Committee on National Security Systems

CNSSD No. 507
January 2014

NATIONAL DIRECTIVE FOR IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT CAPABILITIES (ICAM) ON THE UNITED STATES (US) FEDERAL SECRET FABRIC

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION GUIDANCE

CHAIR

FOREWORD

1. CNSS Directive No. 507 governs how Identity, Credential, and Access Management (ICAM) capabilities will be implemented and managed across the Federal Secret Fabric to promote secure information sharing and interoperability within the Federal Government. It establishes the mandate to implement the capabilities embodied within the *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance version 2.0 (FICAM)*, dated December 2, 2011 on Secret level applications, systems and networks owned, operated or maintained by or on behalf of US Government (USG) Departments and Agencies – hereby referred to as the Secret Fabric – and identifies specific outcomes and deadlines for achieving this goal.

2. The *National Strategy for Information Sharing and Safeguarding* (NSISS) was signed by the President in December, 2012 to provide a strategy for sharing and securing our nation's information assets and directs the Federal government to improve interoperability, security, and discovery of sharable information.

3. Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, signed October 7, 2011, requires all Departments and Agencies of the Federal government to implement reforms to their networks and systems to improve the secure sharing of classified information.

4. CNSS is charged with establishing and managing improved interoperable ICAM capabilities on the Federal Secret Fabric that meet the intent of the *FICAM Roadmap and Implementation Guidance*. This Directive is essential to providing a common approach to achieve these goals and to provide a governance structure that promotes development of secure, interoperable frameworks, systems and networks.

This Directive is available from the CNSS Secretariat, as noted below, or the CNSS website: http://www.cnss.gov.

/s/

TERESA M. TAKAI

NATIONAL DIRECTIVE FOR IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT CAPABILITIES (ICAM) ON THE UNITED STATES (US) FEDERAL SECRET FABRIC

SECTION I—PURPOSE

1. This Directive provides governance and objectives for implementing and managing improved and interoperable ICAM capabilities on the Federal Secret Fabric. It establishes the requirement for all United States Government (USG) Departments and Agencies to implement the applicable requirements embodied in the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* on the Federal Secret Fabric and other ICAM capabilities as directed[1]. This Directive also establishes roles and responsibilities and includes guidance for subordinate policies and execution strategies.

SECTION II—AUTHORITY

2. The authority to issue this Directive derives from National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems,* dated July 5, 1990, which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives.

3. Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* signed October 7, 2011, requires all Departments and Agencies of the Federal Government to implement reforms to their networks and systems to improve the secure sharing of classified information. It further charges that effective technical safeguarding policies and standards must be developed in coordination with the CNSS by the Executive Order's Executive Agent for Safeguarding Classified Information on Computer Networks.

4. Nothing in this Directive shall alter or supersede the authorities of the Director of National Intelligence (DNI).

5. Nothing in this directive shall rescind or supersede existing National, Federal, Agency, and organization-specific requirements for the proper handling and protection of classified information.

[1] In this directive, the term *FICAM* refers to the requirements embodied within the FICAM Roadmap and Implementation Guidance. The term *ICAM* refers to functional ICAM capabilities.

SECTION III—SCOPE

6. This Directive applies to all USG Departments and Agencies who own, procure, operate, or maintain capabilities on the Federal Secret Fabric.

a. The Federal Secret Fabric consists of all USG Department and Agency Secret-level applications, systems, and networks – to include closed or stand-alone systems and networks.

7. This Directive applies to all USG Department and Agency supporting contractors, agents, non-federal affiliates, and international partners that own, procure, operate, or maintain capabilities that interface with the Federal Secret Fabric. Those supporting contractors, agents, non-federal affiliates, and international partners with Secret-level applications, systems, and networks not interfacing with the Federal Secret Fabric are outside the scope of this Directive.

8. This Directive does not apply to National Security Systems (NSS) classified as Unclassified, Confidential, or Top Secret.

SECTION IV—POLICY

9. USG Departments and Agencies shall be responsible for developing their own FICAM implementation plans for the U.S. Secret Fabric and will provide the status of their plans on a semi-annual basis starting April 1, 2014.

10. The end-state objective of FICAM implementation shall be a common set of ICAM operational features that provide assurance and information sharing capabilities. These features must at a minimum include, but are not limited to:

a. Identity – USG Departments and Agencies shall establish an Identity Management capability on Secret networks leveraging and updating the existing identity management processes and technologies to meeting current requirements. They shall work together to perform the activities required to lay the foundation for identifying architecture standards, technologies, processes, and interfaces that will be used in future interoperability. The identity management capability shall have the following features:

i. An onboarding process for new internal and external members of the owning organization which includes identity proofing; vetting; clearance processing; subject attribute issuance, modification, revocation; and unique digital identity creation;

ii. A process and mechanism for the authoritative establishment, exposure, revocation, and alteration of a minimum set of common subject attributes that can be shared across the Secret Fabric for the purposes of directory or white pages lookup or access decision determination;

iii. Issuance of a unique digital credential, bound to the digital identity of the individual and used for network boundary and application authentication and authorization;

iv. Processes and mechanisms for digital identity and credential modification and revocation.

b. Authentication – USG Departments and Agencies shall develop and implement a common authentication capability on Secret networks leveraging the NSS PKI[2] and shall work together to perform the activities required to lay the foundation for identifying architecture standards, technologies, processes, and interfaces that will be used in future interoperability. This authentication capability shall have the following features:

i. Certificate-based network logon including logging each access using a unique identifier contained in PKI digital certificates;

ii. Certificate-based authentication to systems with moderate and high impact for confidentiality, as determined by each Department and Agency[3];

iii. Certificate-based authentication to systems across the Federal Secret Fabric including employees as well as affiliates and international partners as necessary.

c. Access – USG Departments and Agencies shall develop and implement access management capabilities to all designated systems[4] across the Federal Secret Fabric to support secure information sharing, attribution, and data protection. All entities on the Federal Secret Fabric shall work together to perform the activities required to lay the foundation for identifying architecture standards, technologies, processes, and interfaces that will be used in future interoperability. This access management capability shall have the following features:

i. A shared set of subject attributes that are common across the Federal Secret Fabric to ensure interoperability in access requests for shared information;

ii. Designated subject attribute authorities;

iii. Shared digital policy[5] rules used to control access to similarly protected resources across the Federal Secret Fabric;

iv. For all systems, networks and applications – access using a unique identifier in digital certificates that is linked to the user's subject attributes;

[2] CNSSD 506, *National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks*, provides additional architectural and technical detail regarding the NSS PKI.

[3] Determination of moderate and high impact systems is left to the discretion of each Department and Agency based on guidance provided in CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*..

[4] A designated system is one that has been designated as a system on the Federal Secret Fabric.

[5] This may include Natural Language Policies (NLPs), high-level requirements that specify how information access is managed and who, under what circumstances, may access what information. NLPs must be codified into Digital Policy (DP) algorithms or mechanisms.

v. For all specially designated systems – access using Attribute Based Access Control (ABAC)[6] capabilities where access decisions are based on digital policy.

vi. Rules using subject, resource, and, in some cases, environmental attributes. Specially designated systems will be identified by the cognizant Department and Agency representative and shall, at a minimum, include all systems that share restricted information outside of the Department or Agency.

vii. Implemented processes for on-going maintenance and management of attributes and digital policies.

d. Auditing and Reporting – USG Departments and Agencies shall implement auditing and reporting capabilities on all designated systems across the Federal Secret Fabric to support secure and lawful information sharing, attribution, and data protection. All entities on the Federal Secret Fabric shall work together to perform the activities required to lay the foundation for identifying architecture standards, technologies, processes, and interfaces that will be used in future interoperability. This auditing and reporting capability shall have the following features:

i. Ability to log digital identity and event information for each authentication and authorization transaction in order to ensure non-repudiation and enable the capture of forensic data in the event of an intrusion or in response to an internal threat;

ii. Ability to report unsuccessful authentication or authorization attempts for the purposes of helping authorized users gain access and identifying suspicious activities by non-authorized users.

11. Transition to the end state objectives outlined in paragraph 10 shall commence upon approval of this directive. Departments and Agencies may implement capabilities sooner but, at a minimum, are required to meet the following capability milestones by the end date identified for each stage of implementation in Table 1. For more information on transition stages, capability goals, and milestone dates, refer to the *FICAM Planning Guidance for the Secret Fabric*.

SECTION V—RESPONSIBILITIES

12. The CNSS Sub-Committee(s) shall:

a. Approve standards, interfaces and protocols for implementing FICAM on Secret networks.

b. Publish the Policy or Directives, approved by the Committee Chair/Co-Chair, required to support management of ICAM capabilities on the Federal Secret Fabric, deployment of new capabilities, and interoperability with foreign affiliates.

[6] While there are different models for authorization, ABAC has been selected for this policy because it provides the flexibility needed for interoperable secure sharing of information in a wide variety of environments.

c. Publish minimum service level requirements for information confidentiality, integrity and service availability for providers of shared services.

d. Publish a waiver process and guidance to identify systems, networks and applications that should be exempt from specific FICAM requirements.

13. The CNSS Identity and Access Management (IdAM) Working Group shall:

a. Draft guidance for CNSS review and approval related to implementation of FICAM on the Secret Fabric.

b. Recommend a trust model for information sharing between Departments and Agencies that includes common access control methods based on the impact value of the system or data; a common set of shared attributes (subject, resource, and environmental); common digital access rules required for authorization decisions; and data governance models.

c. Determine common or shared ICAM services required by multiple Departments and Agencies that could be offered by a common provider.

d. Identify, with CNSS Committee approval, USG providers of shared ICAM services for shared or common services required by multiple Departments and Agencies across the Federal Secret Fabric.

e. Provide FICAM implementation compliance reports to the CNSS Committee.

f. Develop guidelines for selecting specially designated systems for ABAC implementation.

g. Identify minimum and recommended ICAM capabilities for closed or stand-alone systems and networks that include, at a minimum, auditability and non-repudiation capabilities

h. Coordinate resolution of, or exceptions from, conflicting requirements, standards, interfaces or protocols including coordinating the waiver process.

i. Coordinate the development of Identity and Access policies and standards keeping into account those policies and standards already in use on other networks to support interoperability of applications deployed across multiple networks and cross domain access of data with networks of other classifications.

j. Provide recommendations for standards, interfaces and protocols to the ICAM Sub-Committee (ICAMSC) taking into account those standards, interfaces, and protocols used on other fabrics to promote portability of applications to and from other fabrics (Unclassified, Confidential, or Top Secret).

k. Collaborate with appropriate authorities on the Unclassified, Confidential, and Top Secret fabrics to leverage lessons learned.

14. Each Department and Agency of the USG owning or operating applications, systems, or networks on Federal Secret Fabric shall:

a. Designate a lead official, representative, or governing body to serve as the single point of coordination for that Department or Agency with the CNSS IdAM WG no later than ninety days from the signature on this directive.

b. Publish subordinate policies; implementation plans; and establish the coordination, implementation, and reporting structures required to support the development and deployment of FICAM on the Secret Fabric including policies and activities required by applicable security risk management procedures.

c. Implement applicable ICAM capabilities in accordance with paragraph 8 of this directive.

d. Identify systems that meet the definition of high and moderate impact for confidentiality as defined in CNSSI 1253.

e. Identify closed or stand-alone systems and networks that should be partially or fully exempt and provide justification in accordance with the waiver process defined by CNSS.

f. Identify access control rules and policies for protected resources.

g. Identify subject, resource, and environment attributes needed to satisfy access control rules and policies.

h. In coordination with other Departments and Agencies, identify a common set of subject attributes to be used for information sharing.

i. In coordination with other Departments and Agencies, identify a common set of shared FICAM services to be deployed to the Federal Secret Fabric.

j. Establish trust agreements necessary to make authorization information available for use by access control mechanisms in other Departments or Agencies where interoperability and information sharing is required.

k. Identify specially designated systems that will employ ABAC and which systems will use alternative authorization capabilities.

l. Plan, program, and budget for the appropriate resources to implement and maintain FICAM for the Federal Secret Fabric for their respective applications, systems and networks in accordance with the Office of Management and Budget (OMB) A-130 and peer or subordinate Department or Agency policies and guidance.

m. Prepare semi-annual reports on the status of the Departments’ and Agencies’ FICAM implementation progress and submit them to the CNSS.

15. The Office of the Director of National Intelligence shall:

a. Coordinate with the CNSS IdAM WG on all matters relating to policy, implementation, and management of IdAM capabilities for the Intelligence Community (IC) on the Federal Secret Fabric.

b. Designate the Intelligence Community IdAM Steering Committee (IC IdAM SC) as the IC coordinating body for the Federal Secret Fabric, specifically to represent the DNI, CIA, NSA, NGA, DIA, and SCI users and systems accredited under ICD 503 at the Secret Level.

i. The IC IdAM SC shall report overall activities of the IC as well as specific activities performed by the DNI to include policy creation; progress metrics; and sharing of best practices for IdAM capabilities such as Digital Policy Management (DPM), Entitlements Management, and Secure Token Services.

16. Providers of shared services for FICAM on the Secret Fabric excluding PKI[7] shall execute Service Level Agreements (SLAs) that include required metrics for information confidentiality, integrity, and service availability; as well as provisions for escalation processes, problem resolution, change processes, and performance guarantees with related penalties for lack of performance.

Enclosures:

ANNEX A – Definitions

ANNEX B – References

[7] Responsibilities of providers of shared PKI services are found under Common Service Providers (CSP) in CNSSD 506.

ANNEX A

17. Definitions used in CNSSI No. 4009, National Information Assurance Glossary, revised April 2010, apply as appropriate to this Directive. Listed below are some additional terms and their definitions. Within this Directive, these definitions are used exclusively for these terms.

DEFINITIONS

Attribute-Based Access Control (ABAC): A logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes.

Common Services Provider (CSP): A federal organization that provides NSS-PKI support to other federal organizations, academia and industrial partners requiring classified NSS-PKI support but without their own self-managed infrastructures.

Federal Secret Fabric: All Secret level applications, systems and networks owned, operated or maintained by or on behalf of USG Departments and Agencies.

Identity, Credential, and Access Management (ICAM):[8] An integrated set of capabilities to create and manage identities, credentials, and policy and electronically automate authorization decisions for access to information resources.

International Partner: Foreign government or organization of governments that interfaces with the Federal Secret Fabric.

[8] Also referred to as "Identity and Access Management (IdAM)".

ANNEX B

REFERENCES

1. (U) Executive Order 12333, *United States intelligence activities*, December 4, 1981

2. (U) National Security Directive (NSD)-42, *National Policy for the Security of National Security Telecommunications and Information Systems,* July 5, 1990

3. (U) Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

4. (U) Committee on National Security Systems Instruction Number 1253 (CNSSI 1253), *Security Categorization and Control Selection for National Security Systems*, June 2011

5. (U) *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance version 2.0 (FICAM)*, December 2, 2011

6. (U) *Federal Identity, Credential, and Access Management (FICAM) Planning Guidance for the Secret Fabric,* December 2013

RELATED DOCUMENTS

1. (U) Committee on National Security Systems Policy Number 15 (CNSSP 15), *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, March 2010

2. (U) Committee on National Security Systems Directive Number 900 (CNSSD 900), *Governing and Operating Procedures*, September 12, 2012(U) Committee on National Security Systems Policy Number 506 (CNSSP 506), *National Directive to Implement Public Key Infrastructure for the Protection of Systems Operating on Secret Level Networks,* October 9, 2012

3. (U) Committee on National Security Systems *Recommendations for Implementing FICAM on U.S. Secret Networks,* January 2013

4. (U) NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Final Draft)*, December 2013

5. (U) Committee on National Security Systems Instruction Number 4009 (CNSSI 4009), *National Information Assurance (IA) Glossary*, current edition