICAM functional areas. Discussions with agency representatives focused on their specific implementation of digital identity lifecycle management and attribute exchange, credentialing, authentication, authorization and access, privilege management, and general governance and business processes used to manage these capabilities. The results of the interviews were compared and analyzed against the FICAM requirements. Where gaps in

capability or obstacles to future interoperability existed, they were noted and examined. The requirements derived from the FICAM document are explained further in the next section.

## 1.5 Requirements Derived from FICAM

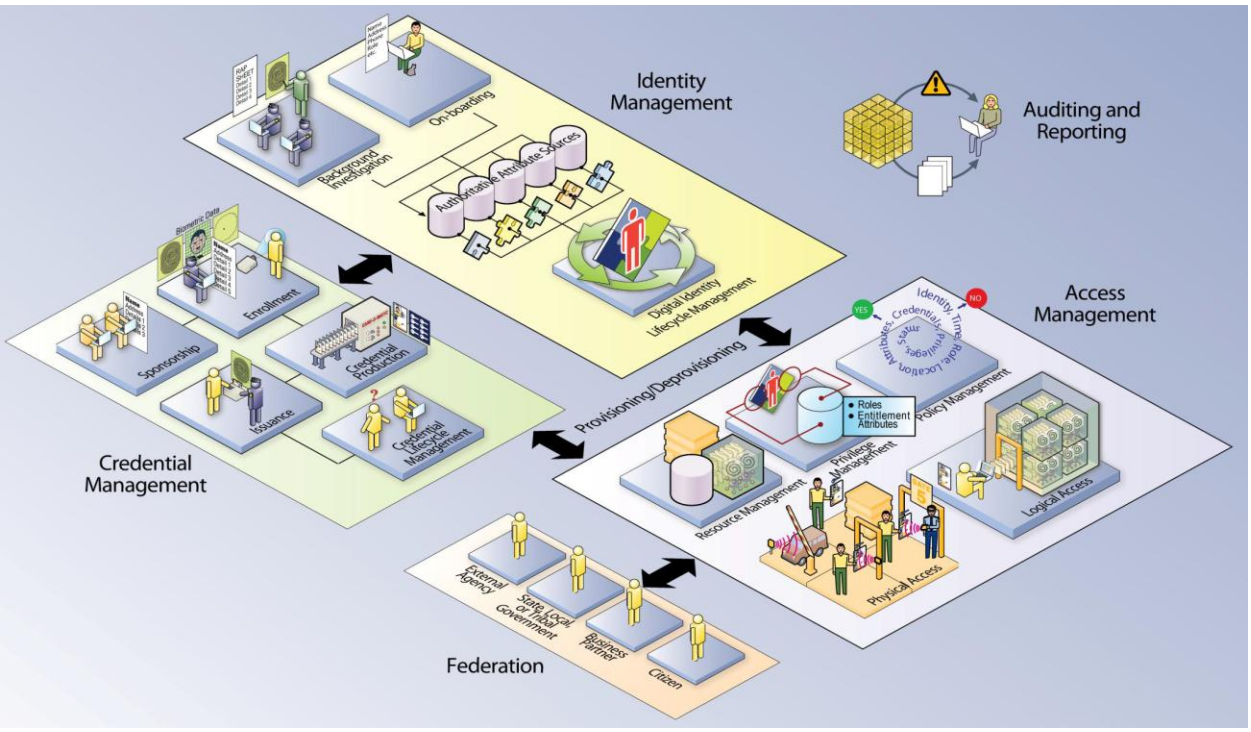


**Figure 2 - ICAM Conceptual Diagram**

The first release of the FICAM Roadmap and Implementation Plan Part A was published in November of 2009. The conceptual framework diagram shown in Figure 2 is from FICAM Part A and provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stove-pipes can intersect to provide an enterprise capability. This high-level view of ICAM depicts the interdependencies between each area, the combination of which creates an enterprise solution. Behind the deployed technology and the solutions are the governance and policies needed for solutions to be successful from a business and security perspective. The following is a brief summary of the salient requirements derived from FICAM, broken out by the five areas illustrated in the conceptual framework. The first three of these: Identity Management, Credential Management, and Access Management provide the key services and processes that are necessary for a functional system. Audit and reporting are supporting services, and federation provides additional functionality necessary for sharing information among different networks. While this section attempts to condense and summarize much of the content in the FICAM, the complete FICAM should be referred to for more detail and a comprehensive description.

**Identity Management**

The FICAM offers an approach to identity management wherein creation and management of digital identity records are shifted from stove-piped applications to an authoritative enterprise view of identity that enables application or mission-specific uses without creating redundant, distributed sources that are harder to protect and keep current. Unlike accounts to logon to networks, systems or applications, enterprise identity records are not tied to job title, job duties, location, or whether access is needed to a specific system. Those things may become attributes tied to an enterprise identity record, and may also become part of what uniquely identifies an individual in a specific application. Access control decisions will be based on the context and relevant attributes of a user—not solely their identity. The concept of an enterprise identity is that individuals will have a digital representation of themselves which can be leveraged across departments and agencies for multiple purposes, including access control. Users and their digital identities from external organizations should be provisioned using data from their source organization to reduce duplicative data collection. As part of the framework for establishing a digital identity, proper diligence should be employed to limit data stored in each system to the minimum set of attributes required to define the unique digital identity and still meet the requirements of integrated systems. A balance is needed between information stored in systems, information made available to internal and external systems, and the privacy of individuals.

Establishment of a digital identity, also commonly referred to as a persona, typically begins with collecting identity data as part of an on-boarding process, unfortunately most of the data for individuals is stored on unclassified systems and is not readily available on the Secret Fabric. There is a minimum requirement for a Secret clearance to access the Secret Fabric and vetting data such as background and clearance information should come from existing sources [for example, Office of Personnel Management's (OPM's) Central Verification System (CVS) and the DoD's Contractor Verification System (CVS)], and where practical should be tied to biometric attributes such as fingerprints and made available on the Secret Fabric.

**Credential Management**

A key distinction in the lifecycle management of credentials versus identities is that credentials expire. The attributes which form a digital identity may change or evolve over time, but an identity does not become invalid or terminated from a system perspective. Credentials however are usually valid for a pre-defined period of time. Another key aspect of credential management is the security and protection of credentials, from the issuance to use and finally destruction of credentials. The trust in a credential is dependent on a multi-layered approach to security that protects the credential from attack as well as who can use the credential. ICAM hinges on the level of trust in a credential and the uniformity of security and integrity across the security architecture to retain that trust throughout the use of the credential. The FICAM envisions the use of a single interoperable credential such as the Personal Identity Verification

(PIV) for both physical and logical access to resources within an organization as well as for access to resources within partner organizations; thus reducing the number of credentials issued for each user. The credential should support securing document communication as well as signing and encryption of emails. Where possible, applications should be public key enabled (PK-Enabled) to accept the common credential. Public key enablement is the process of configuring or customizing an application, or enabling a proxy, to use public key certificates for authentication confidentiality, data integrity, and non-repudiation within individual applications.[13] The credential should be created, issued, and maintained following the guidance in FIPS 201.[14] The reduction of username and password credential types is one of the primary focuses of the FICAM. The FICAM also supports a common approach for issuing and accepting a Facility Access Card (FAC) credential for temporary users.

While the PIV and PIV-Interoperable (PIV-I) are strictly intended for use on unclassified networks, CNSSP 25 makes provisions for a smartcard credential to be used on the Secret Fabric. This credential should have the same protections as defined for the PIV and PIV-I.

### Access Management

Access management is the management and control of the ways in which entities are granted access to resources. A key aspect of access management is the ability to leverage an enterprise identity for entitlements, privileges, multi-factor authentication, roles, attributes and different levels of trust. Logical

*FICAM Explained*

*Key Concepts…*

In 2008, the Federal Information Security and Identity Management Committee (ISIMC), at the request of the Federal CIO Council, created the Identity Credential and Access Management Subcommittee (ICAMSC) to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. The Federal ICAMSC combines the intersection of digital identities (and associated attributes), credentials (including PKI, PIV, and other authentication tokens), and access control into one comprehensive management approach.

The FICAM Roadmap and Implementation Guidance provides a common framework for ICAM capabilities on Unclassified networks within the Federal Government. The Roadmap addresses Unclassified federal identity, credential, and access management programs and how the Executive Branch of the Federal Government will interact with external organizations and individuals. It was written to assist the Federal enterprise in leveraging and building a digital infrastructure to securely conduct business electronically between Federal agencies, their business and coalition partners, and with the American public, by promoting the use of authentication, digital signature, and encryption technologies. To build a successful ICAM architecture, the FICAM Roadmap addresses seven key ICAM Service areas that must be address: Digital Identity, Credentialing, Privilege Management, Authentication, Authorization and Access, Cryptography, Auditing and Reporting.

The FICAM Roadmap includes use-cases to outline the components of the ICAM segment architecture within the business functions that they support. Each use case describes a series of actions taking place, the actors involved, the data being exchanged and the systems, applications, technology and standards being leveraged. The document has been developed in two phases. The first phase was completed in November 2009 and focused on the development of the common, government-wide ICAM segment architecture. The Phase 2 draft was published in May 2011 and builds on Phase 1 to include the documentation of ICAM best practices and implementation guidance.

[13] Derived from PK-Enabling definition in CNSS NSS Identity, Credential and Access Management Lexicon, Version 0.5, 24 March 2011.

[14] 14.FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors; March 2006.

and physical access are often viewed as the most significant parts of ICAM from a return on investment perspective. To maximize that return, a successful access management solution is dependent on identity, credentials, and attributes for making informed access control decisions, preferably through automated mechanisms. The FICAM envisions an access control mechanism using authorization attributes tied to the user. Users on the Secret Fabric should be able to authenticate themselves for logical access control utilizing a smartcard credential. Although authentication is an important step in the process, it does not imply access by default. Applications should reach to authoritative attribute sources when making access control decisions. Physical and logical access should be enabled using a common smartcard. Agencies should ensure that access management is performed consistently throughout an agency by following authoritative enterprise standards. In addition, access control sets the stage for additional activities outside of the traditional access control paradigm. One corollary to access management is the ability to ensure that all individuals attempting access have a genuine need. This determination is tied to authentication and authorization, but also to the business rules surrounding the data.

### Auditing and Reporting

The FICAM goal for auditing and reporting addresses the review and examination of records and activities to assess adequacy of system controls and the presentation of logged data in a meaningful context. Solutions adopted as part of federal ICAM initiatives will provide robust auditing capabilities to support accountability, provide discrete non-repudiation, and enhance transparency in security effectiveness.

This capability needs to support addressing the insider threat problem as well as day-to-day analysis of system activities and performance tuning. The auditing, monitoring, and reporting capabilities are the foundation of establishing and maintaining the trust required for the Federation.

### Federation

Identity federation, commonly referred to simply as federation, is a term used to describe the governance, policies, agreements, standards, and ultimately processes and technologies that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization. Federation is made possible through the establishment and use of common exchange protocols and agreed-upon open standards/specifications that allow an agency to authenticate a user from another organization or trust an authentication conducted outside of the agency. The use of these common rules enables an agency to place a level of trust in the federated identity and credential to which that identity is bound. Within the Federal Government, the business need to federate with a non-federal partner is driven primarily by each agency's mission. Agencies with missions that involve significant collaboration with non-federal organizations or provide a large number of citizen-focused services will likely be the largest consumers of federated identity data. Each agency should evaluate its cross-organizational collaboration and information sharing needs to determine the need for implementing federation capabilities within the agency.

The vast majority of federation transactions that occur within the Federal Government can be grouped into two categories, namely: Interagency federation and federation with entities external to the Federal Government. Even on the Secret Fabric there will be federation with external partners, which includes federation that occurs between a federal agency and any other non-federal organization or entity (e.g., state, local, or tribal governments, and commercial entities).

## 1.6 Assumptions

Several assumptions guided the analysis employed in this document:

- The goals of the Federal Government are:
  - ICAM interoperability for the purpose of efficiencies of scale and information sharing on Secret networks and among its applications while maintaining effective mission-oriented operational security
  - ICAM interoperability among security domains to support assured information sharing, efficiency, and critical capabilities such as audit data sharing
  - Assured information sharing to support mission needs
- The FICAM Roadmap is a comprehensive framework approved by departments and agencies and the White House; as such, FICAM may be the appropriate basis for ICAM policies on all fabrics and security domains
- Gaps are where:
  - Agencies do not meet the FICAM end-state vision
  - Agencies differ in ICAM implementation such that those implementations are not interoperable
  - Requirements for classified networks are divergent from FICAM
  - Secret networks have ICAM requirements that are not addressed in FICAM
- Other observed obstacles to interoperability and information sharing not specifically called out in FICAM or in ICAM guidance for classified networks may be identified as gaps
- Agencies were viewed in the context of current capabilities and the trajectory of planned capabilities and how well that aligned with the FICAM end-state vision
- This report is meant to be non-attributional and comments on the overall state of the collective agencies evaluated
- This report is not comprehensive, but limited in scope of findings to the agencies interviewed and the networks those agencies manage
- The data obtained in this report is only as accurate as the knowledge of the individuals interviewed and should not be considered authoritative for any specific agency

## 1.7 Document Organization

The remainder of this document is organized as follows:

- Section 2 describes the current state of the Secret networks examined during this analysis
  - 2.1 Governance and Policy Framework – Discusses the current state of policies and governance as they pertain to Secret networks
    - 2.1.1 – Identifies gaps in the current state of governance including the lack of policy framework and clearly defined governing bodies
    - 2.1.2 – Describes the impact of the governance and policy gaps and what that means as Secret networks move towards the target state
  - 2.2 – Identity Management – Defines identity and the current state of creating and maintaining identities for Secret network access
    - 2.2.1 – Identifies gaps in identity management on Secret networks including lack of common framework and repositories

        - 2.2.2 - Describes the impact of those identity management gaps and how they may affect Secret networks moving forward
    - 2.3 – Credential Management – Discusses the credentials most often used on Secret network
        - 2.3.1 – Identifies the current gaps in credential management including the unsuitability of PIV for Classified environments and the lack of a standard interoperable credential at this time
        - 2.3.2 – Describes the impact of the current state including the gaps and how that will affect implementing the FICAM
    - 2.4 – Access Management – Describes the challenges relating to access management on Secret networks
        - 2.4.1 – Identifies the gaps in access management including lack of uniform implementation in general, in data tagging and in PK-enabling applications
        - 2.4.2 – Describes the impact of the current gaps and how the FICAM target state could be affected by them
    - 2.5 – Audit and Reporting – Defines audit and reporting functions and how Secret networks currently approach that functionality
        - 2.5.1 – Identifies gaps in audit and reporting as it relates to information sharing and creating efficiencies across Secret networks
        - 2.5.2 – Describes the impact of the current gaps and how the FICAM target state could be affected by them
    - 2.6 Federation – Discusses the evolution of information sharing and how agencies currently approach sharing information across organizational boundaries
        - 2.6.1 – Defines the current gaps impeding federation across Secret networks including lack of robust transfer and interoperability capabilities
        - 2.6.2 – Identifies the impact of these gaps on creating a federated environment for Secret networks
- Section 3 summarizes the findings presented in the document
- Appendix A – Defines acronyms used in the document
- Appendix B – Lists references used in the document

# 2 ANALYSIS OF SECRET NETWORK ICAM CAPABILITIES

Secret networks were originally created to support specific mission needs and access was controlled essentially by group membership. In many cases there was an assumption that everyone with network access had a need to know all information stored on the network, so access control did not extend beyond access to the network itself.

As operational requirements developed, the number of users increased and Secret networks began to connect to one another and to Unclassified and higher classified networks. These connections operated with strict technical and procedural controls designed to prevent the transfer of information with higher classification to networks of lower classification, and to prevent the transfer of viruses or other malware from networks of lower classification to networks of higher classification.

The term "Federal Secret Fabric" evokes the image of a cohesive, interconnected, and meshed network infrastructure across the Federal Government designed to seamlessly and simultaneously share and protect classified information at the Secret level. The actual state of the U.S. Secret networks is different from what the term suggests. While most Secret networks were derived from specific mission needs of the agencies and organizations in which they evolved, others were established or consolidated in response to the need to share information so prominently highlighted in the 9/11 Commission Report.[15] These Secret networks were established or consolidated to meet the mandates set forth in Homeland Security Presidential Directive-20 (HSPD-20)[16] and National Communications System Directive 3-10 (NCSD 3-10)[17] which drove the need for continuity of operations (COOP), continuity of government (COG), and seamless communication – voice and data – at all levels of classification.

The result is a patchwork of networks, unique to each agency, the majority of which were not designed to be interoperable. Yet, given this disparity, each network seems to meet the internal needs of its owning agency, while managing to support inter-network information sharing when required by the mission. As more attention is paid to implementing ICAM capabilities and designing rigor

*Secret Networks Evolved Differently – Focused on Varying Missions*

*For Example…*

The DOE NNSA's Enterprise Secure Network is designed to provide enterprise security and compartmented data sharing services to less than 1,500 users in dozens of nuclear research facilities across the country. Meanwhile, the DoD's SIPRNet is the primary tactical and Command and Control Network for the DoD – with over 800,000 users around the world.

[15] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States; http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

[16] HSPD-20: National Continuity Policy ; 4 May 2007.

[17] NCSD 3-10: Minimum Requirements for Continuity Communications Capabilities; 10 August 2000.

into Unclassified networks, agencies are slowly starting to plan and pursue similar thinking for their Secret networks.

This section summarizes the analysis of the ICAM capabilities of six predominant Secret networks in use within the Federal Government: DoD – SIPRNet, FBI – FBINet, DOE NNSA – ESN, DHS – HSDN, DOJ – JCON-S, and DOS – ClassNet. It identifies policy and technical challenges to the implementation of the guidance in the FICAM Implementation Plan and Roadmap (FICAM) on Secret networks as well as challenges to the future interoperability of the Federal Secret Fabric.

Table 1 summarizes the networks analyzed.

**Table 1: Agencies Evaluated for Secret Network ICAM Analysis**

| | DoD | DOS | DHS | DOJ | FBI | DOE[18] |
|---|---|---|---|---|---|---|
| **Network Name** | Secret Internet Protocol Router Network (SIPRNet) | ClassNet | Homeland Secure Data Network (HSDN) | Justice Consolidated Office Network – Secret (JCON-S) | FBINet | National Nuclear Security Administration (NNSA) Enterprise Secure Network (ESN) |
| **Approximate # of Users** | >800,000 | 25,000 | 7,000 | 3,000 | 50,000 | 1,500 |
| **Purpose of Network** | Tactical and Command and Control | Share diplomatic mission and intelligence data in support of nation interests, international law enforcement, and counter-terrorism | Share intelligence and mission data primarily for counter-terrorism | Share intelligence and mission data primarily for prosecution and counter-terrorism | Primary corporate business network (HR and mission functions) | Support compartmented data sharing |
| **Info Sharing Needs** | DOJ, DHS, DOE, FBI, DOS, Foreign and coalition partners, industry partners, IC | DoD, DHS, DOJ, FBI | DoD, DOS, state and local government | DoD, FBI, local law enforcement | DoD, DOJ, DHS, IC | DoD |
| **Authentication** | Username and Password; currently piloting PKI Smartcard | Username and Password, Hardware PKI Smartcard pilot | Username and Password | Username and Password | Hardware PKI Smartcard (optional); Username and Password | Username and Password, RSA OTP Token |
| **Access Control** | Access Control List (ACL) | ACL | ACL, Limited RBAC | ACL | ACL, Limited ABAC | ACL, Limited ABAC |

**Note: Information in this table is derived from agency expert interviews and not independently validated.*

[18] This analysis focuses on the DOE-NNSA ESN. Other networks at DOE were not included in this data.

## 2.1 Governance and Policy Framework

The Federal Secret Fabric lacks comprehensive policies for ICAM functions, clear mandates for use, and the recognized means to govern this function to achieve federal-wide interoperability. A number of multi-agency ICAM policy frameworks exist throughout the federal government with varying mandates for use. The FICAM Roadmap, which was developed for unclassified systems and whose use is mandated by OMB M-11-11,[19] is one of these frameworks. The Intelligence Community (IC) IdAM Framework is evolving, which is intended to be applied to all IC systems across all security domains, the use of which will be mandated in IC-wide policy. The National Institute of Standards and Technology (NIST) also developed the NIST SP 800-53 Federal Public Key Infrastructure (FPKI) Security Controls Profile[20] to list the controls and enhancements required for Federal PKI systems and their evaluations as well as the corresponding Assessment Guide[21] to provide guidance for evaluating a PKI system against those controls. Finally, CNSS has developed several ICAM- related policies for use on National Security Systems, including CNSSP 25,[22] CNSSI 1300,[23] CNSSI 1253,[24] and a lexicon for ICAM terminology using CNSSI 4009[25] as a reference.

For the Federal Secret Fabric, these multi-agency ICAM policy frameworks overlap in some instances, and are duplicative in others. Additionally, gaps exist in these ICAM policy frameworks such that no framework provides a comprehensive set of policies and standards that can produce fully implemented interoperable ICAM for all U.S. Secret networks.

Commensurate with the gaps and overlaps in the various multi-agency ICAM policy frameworks is a lack of comprehensive governance related to ICAM for the Federal Secret Fabric. No single authoritative ICAM governance and mandate for use on Secret networks exists among the Intelligence, Defense, and civilian communities. Additionally, because ICAM is both a sharing and a security capability, existing governance for ICAM on Secret networks is divided between CNSS for security functions and the ISA IPC's ASNI Working Group for sharing functions.

Implementation Guidance for the FY2013 Programmatic Guidance for the Information Sharing Environment[26] directs federal agencies operating Secret networks to program funds to implement the FICAM Framework on Secret networks, and directs use of a PKI solution described in CNSSP 25, or an interoperable solution, for operators of Secret networks by September 30, 2013. This represents the first time federal-wide guidance for Secret networks has been issued. This guidance was further clarified by

[19] OMB M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors (03 FEB 2011).

[20] NIST SP 800-53 FPKI Security Controls Profile: Federal Public Key Infrastructure Security Controls Profile of Special Publication 800-53; 9 February 2011.

[21] NIST SP 800-53A FPKI Security Controls Profile: Assessment Guidance for Security Controls in PKI Systems; 9 February 2011.

[22] CNSSP 25: National Policy for Public Key Infrastructure for National Security Systems.

[23] CNSSI 1300: National Instruction on PKI X.509 Certificate Policy.

[24] CNSSI 1253: Security Categorization and Control Selection for National Security Systems.

[25] CNSSI 4009: National Information Assurance Glossary, April 2010.

[26] PM-ISE Memorandum: FY2013 Implementation Guidance for the ISE; 4 August 2011.

OMB in November, 2011. Additionally, the promulgation of EO 13587, with its focus on both sharing and safeguarding, may provide a path towards comprehensive ICAM governance for the Federal Secret Fabric in the context of a comprehensive solution for governance on classified networks.

### 2.1.1 Gaps

**Policy frameworks for ICAM, interoperability, and information sharing on U.S. Secret networks are incomplete.**

As noted above, none of the existing ICAM policy frameworks provide a complete set of policies covering all aspects of ICAM that, when implemented, will result in an interoperable ICAM solution for U.S. Secret networks that achieves both sharing and safeguarding. In addition to the lack of a complete ICAM policy framework, the Federal Secret Fabric lacks a common policy framework covering all networks across all communities. A common - or at a minimum, interoperable - policy framework is needed to ensure interoperability and information sharing, commonly understood security controls, and access management.

*Moving in the Right Direction…*

DHS established an executive-level working group to determine the strategy and an implementation plan for ICAM capabilities on their Secret network, HSDN. While advisory and collaborative in nature, this working group's recommendations will be endorsed at the Deputy Secretary level and worked into the acquisition planning process for the Department.

**There is no clearly understood and authoritative interagency body to govern ICAM on Secret networks.**

Along with the overarching lack of a clear governance body for the Federal Secret Fabric, no comprehensive interagency ICAM governance body exists that can address both security and sharing. Additionally, departments and agencies frequently lack an enterprise governance function that coordinates ICAM issues for classified networks.

### 2.1.2 Impact

There are several impacts resulting from the gaps in policy and governance for ICAM functions on Secret networks. First and foremost, a lack of common policies and standards for ICAM on Secret networks all but guarantees a lack of reciprocity and interoperability, which in turn impedes information sharing and mission fulfillment. Second, the lack of a clear federal mandate for use of a common ICAM solution for federal Secret networks, including a timeframe for implementation, results in an inability for departments and agencies to budget for an ICAM solution. The inability to plan resources for an ICAM solution delays improving this critical aspect of information assurance, and increases risk that departments and agencies will fund non-standard solutions for Secret networks. Finally, the lack of overall ICAM governance for Secret networks means that no forum exists in which to discuss and resolve interagency issues to support interoperability, shared services and efficiency, and shared risk management.

## 2.2 Identity Management

As noted in the FICAM, the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management defines identity management as the combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information.[27] The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual. Identity management includes the processes for maintaining and protecting the identity data of an individual over its lifecycle. Additionally, many of the processes and technologies used to manage a person‘s identity may also be applied to Non-Person Entities (NPEs) to further security goals within the enterprise.

The DoD/IC Authorization and Attribute Services Committee (AASC)[28] is focused on promoting a common, standardized approach to achieving federated authorization and access control that spans the various network infrastructures. To achieve federation across the DoD and IC, there has been a thrust to capture attributes for a non-person for access control. The IC, with endorsement from the AASC, has established NPE goals and is developing an NPE model to ensure solutions are security domain agnostic, can be transportable across many technologies and capabilities, and are fully aligned across the DoD and the Federal Government.

Agency requirements for enrollment are similar, but executed with varying processes and formats. A typical process involves a standardized form for data collection that feeds into a central database on an Unclassified network. Some agencies connect to external authoritative attribute stores to populate user attributes at the time the account is provisioned, but the majority populates the desired attributes based on data collected from the enrollment form. Obtaining an account on a Secret level network generally requires holding either a Secret clearance granted by a U.S. Agency or a clearance granted by a U.S. allied or coalition partner that has been determined to be comparable to a U.S. Secret clearance. Clearance information is collected at the time of enrollment and vetted with the appropriate data source.

---

[27] National Science and Technology Council (NSTC) Archives; Identity Management Task Force Report 2008; http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-identitymgmt-2008.pdf; 3 October 2011.

[28] Strategic Letter of Intent Between the Department of Defense Chief Information Officer and the Associate Director of National Intelligence and Chief Information Officer; http://cio-nii.defense.gov/docs/DoDAASI.pdf ;21 April 2008.

*Moving in the Right Direction…*

The FBI utilizes external authoritative attributes for the population of user attributes during the provisioning process. These attributes are populated into a local authoritative attribute store on the target domain that is used by other applications within the network – rather than populated on an unclassified network and replicated to the Secret network. These attributes are used by some applications for attribute based access control. Rather than maintaining multiple attribute stores many of the applications utilize the enterprise attribute store. These attribute are controlled through a change management process to evaluate the need for the attribute and the approved attribute values.

The majority of Secret networks have at least one user account for network logon and additional application specific accounts used to log in to other network resources. There are some applications that are linked to the user directory for network logon, but the majority maintains an application specific user database.

Identity management capabilities on Secret networks are largely disparate. Each agency follows its own set of processes and, because of the diverse methods of authentication and access control within each network, has varying requirements for account provisioning and capturing identity attributes. The only exceptions are the entry criteria for account provisioning where validation of Secret clearance and need-to-know is uniformly performed. Few agencies employ automated solutions for account request and provisioning and most process steps are manually performed. Identity attributes are populated at account provisioning but few agencies allow attributes to be automatically pulled from authoritative sources like Human Resources (HR) records. For most agencies, the attributes collected are primarily white-pages type information like role, supervisor, organization and phone number, rather than access control attributes.

### 2.2.1 Gaps

**Agencies lack a common digital identity and identity attribute framework for Secret networks.**

The attributes captured during enrollment are not standard and not captured in a standard format to include definition of unique identifiers. Identity attributes do not have standard schemas or standard attribute value sets across the Federal Government or standard approaches to attribute usage, quality of data, etc. Secret network digital identities are created and managed differently by each agency. Within each agency, these digital identities are also managed differently from the way Unclassified digital identities are managed on their Unclassified networks. Enrollment and account provisioning is performed differently by each agency. Historically, these approaches have been sufficient to meet mission requirements. However, to advance information sharing and interoperability between agencies, greater consistency in these processes is needed.

*For Example…*

An agency with a relatively small user base manually populates a rudimentary set of attributes upon digital identity creation. Given that authentication and access control to the network and enterprise applications is enabled through simple username and password credentials, there is no need to populate or maintain an extensive set of attributes. On the other end of the spectrum, another agency with a relatively large user base uses an integrated identity attribute management capability that automatically populates identity attributes from the authoritative Unclassified HR database to an authoritative database on the Secret network. These attributes are available to applications for use in access decisions throughout the enterprise. For each organization, these identity management capabilities work.

*Mission Impact*

The challenge will come when one organization needs information from the other. If one organization mandates the use of identity attributes to allow access to information and the other does not have attributes available or the attributes follow a different schema with different acceptable values, this inconsistency can cause an obstacle to information sharing.

**Most agencies have not identified authoritative attribute sources for access management or the means to make these attributes available for agency or enterprise use.**

For many agencies, identity attributes are not maintained at the agency level nor made available to applications on the Secret network either within the agency or to the enterprise. Instead, individual identities are maintained at the application level.

### 2.2.2 Impact

Managing multiple, often duplicative identity stores is expensive and error-prone. The inability to uniquely identify individuals across the Secret fabric makes it impossible to automate information sharing and interoperability.

## 2.3 Credential Management

Username and password is the current de-facto standard for authentication to Secret networks, although some agencies are implementing PKI or other two factor validation. Resources and applications that require authentication beyond network access tend to require credentials separate from the network logon credential causing the need for users to remember multiple usernames and passwords. Analysis of single sign on (SSO) is underway, but the results of the analysis are not available.

With the publication of CNSSP 25 in 2009 and CNSSI 1300 in 2011, the NSS PKI has been established, and CNSS member agencies have begun planning or implementation of interoperable PKI based

credentials on smart card hardware tokens. Both the DoD and State Department have plans in place to use these credentials for network authentication. The FY13 Implementation Guidance for the ISE requires all users of U.S. Secret level networks to use PKI based credentials that are part of or interoperable with the NSS PKI. There is also a DoD memorandum[29] requiring all applications on SIPRNet to be PK-enabled by June 30, 2013.

Figure 3 shows the current architecture of the NSS PKI. Items in red are planned, but not yet operational. The NSS PKI consists of a Root CA operated by the NSA and subordinate CAs operated by those CNSS member agencies that choose to manage their own CA services. In addition, the NSS PKI will operate a Common Services CA that will provide certificates on a fee-for-service basis to agencies who do not wish to operate their own. Both the DoD and the FBI have existing CAs that predate the establishment of the NSS PKI. As an interim solution, the NSS Root CA may issue cross certificates to these legacy CAs to bring them into the NSS PKI until all users can be accommodated by CAs that are subordinate to the NSS Root, as shown by dotted lines in the figure.

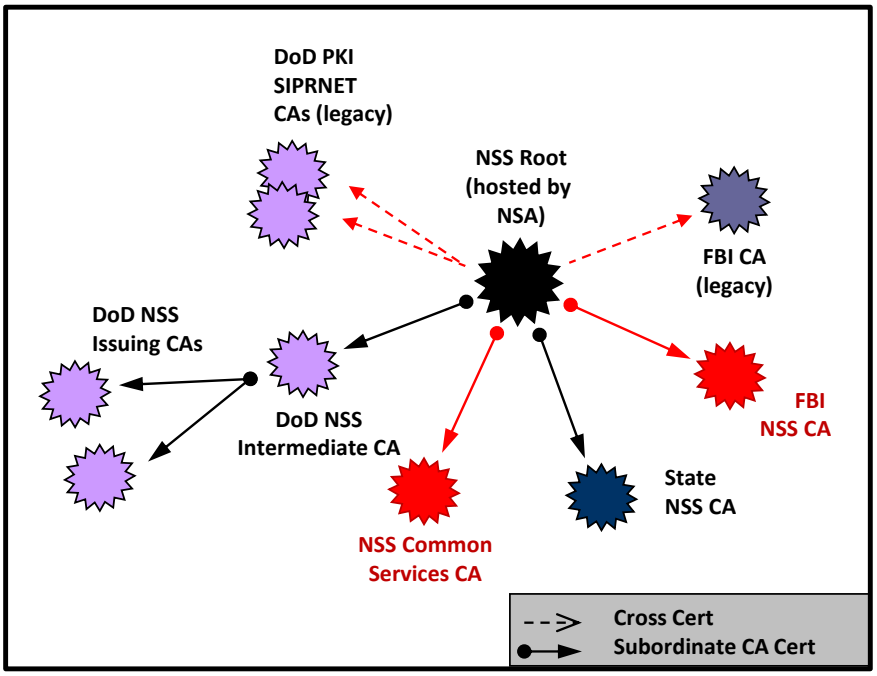


**Figure 3: NSS PKI Architecture**

Credential management on Secret networks has been slow to evolve. Because physical access to Secret network terminals is tightly controlled and the user community for these closed networks relatively homogeneous, simple username and password credentials have sufficed for authentication to the network. As networks become more interconnected and the need for information sharing increases, these authentication mechanisms no longer suffice. Advanced authentication mechanisms that provide higher levels of authentication assurance and non-repudiation are needed at the network boundary and

[29] DoD SIPRNet Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNet Applications and Web Servers; department of Defense; Teresa Takai; 14 October 2011.

application layer to maintain positive control of sensitive information within classified networks. Despite progress in policy and technology implementation of interoperable authentication mechanisms, several challenges remain as illustrated in the gaps below.

### 2.3.1 Gaps

**Personal Identity Verification (PIV) and PIV-Interoperable cards do not meet information security requirements of Classified networks.**

This is a gap between the FICAM and Secret network requirements. HSPD-12 and FICAM mandate the use of FIPS-201 compliant PIV cards throughout the Government for identification and authentication.[30] PKI hardware certificates on the PIV card are used for authentication on Unclassified networks. The General Services Administration (GSA) maintains and approves products list for available PIV cards for Unclassified networks. However, classified environments require a different set of standards baselines, evaluations, and approval processes for credentials. The PIV card was never designed for use on classified networks. Currently, there is a smart card PKI token approved for use in the NSS PKI environment that is certified for use on Secret networks due to the ability to remain Unclassified when removed from the network device. The NSA maintains an approved products list for hardware tokens authorized for use on Secret networks. These differences cause challenges for agency leadership in determining appropriate long-term investments.

**There is not yet a common or interoperable credential implemented across Secret networks.**

Currently the Federal Government uses a mix of username/password and PKI authentication to access Secret networks. Even for those agencies using PKI, it is not yet mandatory for network authentication and only used by a handful of Public Key Enabled applications. While CNSSP 25 requires that PKI implementation on Secret networks be part of the NSS PKI, it does not mandate that agencies use PKI for authentication to the network or applications and data.

### 2.3.2 Impact

The level of interoperability prescribed in the FICAM is not possible without interoperable credentials that can be used for network and resource authentication across the Federal Secret Fabric. These credentials must meet the special requirements of Secret networks, including technical, risk management, and operational needs. Until suitable credentials are defined, mandated, and deployed, the interoperability laid out in the FICAM Roadmap is not a possibility.

[30] HSPD-12: Policies for a Common Identification Standard for Federal Employees and Contractors; 27 August 2004.

*Mission Impact*

In addition to policy and technical challenges associated with deploying PKI solutions on Secret networks, there are tactical environmental considerations that need to be addressed when migrating to a hardware based PKI authentication solution. Imagine a firefighter or other First Responder having to carry multiple hardware tokens to access homeland security information stored on networks at multiple classification levels or a soldier in the field that needs immediate access to tactical command and control information for defense of a forward operating base. Hardware tokens that are lost or damaged in the field may be difficult or dangerous to replace, having a negative impact on mission critical functions.

## 2.4 Access Management

There are both physical and logical components to accessing Secret networks. Because access terminals for Secret level networks are hosted in facilities that meet stringent physical access control requirements, accessing a Secret level network first requires obtaining physical access to the facility where the workstation is housed. Once access to the physical workstation is granted, the user must log on to the network. Today, almost all network logon to Secret level networks is with username/password credentials; however some agencies have begun to use smart cards with PKI credentials. In most cases, individual resources on the network may have their own access controls, including a separate username and password.

Logical access management within Secret networks is largely performed on an application-by-application basis and controlled by the data and application owners. There are few enterprise access control capabilities and most access to data and services is through lookup on an access control list (ACL). Access control capabilities are predominantly very coarse-grained – providing unhindered access to all information with one access control decision. More fine-grained access control mechanisms are needed. These mechanisms evaluate multiple identity, resource, and environmental attributes against specific policy written for the resource being protected. Only in limited instances do agencies perform data tagging for advanced access control decisions. Rather agencies rely on the data owners to control access to their resources by evaluating need-to-know, and not need-to-share. Very few physical access capabilities are integrated with logical access capabilities.

*Key Concept:*
*Access Control vs. Authentication*

Authentication is not the same as Access Control or Authorization. Authentication is the act of validating that the entity performing an action (subject or user) is actually who they say they are. Authentication can be performed using a variety of credentials – typically something that is unique to that user (username and password, public/private key pair in a PKI, biometrics, or other unique characteristic that only the user has, knows, or is). These credentials logically bind the user to a known digital identity – which is made up of identity attributes or information about that user that, when put together, form a unique set of characteristics about that user.

Access Control or Authorization, on the other hand, is the decision (implicit or explicit) to allow or deny a user access to a specific resource (network, data, application, service, etc.). That decision is made by evaluating a number of factors such as identity attributes, access policy, resource information, and other environmental factors (location, risk level). One of the most basic forms of access control is Identity Based Access Control (IBAC), where the identity of the user determines the access. This is most commonly represented by an access control list (ACL) associated with the resource.

Keep in mind that these are two very different functions that often are confused as synonymous because of the prevalence of IBAC as an access control methodology within the Federal Government.

### 2.4.1 Gaps

**Application and Data Access Control is not mandated or implemented uniformly.**

The FICAM envisions an enterprise Logical Access Control System (LACS) that will authenticate users and provision the policies and attributes needed for an access control decision to networks, applications, and data. Of the applications and data that are protected on Secret networks, the application owners write access control rules without the assistance of organization-level guidance. Access control policies and access rules are not managed or recorded at the enterprise level. This prevents the use of a common methodology for controlling access and thereby limits the ability to share information between organizations in a consistent way.

**Data tagging is not performed uniformly.**

This is a gap both within the FICAM requirements and agency capabilities. Access to resources can be controlled by evaluating metadata (data about data). A good example is comparing the user's clearance with the classification of the data to determine whether or not the user should have access. Currently,

metadata is not consistently populated or used in access decisions. In the few instances in which it is being populated, it is only performed to record data classification. Lack of consistent data tagging creates an environment that is insufficient for secure and agile information sharing.

**Few applications are Public Key-Enabled (PKE).**

Among the Secret networks that employ PKI for network authentication, few applications on those networks are public key enabled – or have the ability to use PKI credentials for application authentication and subsequent access.

*Moving in the Right Direction…*

The Department of Energy National Nuclear Security Administration (DOE NNSA) has a data-centric approach to access control. All access to any information on their Secret network, ESN, is dictated by need-to-know. They employ an enterprise attribute repository with a rich set of over two dozen attributes that are passed as SAML attribute assertions to the data repositories and applications to support access decision and enforcement. Policy and rule-sets are still maintained by the data and application owners, but the user attributes are centrally managed and maintained.

### 2.4.2 Impact

Without the FICAM-recommended fine-grained access control mechanism of attribute-based access control (ABAC), anyone who has a Secret clearance and authenticates with their credentials would have access to many resources residing on the Secret network. Access control mechanisms can be utilized for attribute-based decision making such as permitting or denying the discovery of resources and enforcing that decision. By implementing layers of proper access controls, use of a particular resource can be limited. Only those people, programs or devices specifically permitted will have access to the resource.

## 2.5 Audit and Reporting

Auditing and reporting involves identification, collection, correlation, analysis, storage of information, monitoring and maintenance. An auditing and reporting solution should be deployed to centralize data collection and provide appropriate storage for and access to the data. Events should be identified and audited to properly capture and store logs so analysis and reporting can be performed. Certain high-profile events should even trigger automated notification to individuals such as systems administrators and counterintelligence officers.

### 2.5.1 Gaps

**Audit data is not aggregated and correlated internal to the agency.**

While all agencies maintain system logs collecting auditable data like login, configuration changes, file download, etc., most agencies currently do not have an internal capability for automatically collecting data from those logs, aggregating the data to a central repository, correlating event data, and analyzing this data in near real time to identify and respond to unauthorized activity. Audits are primarily performed in response to events to forensically recreate events and identify actors, methods, and impact.

**Audit data is not sharable for correlation of events across agency boundaries.**

Agencies currently do not have the ability to automatically share audit data between agencies for the purposes of correlating Government-wide events. Audit data sharing is limited to forensic analysis of data from multiple agencies in response to an unanticipated or unauthorized event.

### 2.5.2 Impact

FICAM asserts that audit capabilities must be in place to detect certain types of events that cannot be anticipated or protected through traditional ICAM mechanisms (i.e., insider threat). While audit data is collected, the act of the audit – or evaluation of the audit data for anomalies – often only occurs after an incident. Agencies waiting to respond to events after they occur are at a disadvantage. Without proper mechanisms in place, agencies would have difficulty discovering and analyzing issues or security breaches. Further, anomalous behavior may not be considered an incident unless correlated between multiple end-points and sometimes between multiple agencies. Seemingly benign failed login attempts occurring simultaneously on multiple agency networks and timed to interfere with a specific mission function takes on more significance than an isolated attempt. Without the mechanisms needed to correlate this data across organizations, these types of incidents often go unnoticed.

## 2.6 Federation

Information sharing between agencies has evolved out of mission necessity. Federation between Secret networks is currently non-automated and usually established to meet specific mission needs. Access between networks is primarily performed through individual gateways and portals that allow users from other organizations to log into or access networks as internal users to that network. In other cases, information sharing is performed manually using removable media. True federation, accessing another agency's network by using the home organization's credentials and attributes, cannot yet be performed. One of the most significant discoveries is that a majority of the agencies interviewed are reliant upon DoD SIPRNet for a large portion of their mission and information sharing needs. Several agencies have unrestricted unilateral access to SIPRNet upon receiving access to their own network. Other agencies are required to access SIPRNet through a gateway using DoD-issued username and password credentials.

All agencies interviewed have some form of SIPRNet access and only a few of those agencies provide limited bilateral access to their own networks to DoD users.

### 2.6.1 Gaps

**No framework for federated identity exists on Secret networks.**

There is no common governing organization, governance, policy, trust model, or set of interoperability requirements that allow federation of identities on Secret networks. The processes and technologies that Secret network organizations use to provision and manage users are not interoperable and most information sharing is accomplished by provisioning a user account providing access to the external user as if they were an internal user.

**There is currently limited interoperability between Secret networks which impedes information sharing.**

Information sharing solutions on the Secret Networks are currently done in an ad-hoc fashion that is engineered to support a specific information sharing need. Standard methods and technologies are not utilized to promote interoperability.

**Most Secret networks lack a robust transfer capability across security domains.**

This is a gap both within the FICAM requirements and agency capabilities. Most agencies have largely manual or limited data transfer and discovery capabilities across security domains. Both the FICAM and existing agency capabilities lack standard processes, procedures, and technical specifications for sharing information horizontally across enclaves and vertically between security domains. Supporting requirements such as the need for utilizing a single identity and credential are outlined in the FICAM but are not currently implemented within organizations.

**Information sharing between networks is performed on an application-by-application basis.**

Currently, if organizations want to share information, they do so by engineering solutions specific to that application rather than utilizing organization level processes, policies, and technology. An organization-wide information sharing strategy includes policies that dictate information sharing requirements, processes that provide guidance on how information should be shared, and enterprise level technology that is based on interoperable standards.

### 2.6.2 Impact

Due to the lack of governance and infrastructure in place for federation, agencies need to rely on provisioning individual accounts for users that are external to their organization. New information sharing needs require significant lead time to establish agreements between agencies and the technical infrastructure required to share that information. Lack of federation capabilities causes increased logistics such as users having to carry or remember multiple authentication credentials to individually access another agency's resource or application.

This page intentionally left blank

# 3 SUMMARY AND RECOMMENDATIONS

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

The agencies evaluated for this effort recognize their networks were at different stages of implementing the FICAM vision. Most agencies lack a common technical approach to ICAM implementation as illustrated by the gaps mentioned in this report. Additionally, there are ICAM requirements unique to Classified networks that are not addressed in the FICAM as written. These gaps must be bridged in order for agencies to move forward with implementing the FICAM vision on Secret networks.

Now that this report is complete, the next step is to close the identified gaps. As noted in this report, changes to the FICAM are necessary to address the specific needs of Classified networks. As part of this process, representatives responsible for operating Secret networks not included in this report will be contacted to obtain their feedback and perspective to ensure the needs of the entire NSS community are addressed. Once the requirements of Classified networks have been addressed, an implementation plan will follow. This implementation plan will identify specific recommendations to achieve interoperable and secure ICAM capabilities for the Federal Secret Fabric and provide a timeline for addressing them. In addition, the CNSS will develop and publish policy advising departments and agencies to follow the implementation plan in support of the FICAM goals and objectives.

Overall, the agencies interviewed in this analysis are ready and willing to move forward with the FICAM vision and to create an interoperable environment which facilitates information sharing across networks. Additional work is needed in partnership with the Secret network community to identify a viable roadmap and implementation plan. Authoritative policy and governance structures must also be established to facilitate a unified path towards achieving the FICAM vision.

This page intentionally left blank

# APPENDIX A ACRONYMS

| | |
|---|---|
| AASC | Authorization and Attribute Services Committee |
| ABAC | Attribute Based Access Control |
| ACL | Access Control List |
| ASNI | Assured Secret Network Interoperability |
| CA | Certificate Authority |
| CIO | Chief Information Officer |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| COG | Continuity of Government |
| COOP | Continuity of Operations |
| CVS | OPM's Central Verification System or DoD's Contractor Verification System |
| DEERS | Defense Enrollment Eligibility Reporting System |
| DHS | Department of Homeland Security |
| DoD | Department of Defense |
| DOE | Department of Energy |
| DOE-NNSA | Department of Energy-National Nuclear Security Administration |
| DOJ | Department of Justice |
| DOS | Department of State |
| EO | Executive Order |
| ESN | Enterprise Secure Network |
| FAC | Facility Access Card |
| FBI | Federal Bureau of Investigation |
| FBINet | Federal Bureau of Investigation Network |
| FICAM | Federal Identity, Credential, and Access Management Roadmap and Implementation Plan |
| FIPS | Federal Information Processing Standard |
| FPKI | Federal Public Key Infrastructure |
| GSA | General Services Administration |

| | |
|---|---|
| HR | Human Resources |
| HSDN | Homeland Secure Data Network |
| HSPD | Homeland Security Presidential Directive |
| IBAC | Identity-Based Access Control |
| IC | Intelligence Community |
| ICAM | Identity, Credential, and Access Management |
| ICAMSC | ICAM Subcommittee |
| IdAM | Identity and Access Management |
| IPC | Interagency Policy Committee |
| ISA | Information Sharing and Access |
| ISE | Information Sharing Environment |
| ISIMC | Information Security & Identity Management Committee |
| JCON-S | Justice Consolidated Office Network – Secret |
| LACS | Logical Access Control System |
| MGB | Member Governing Body |
| NCSD | National Communications System Directive |
| NIST | National Institute of Standards and Technology |
| NPE | Non-Person Entity |
| NSA | National Security Agency |
| NSD | National Security Directive |
| NSS | National Security Systems |
| NSTC | National Science and Technology Council |
| ODNI | Office of the Director of National Intelligence |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| PIV | Personal Identity Verification |
| PIV-I | Personal Identity Verification-Interoperable |
| PKE | Public Key-Enabled |
| PKI | Public Key Infrastructure |
| PM | Program Manager |
| PM-ISE | Program Manager for the Information Sharing Environment |
| SAML | Security Assertions Markup Language |

| | |
|---|---|
| SIPRNet | Secure Internet Protocol Router Network |
| SSP | Shared Service Provider |
| RBAC | Role-Based Access Control |
| RSA | Rivest, Shamir, and Adleman |
| U.S. | United States |
| USG | United States Government |
| WG | Working Group |

This page intentionally left blank

# APPENDIX B **REFERENCES**


1. http://www.nist.gov/nstic/about-nstic.html
2. Identity, Credential, and Access Management, http://www.idmanagement.gov/pages.cfm/page/ICAM, 3 October 2011.
3. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, 10 November 2009.
4. http://www.cnss.gov/history.html
5. CNSS Policy 25: National Policy For Public Key Infrastructure In National Security Systems; March 2009.
6. ASNI Working Group Charter; 17 November 2010.
7. CNSS Conference 2010 Final Report.
8. CNSS NSS Identity, Credential and Access Management Lexicon, Version 0.5, 24 March 2011.
9. Congressional Testimony; Teresa Takai; "Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"; 10 March 2011.
10. Congressional Testimony; Kshemendra Paul; "Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"; 10 March 2011.
11. PM-ISE Memorandum: FY2013 Implementation Guidance for the ISE; 4 August 2011.
12. Executive Order - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; 07 October 2011.
13. http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
14. CNSS NSS Identity, Credential and Access Management Lexicon, Version 0.5, 24 March 2011.
15. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors; March 2006.
16. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States; http://www.gpoaccess.gov/911/pdf/fullreport.pdf.
17. HSPD-20: National Continuity Policy ; 4 May 2007.
18. NCSD 3-10: Minimum Requirements for Continuity Communications Capabilities; 10 August 2000.
19. OMB M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors (03 FEB 2011).

20. NIST SP 800-53 FPKI Security Controls Profile: Federal Public Key Infrastructure Security Controls Profile of Special Publication 800-53; 9 February 2011.
21. NIST SP 800-53A FPKI Security Controls Profile: Assessment Guidance for Security Controls in PKI Systems; 9 February 2011.
22. CNSSP 25: National Policy for Public Key Infrastructure for National Security Systems.
23. CNSSI 1300: National Instruction on PKI X.509 Certificate Policy.
24. CNSSI 1253: Security Categorization and Control Selection for National Security Systems.
25. CNSSI 4009: National Information Assurance Glossary, April 2010.
26. PM-ISE Memorandum: FY2013 Implementation Guidance for the ISE; 4 August 2011.
27. National Science and Technology Council (NSTC) Archives; Identity Management Task Force Report 2008; http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-identitymgmt-2008.pdf; 3 October 2011.
28. Strategic Letter of Intent Between the Department of Defense Chief Information Officer and the Associate Director of National Intelligence and Chief Information Officer; http://cio-nii.defense.gov/docs/DoDAASI.pdf; 21 April 2008.
29. DoD SIPRNet Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNet Applications and Web Servers; department of Defense; Teresa Takai; 14 October 2011.
30. HSPD-12: Policies for a Common Identification Standard for Federal Employees and Contractors; 27 August 2004.