BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
(DAF) MANUAL 17-1304

18 AUGUST 2021

Cyberspace Operations

IIDENTITY, CREDENTIAL AND ACCESS MANAGEMENT (ICAM)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNZ

Certified by: SAF/CNZ
(Wanda T. Jones-Heath)

Supersedes: N/A

Pages: 61

This Department of the Air Force Manual (DAFMAN) implements Air Force Policy Directive 17-1, *Information Dominance Governance and Management* and Air Force Instruction (AFI) 17-130, *Cybersecurity Program Management*. This manual applies to all civilian employees and uniformed members of the Department of the Air Force (DAF), Air Force Reserve (AFR), Air National Guard (ANG), and those with contractual obligation to comply with DAF publications, regardless of Air Force specialty code, who develop, acquire, deliver, use, operate, or manage ICAM for DAF organizations. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force records disposition schedule located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This DAFMAN may be supplemented but all supplements to this publication must be routed to SAF/CN, Cybersecurity Division, for coordination prior to certification and approval. **(T-3).** The authorities to waive wing or unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, in accordance with DAFI 33-360_DAFGM2020-01, Attachment 3, paragraph 6.5.6.3.5, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. The use of the name or mark of any specific

manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

Chapter 1

INTRODUCTION

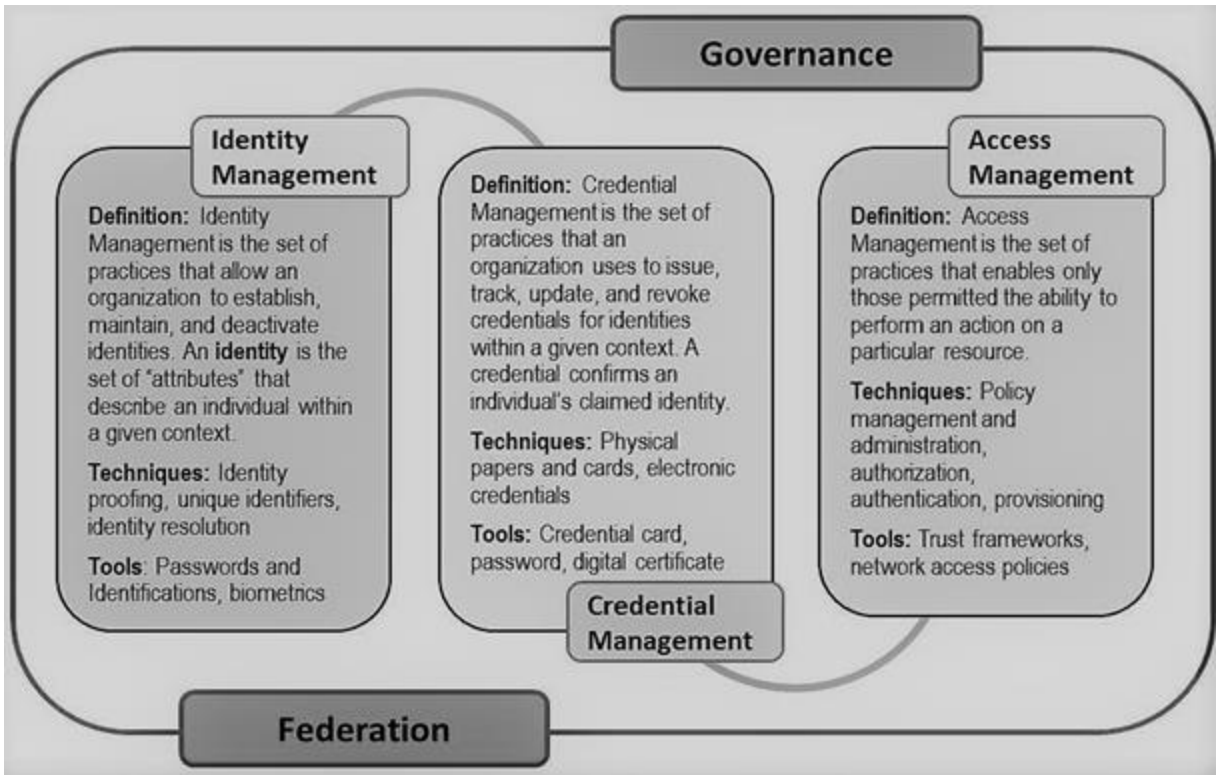
1.1. Overview. ICAM is the solution to build trust by aligning all participants to an agreed-upon set of policies, technical standards and best practices. DoD chief information officer (CIO) manages ICAM programs with combatant commanders, services, and agencies that the DAF supports and implements. While identity management, credential management, and access management are closely interrelated, it is important to understand each individual ICAM facet. Identity management, access management, and credential management are supported and enabled by a foundation of governance and federation accepting the ICAM information from other entities across organizational boundaries. Governance is what enables organizations to implement and manage effective ICAM policies and capabilities. Federation is how organizations are able to accept ICAM information from other organizations, (e.g., services, agencies, mission partners) thereby enabling interoperability, because no one organization can operate in a bubble, as illustrated in **Figure 1.1** from the Department of Homeland Security (DHS) *ICAM 101 Briefing for Public Safety Officials*.

1.1.1. Identity management allows an organization to construct a trusted digital identity based on an individual's defining attributes. It establishes identity using trusted evidence, creates an identity account, provisions the account with required attributes, updates identity account over the life cycle, and de-provisions and deletes identities.

1.1.2. Credential management allows an organization to associate a digital identity with authoritative proof of the claimed identity. The life cycle establishes a sponsor need, registers subscribers in identity databases, issues and maintains credentials, and revokes those credentials, adding them to revocation lists.

1.1.3. Access management allows an organization to leverage trusted identities (person and non-person entities) and authoritative credentials to ensure only permitted individuals are granted access to protected resources. This is the set of practices and services for ensuring only those with proper permissions can interact with a given resource. Access control policies at all levels govern access requirements. Authentication verifies a claimed identity is genuine based on valid credentials. Authorization is the decision to grant or deny access to a resource based on policy.

Figure 1.1. Definition of Identity, Credential and Access Management.



1.2. Objective. The objective of this publication is to explain how Airmen at all levels employ technologies and techniques to comply with DoD and AF ICAM policy when accessing Air Force information systems (ISs) in accordance with all relevant cybersecurity and data policies (SAF/CN).

1.3. Applicability. This publication applies to all DAF information technology (IT) and devices used to process, store, display, transmit and protect DAF information and the authorized users of these resources.

1.3.1. DAF IT includes but is not limited to ISs (major applications and enclaves), platform information technology (PIT) and PIT systems, IT services (internal and external), standalone systems, and IT products (software, hardware, and applications), unless specifically exempted. Specific use cases exempted from public key infrastructure (PKI) and two-factor authentication are listed in the DoD CIO Memorandum, *Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems*, and are authorized to use DoD approved usernames and passwords. These use cases include: 1) stand-alone networks and systems and kiosks; 2) closed restricted networks; 3) platform information technology (PIT); 4) lab and testing environments; 5) emergency, backup, and local logon accounts; and 6) tactical, deployed, or low bandwidth environments.

1.3.2. Compliance is mandatory for all military, mission partners, civilian, and contract employees who develop, acquire, deliver, use, operate, or manage DAF IT.

1.3.3. The DAF relies on two-factor authentication (2FA), a digital identity bound to a credential used for authentication to a relying party (RP). Relying parties are system

application owners that support one or multiple credentials, including PKI certificates, security assertion markup language, and other claims-based identifiers.

1.3.4. The DAF follows defined sensitivity levels to determine appropriate authentication methods, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Digital Identity Series*, and DoD Instruction (DoDI) 8520.03, *Identity Authentication for Information Systems*.

1.3.5. More restrictive federal, DoD, or DAF guidance take precedence over this publication, (e.g., DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, and DoDI 8520.03).

1.3.6. This publication and implementation guidance identified within is not applicable to special access programs or intelligence community (IC) ISs, to include sensitive compartmented information (SCI) ISs. Refer to the IC Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, and AFI 16-701, *Management, Administration and Oversight of Special Access Programs*.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force, DAF Chief Information Officer (SAF/CN). Oversees the configuration and implementation of DAF cybersecurity and ICAM policies, to include evaluation and implementation of changes required by DoD services and agencies to promote identity management, credential management, and access management.

2.2. Air Force Chief Information Security Officer (SAF/CNZ CISO).

2.2.1. Establishes DAF related doctrine, plans, and policies supporting the use of DoD, National Security Systems (NSS), and DAF Public Key Infrastructure and ICAM related initiatives.

2.2.2. Serves as the DAF policy authority, ensuring all applicable initiatives, systems, services, and capabilities are consistent with DoD, NSS, and DAF PKI policy.

2.2.3. Designates SAF/CNZ office responsible to represent DAF at the DoD PKI certificate policy management working group and supports DoD ICAM and PKI related working groups.

2.2.4. Performs all duties and responsibilities in accordance with AFI 17-130 and AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*.

2.2.5. Performs all duties and responsibilities as stated in accordance with Committee on National Security Systems Instruction (CNSSI) 1300, *Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy Under CNSS Policy No. 25*, DoD *X.509 Certificate Policy v.10.6,* and other DoD directives and cyber orders.

2.2.6. Participates in PKI member governing body discussions.

2.2.7. Nominates appropriate persons as Registration Authority (RA) to the DoD Program Management Office (PMO).

2.2.8. Reviews periodic compliance audits to ensure that Certification Authorities (CA), RAs, and other components operated by the agency are operating in compliance with their approved certification practice statements (CPSs).

2.3. Air Force Chief Technology Officer (SAF/CN CTO).

2.3.1. Serves as the DAF representative at the DoD Identity Protection Management Senior Coordinating Group.

2.3.2. Performs all duties and responsibilities in accordance with Headquarters Air Force Mission Directive (HAFMD) 1-26, *Chief, Information Dominance and Chief Information Officer*.

2.4. Air Combat Command (ACC) A6 . Designated as the DAF lead command for Cyberspace. Reviews and provides implementation recommendations for cyberspace doctrine, policy, and procedures to SAF/CN. A6O serves as ICAM service owner. Primary duties include:

2.4.1. Evaluating requirements for alignment to Air Force strategy and mission, ensuring solutions meet the needs of the user community.

2.4.2. Advocating for funding and prioritizing resources that support ICAM.

2.4.3. Working with service managers to evaluate service quality, and if required, develop improvement plans.

2.4.4. Acting as the single voice to program executive officers for priorities and requirements.

2.5. Authorizing officials (AOs). The AO is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, in accordance with AFI 17-101. The Air Force Enterprise AO is the only authority permitted to grant an approval to connect to Air Force information networks. Approval to connect authorities for other DAF appointed AOs are approved by SAF/CN, in coordination with the Enterprise AO. In addition to the AO responsibilities above, the Enterprise AO:

2.5.1. Establishes acceptable security controls and risk tolerance for connecting to the Air Force information network (AFIN) and provides guidance to implementing organizations to mitigate risks commensurate with established risk tolerance.

2.5.2. Reviews the security authorization package for all requests to connect to the Air Force Information Network and assesses the impact to enterprise community risk.

2.5.3. Renders AFIN connection decisions in the form of an approval to connect for non-AF systems and for AF systems falling under another AO.

2.5.4. Responds to urgent or emergency requests to connect to the AFIN. This can be delegated to an Enterprise AO designee.

2.6. 16th Air Force (16AF). 16 AF is responsible for implementing ICAM guidance and technologies for DAF ISs.

2.7. 688th Cyber Wing /690th Cyber Operations Group. This organization serves as the AFIN helpdesk.

2.8. Cyberspace Capabilities Center (CCC). CCC is the ACC/A6 executive agent. On behalf of ACC/A6, CCC:

2.8.1. Provides clarification of ICAM policy and guidance for the USAF.

2.8.2. Gathers identity management and credential management requirements for ICAM to SAF/CN and all Major Commands (MAJCOMs)/Field Operating Agencies (FOAs)/Direct reporting units (DRUs).

2.8.3. Drafts policy updates regarding implementation, management, and use of PKI.

2.8.4. Provides identity management administrative support to USAF and Combatant Commands (CCMDs).

2.8.5. Ensures ICAM policies, standards, and instructions implemented by USAF users in CCMDs align with AF ICAM policy and instructions.

2.8.6. Recommends any necessary ICAM policy changes through ACC/A6 to the AF PKI System Program Office (SPO) for higher level guidelines or directives.

2.8.7. Serves as a voting member on the Requirements Review Board for Air Force Directory Services (AFDS).

2.8.8. Coordinates with the ACC Cybersecurity Division as required and accomplishes other roles and responsibilities as directed by ACC/A6.

2.9. Air Force Life Cycle Management Center (AFLCMC/HNID). Enterprise IT & Cyber Infrastructure Division, Commoditized Infrastructure Branch, Identity Solutions Branch. Acquires, adapts, and evolves cybersecurity and information assurance (IA) capabilities and systems across the AFIN, providing ICAM solutions as directed by DoD and the DAF; engages with lead command to establish priorities for ICAM requirements.

2.9.1. In coordination with lead command and SAF/CN, reviews, evaluates, interprets, and incorporates ICAM policy and guidance for the DAF.

2.9.2. In coordination with lead command and SAF/CN, maintains and enforces the integrity of the identity management process and infrastructure and its use, including PKI.

2.9.3. In coordination with lead command and SAF/CN, provides ICAM research, engineering, and policy support, and management of ICAM and PKI to SAF/CN, DAF organizations, AFR, ANG, CCMDs, and DoD PKI (PMO), as directed.

2.9.4. In coordination with lead command and SAF/CN, drafts and updates DAF policy on implementation, management, and use of ICAM and PKI, and identifies, documents, reviews, and approves all PKI policy requirements with DoD and PKI leaders.

2.9.5. In the absence of a program of record designation, serves as the AF ICAM program management office. Supports AF ICAM technical services to DAF systems, which includes consultation with DoD CIO, DoD PKI PMO, National Security Agency, Defense Information Systems Agency (DISA), United States Cyber Command (USCYBERCOM), Defense Security/Cybersecurity Authorization Working Group , SAF/CN, MAJCOMs, DRUs, FOAs, and supported CCMDs.

2.9.6. Provides technical assistance and guidance to subscribers and program managers, ensuring systems are in compliance with ICAM policies, standards and instructions.

2.9.7. Researches alternative authenticator form factors, including how to accomplish credentialing and identity binding. Provides integration guidance to application and system owners and assists program offices in defining attributes needed for authorization decisions.

2.9.8. Provides ICAM helpdesk and field support to the DAF and supported CCMDs.

2.9.9. Integrates AFDS and provides attribute exchange services between designated authoritative attribute data sources, DoD, and DAF credential service providers (CSPs), as required.

2.9.10. In coordination with lead command and SAF/CN, plans and budgets the activities supporting the fielding and sustainment of identity assurance programs.

2.10. Information System Owner (ISO) Official is responsible for the overall procurement, development, integration, modification, operation, and maintenance of DAF IT, in accordance with AFI 17-101, Air Force Manual (AFMAN) 17-1301, *Computer Security (COMPUSEC)*, and DoDI 8500.01, *Cybersecurity*.

2.10.1. Non-DoD Federal agencies that require access to data in the IS must be approved by the ISO. ISO to follow data sensitivity levels within NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*.

2.10.2. Ensures compliance with the requirements in accordance with DoDI 8520.03 prior to granting or authorizing IS access.

2.11. Information System Security Officer (ISSO) . ISSO is responsible for the technical implementation of a cybersecurity program. When circumstances warrant, a single individual may fulfill both the Information System Security Manager (ISSM) and the ISSO roles. AFI 17-101, AFMAN 17-1301, and DoDI 8500.01 outline the duties of the ISSO.

2.11.1. The ISSO (referred to as the "Information Assurance Officer" on the DD Form 2875, *System Authorization Access Request (SAAR)*).

2.11.1.1. Retains the account request according to instructions outlined on the form for non-AFNET information systems. The organization or the system ISSO retains the account access request according to the instructions on the form for Air Force information systems.

2.11.1.2. Immediately notifies the supporting Trusted Agent (TA), Local Registration Authority (LRA), or the AF RA (**afpki.registration@us.af.mil**) directly by encrypted email when an AF PKI certificate holder (software certificate or token) suspects a compromise of the holder's private key in accordance with DoD RA-LRA CPS.

2.11.1.3. Performs audits on the RA/LRA workstations in accordance with CNSSI 1300.

2.11.1.4. Performs archive and delete functions of the security audit log and other archived data, manages the audit trail, examines audit trails and archival activities, and ensures overall security of the workstation or system.

2.11.1.5. Performs Self-Assessment Checklist in accordance with the DoD PKI *Registration Authority/Local Registration Authority Certification Practice Statement* (RA/LRA CPS) and the NSS PKI DoD Registration Practice Statement (RPS).

2.11.1.6. Retains account access requests according to instructions on the form for Air Force information systems.

2.12. Information System Security Manager (ISSM). Appointed and performs all duties and responsibilities in accordance with AFI 17-101, for DAF IT.

2.12.1. Primary cybersecurity technical advisor to the AO for the DAF IT.

2.12.2. Duties are outlined in accordance with AFI 17-101, AFMAN 17-1301, and DoDI 8500.01.

2.12.3. Initially validates requests for role-based and group accounts.

2.12.4. Collects PKI requirements affecting the base enclave (e.g., common access card (CAC) removal behavior, screen-lock exemption) from Commanders support staff (CSS) and all FOAs and DRUs.

2.12.5. Updates Information Technology Investment Portfolio Suite (ITIPS) with PKI status and submits waiver requests as needed.

2.12.6. Accepts or rejects Plan of Action and Milestones through the Change Control Requirements Board to be included into the RMF package.

2.13. Wing Cybersecurity Office (WCO). Provides ICAM policy and technical subject matter expertise for IT under the control of the base communications squadron or flight, including IT for tenant units (e.g., FOAs, DRUs, other service units), unless formal agreements exist. **Note:** For bases with more than one wing, the designated host wing will provide this function. For Joint Bases, the AF is responsible for all AF-owned IT and infrastructure.

2.13.1. Provides ICAM requirements gathering for any users within their enclave.

2.13.2. Supports base cybersecurity initiatives.

2.13.3. Reviews, evaluates, and clarifies AF ICAM doctrine, policy, and procedures.

2.13.4. Develops and coordinates recommendations on implementation of the doctrine, policy, and procedures to the CSS or similar function.

2.14. Commanders Support Staff (CSS). Organizational commander implements and enforces AFNET account management administrative processes and procedures using the guidance within this instruction, in accordance with AFI 17-130.

2.14.1. Maintains AFIN access documentation.

2.14.2. Collects PKI subscriber requirements and provides to the ISSM.

2.15. Communications Unit. Any local communications-supporting unit, (e.g., flight, squadron, group, directorate).

2.15.1. Issues authenticators as needed.

2.15.2. Assists with identity management (e.g., building information, phone number) and access management (e.g., work hours, office affiliation).

2.16. Certification Authorities (CAs). An entity authorized by the CISO to create, sign, and issue public key certificates to be used within an enterprise.

2.16.1. Responsible for all aspects of the issuance and management of certificates, to include the registration process, identification and authentication, publication, revocation, and re-keying of certificates.

2.16.2. When a new CA is established, the CA root certificates are loaded and built into the root chains that must be added to every device trusting the new CA and added to the servers, workstations, and devices of relying parties, in accordance with the DoD Certificate Policy. **(T-0)**.

2.16.3. Maintains and updates a Certificate Revocation List (CRL) for certificates it has issued.

2.16.4. Coordinates with AFLCMC to add a new CA into the Certificate Trust List.

2.16.5. Ensures all Secret Internet Protocol Router Network (SIPRNET) networks use the NSS Root CA and are current with all PKI security patches and configuration settings, in accordance with DoD RA-LRA CPS.

2.16.6. Both the CA and RA are Certificate Management Authorities (CMAs). This policy uses the term CMA when a function may be assigned to either a CA or a RA, or when a requirement applies to both CAs and RAs. The division of subscriber registration responsibilities between the CA and RA may vary among implementation of this certificate policy. This division of responsibilities are described in the CA's CPS.

2.17. AF PKI Registration Authority (RA) . RAs are individuals authorized by the CMA to collect, verify, and submit information provided by potential subscribers, which is entered into public key certificates. AF RAs are appointed by SAF/CNZ.

2.17.1. CCMDs establish their own RA or use the RA of their designated supporting service and abide with their operational policies.

2.17.2. Authorized by the DoD PKI PMO and in accordance with AFI 17-130 and DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

2.17.3. Duties and responsibilities are outlined in DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

2.17.4. AF RAs manage the certificate registration program for the DoD and govern the functions and approval process for Local Registration Authority(LRA)/Trusted Agent (TA)/alternate TA throughout the DAF.

2.17.5. RAs have unique privileges:

2.17.5.1. Manage certificate revocation, key recovery, and other aspects of certificate management.

2.17.5.2. Verify and validate the identity and subscriber information and all renewals of non-privileged subscriber Alternate Logon Token (ALT) and SIPRNET group or role identity certificates for each subscriber in the RAs organization.

2.17.5.3. RAs may delegate the responsibility for individual subscriber authentication to LRAs/TAs.

2.18. Local Registration Authority (LRA) . A type of RA with responsibility to perform some aspects of certificate issuance and management for a local community. An individual with privileged access authorized to perform operations on the RA/LRA workstation.

2.18.1. Appointed in accordance with DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

2.18.1.1. Designated LRAs have certificate issuance authority for the entire installation, including tenant organizations and geographically separated units supported by the installation.

2.18.1.2. LRAs normally reside at the base communications unit or communications focal point but can be located anywhere, as long as they have SIPRNET and Non-classified Internet Protocol Router Network (NIPRNET) connectivity.

2.18.1.3. Bases and sites need a minimum of two LRAs. Bases can request additional LRAs; however, AF RAs have final approval, based on number of SIPRNET users, SIPRNET token issuance, LRA usage, and justification from the base.

2.18.2. Trained in accordance with **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/Help%20and%20Training%20for%20Local%20Registration%20Authorities.aspx**.

2.18.3. Upon completion of the training course, military and civil service personnel are eligible to be awarded the Special Experience Identifier 044.

2.18.4. Performs the duties as outlined in DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

2.18.5. Verifies subscriber identities, issues organizational e-mail encryption certificates, NSS SIPRNET tokens, and forwards revocation requests to the AF RA, in accordance with DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

2.18.6. Configures Firefox™ on the LRA workstation in accordance with **https://inteldocs.intelink.gov/inteldocs/page/repository#filter=path%7C/Group%20Folders/A/AF%20PKI%20SPO/LRA%20Resources%20%28Restricted%29**.

2.18.7. Performs annual self-assessments using the AF LRA PKI Self-Assessment Checklist (**https://intelshare.intelink.gov/sites/usafpki/_layouts/15/start.aspx#/SitePages/AF%20Public%20Key%20Infrastructure%20System%20Program%20Office.aspx/html/lra_trg.cfm**).

2.18.7.1. Submits results of annual self-assessment to RAs.

2.18.7.2. Uploads results into the management internal control toolset.

2.19. Trusted Agent (TA) and Alternate TA. Perform face-to-face subscriber authentication of PKI sponsors for NPEs and code signing certificates on behalf of the LRA.

2.19.1. Appointed by the commander or designee at the request of the LRA, in accordance with DoD PKI RA/LRA CPS and the NSS PKI DoD RPS. The template for the TA designation letter and information on the TA role and responsibilities is found at **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/Help%20and%20Training%20for%20Trusted%20Agents.aspx**.

2.19.2. Training requirements are outlined in **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/Help%20and%20Training%20for%20Local%20Registration%20Authorities.aspx**.

2.19.3. Provide subscriber support during certificate issuance and personal identification number (PIN) reset.

2.19.4. Submit requests to the RA or LRA for certificate revocation, suspension, and restoration.

2.19.5. Configure a TA workstation in accordance with https://inteldocs.intelink.gov/inteldocs/page/repository#filter=path%7C/Group%20Folders/A /AF%20PKI%20SPO/LRA%20Resources%20%28Restricted%29**.**

2.19.6. NSS TA. Uses SIPRNET Token Management System (TMS) workstation to provide tokens derived from the Certificate Registration Instructions (CRI) provided by the LRA.

2.19.7. CAC PIN Reset (CPR) TA. Supports the Trusted Associate System Manager by acting as a trusted agent to verify positive identification of a CAC PIN reset requestor, in accordance with Defense Manpower Data Center (DMDC) CPR Business Program Policy v2.0. More information regarding CPR, appointments, and roles and responsibilities can be found at https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/CAC%20PIN%20Reset%20(CPR).aspx**.**

Chapter 3

IDENTITY MANAGEMENT

3.1. Introduction. Identity management is the combination of technical systems, policies, and processes to create, define, govern, and synchronize the ownership, utilization, and safeguarding of digital identities. The primary goal of identity management is to establish a trustworthy process of assigning attributes to a digital identity and to connect that identity to a person or NPE in accordance with NIST SP 800-63-3, *Digital Identity Guidelines and DoD policies*.

3.1.1. Identity Assurance Level (IAL) refers to the identity proofing process (**see paragraph 3.3**).

3.1.2. Authenticator Assurance Level (AAL) refers to the authentication process that addresses how an individual can securely authenticate to a CSP to access a digital service or set of digital services.

3.1.3. Federation Assurance Level refers to the strength of an assertion in a federated environment used to communicate authentication and attribute information (if applicable) to an RP.

3.2. Identity. Identity is the set of attributes defining an individual within a given context or environment. The identity associated with an individual or an NPE is used in establishing trust and gaining access to physical or logical cyber resources.

3.2.1. Types of Identities.

3.2.1.1. With regard to PEs, identities are verified via DMDC. When the subscriber builds an identity from a trusted process, the identity meets IAL2. When the subscriber accomplishes the face-to-face requirement, the identity meets IAL3, in accordance with NIST SP 800-63-3.

3.2.1.2. NPE identities are proofed by a system administrator through a documented local process approved by the ISO. When the identity is built via automated method, the identity meets IAL 2. When the administrator is actively involved in building the identity, the identity meets IAL 3, in accordance with NIST SP 800-63-3 and DoD X.509 Certificate Policy.

3.2.2. The primary CSP for a DAF-affiliated person is the DMDC. The DoD CAC, for those eligible, serves as the authoritative assertion of identity and is used as proof of DoD or DAF affiliation, in accordance with DoDI 1000.25, *DoD Personnel Identity Protection (PIP) Program*, and NIST SP 800-63-3. **(T-0).** Ineligible CAC individuals (e.g., retirees, dependents) affiliated with DoD or DAF will use the DMDC as the primary CSP. **(T-0).**

3.2.2.1. Mission partners, temporary employees, volunteers, and FNs that do not have the DMDC as a primary CSP will use an External Certification Authority (ECA) program to issue PKI credentials to prove their identity on the network, in accordance with DoDI 8520.02 and Methods and Procedures Technical Order (MPTO) 00-33A-1300 **(T-0).**

3.2.2.2. For a list of all attributes, see MPTO 00-33D-2001, *AFNET Enterprise Naming Conventions.*

3.2.2.3. Systems shall adhere to DoD CIO memorandum, *Interim Digital Authentication Guidelines for Unclassified and Secret-level DoD Networks and Information Systems*, for specific use cases and exceptions. **(T-0).** Any system or organization that is unable to use DMDC or other DoD approved CSP shall contact ACC HQ CCC/CYX ICAM (**acc.cyss.cyz.pki@us.af.mil**) or AF PKI SPO (**AFPKI.Helpdesk@us.af.mil**) for further guidance. **(T-3).**

3.2.3. DoD personnel in Defense Enrollment Eligibility Reporting System (DEERS)/Real-time Automated Personnel Identification System RAPIDS) are bound to credentials (e.g., CACs, ALTs at IAL3 and AAL3) in accordance with AFI 36-3026V1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, and AFI 36-3026V2, *Common Access Card (CAC)*. All other populations and credentials shall target IAL3 and AAL3. **(T-3).** IAL1 and IAL2 and AAL1 and AAL2 bound credentials are allowed on a case-by-case basis. All non-DoD credentials and binding process requests must be coordinated with ACC HQ CCC ICAM and/or AF PKI SPO. **(T-3).**

3.3. Identity Proofing. Identity proofing is the process of an identity being initially established. This includes both the assigning and documenting of unique attributes, and in the cybersecurity context, establishing an electronic identity or account bound to the subscriber's and NPE-unique attributes, in accordance with AFI 36-3026V1 and AFI 36-3026V2 for DoD connected personnel and NIST SP 800-63-3. Non-unique attributes may also be assigned or gathered at this time but are not part of the identity proofing. The responsibility for assigning and documenting unique attributes may vary by subscriber or NPE type, but the correct binding of the identity attributes to the account is the ultimate responsibility of the ISO. The ISO must ensure that procedures are established and followed to correctly bind attributes to accounts, in accordance with NIST SP 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing Requirements.* **(T-0).**

3.4. Attributes. An attribute is any distinctive feature, characteristic, or property of an object that can be identified or isolated quantitatively or qualitatively by either human or automated means. AFDS provides authoritative identity and attribute management for DAF person entities through an end-to-end life-cycle process that includes generation, provision, maintenance, and termination of individual digital identity records.

3.4.1. Attributes are unique identifiers for individuals (e.g., Electronic Data Interchange Personal Identifier (EDIPI), Federal Agency Smart Credential Number (FASCN), email address, biometrics). Attributes for NPEs (e.g., UID, email address) are provided by its service provider.

3.4.2. Non-unique identifiers or attributes assigned, gathered, and managed can be used to further support authorization and access control decisions (e.g., Air Force Specialty Code, Office, base).

Chapter 4

CREDENTIAL MANAGEMENT

4.1. Introduction. Credential management is the set of practices that an organization uses to issue, track, update, and revoke credentials for identities. A Personal Identity Verification (PIV) credential contains a picture, the issuing agency logo, and cryptographic key pairs used for authentication. Authentication to DAF ISs is performed through a DoD-approved method within DoD and in accordance with NIST standards.

4.1.1. Identity information must be used to ensure strong identification and authentication and eliminate anonymity. **(T-0).** DAF ISs will use only DoD-approved and DAF identity credentials to authenticate entities requesting access to or within DAF information environments. **(T-0).** All information in electronic format will be given an appropriate level of confidentiality, integrity, and availability reflecting the importance of information sharing and protection. **(T-0).**

4.1.2. DAF ISs connect to the DoD Information Network (DoDIN) subnetworks (e.g., NIPRNET, SIPRNET) in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, *Defense Information System Network (DISN) Responsibilities*. **(T-0).**

4.1.3. An IS subscriber is an individual who has access to standalone systems, specialized or functional ISs, enterprise ISs, and/or mission systems.

4.2. Credentialing. All network, system, or application accounts that use DoD-issued or approved PKI, multifactor authentication credentials, or Identity Federation Services (IFS) will be implemented as required by DoD policy. **(T-0).** DoD-issued medium-hardware assurance PKI credentials meet the criteria for IAL-3/AAL-3, in accordance with NIST SP 800-63-3. Other credentials will be validated against NIST SP 800-63-3. **(T-0).**

4.2.1. Strength. The strength of a credential is the measure of its ability to resist unauthorized use. The required strength a credential must have varies according to the classification of the system to be accessed (unclassified or classified), in accordance with NIST SP 800-63-3 and DoDI 8520.03. **(T-0).**

4.2.2. Assurance Levels specify the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

4.2.2.1. DoD PKI certificates are at the medium assurance level, as defined by NIST SP 800-63. **(T-0)**. This is a portable certificate and can be used on any computer with the required utilities and drivers installed**.**

4.2.2.2. Hardware-based certificates are stored on a Federal Information Processing Standard (FIPS) 140-2 Level 2 or higher cryptographic device (e.g. smart token, universal serial bus (USB) device). **(T-0).**

4.2.3. Composition. Credentials contain one or more attributes, often in the form of PKI certificates, that when aggregated, represent the identity of a person or an NPE. **(T-0).**

4.2.4. Authenticators/Tokens.

4.2.4.1. PKI hardware tokens use asymmetric cryptography to identify and authenticate subscribers to systems and networks for the NIPRNET and SIPRNET.

4.2.4.2. An issued token remains the property of the U.S. Government, in accordance with AFI 36-3026V1. **(T-0).** All NIPRNET Tokens shall be returned to the Alternate TA, and SIPRNET tokens shall be returned to an LRA for accountability. CACs are returned to a RAPIDS location. **(T-0).**

4.2.4.3. Expired, unneeded, or found tokens shall be turned in to the nearest RAPIDS facility by the individual, Contracting Officer Representative (COR) for DoD contractors, or Trusted Associate Sponsorship System (TASS) Trusted Agent (TA). **(T-0).**

4.3. Credential Life Cycle.

4.3.1. Credential creation. User credentials will be created by the authorized issuing agency (e.g., DEERS, AF RA) based on specific use cases and access needs. **(T-0).** The credential binds the logical identity with a physical identity through use of registration. Depending on the IAL/AAL level, registration might require face-to-face verification of the individual's identity using a government issued identification, such as the CAC, where a user presents this information to the VO at the DEERS/RAPIDS workstation. Finally, the credential is issued to the user.

4.3.2. Credential maintenance. Credential maintenance is required for the duration of the credential, until it is terminated. **(T-0).** Maintenance of the credential may include reissuance, updates to identity information, or replacement due to compromise.

4.3.3. Credential termination. Credential termination means revoking the credential so that it is no longer used for expressing the logical identity of the user. Termination may be the result of the credential being lost, potential compromise, changes of employment status, or no longer a need by the individual.

4.4. Types of Tokens. Various types of tokens are used for specific purposes to authenticate on the AFIN. A hardware token is a portable, user-controlled, physical device used to generate, store, and protect cryptographic information. They are used to perform encryption and provide 2FA access NIPRNET and SIPRNET, in accordance with DoDI 8520.02. The CAC is the primary hardware token for authenticating individuals for access to NIPRNET assets and physical access to DoD facilities, in accordance with DoDI 8520.02, Department of Defense Manual (DoDM) 1000.13V1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* and AFI 31-101, *Integrated Defense (ID)*.

4.4.1. Hardware Based PKI. Tokens must meet FIPS 140-2, *Security Requirements for Cryptographic Modules*, Level 2.**(T-0)**. Compliance with the FIPS standards include anti-tamper detection, evaluation to Protection Profile at Evaluated Assurance Level 2 or greater, and a secure distribution capability, in accordance with NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*. **(T-0).**

4.4.1.1. The CAC, which meets FIPS 140-2 level 3, provides a cryptographic, certificate-based login identity for NIPRNET that is valid until its expiration.

4.4.1.2. The SIPRNET hardware token, which meets FIPS 140-2 level 2, provides the trusted subscriber identification, authentication, and non-repudiation on SIPRNET, providing improved interoperability across the DoD through PKE applications.

4.4.2. Software-based PKI certificates must be FIPS 140-2 Level 2 compliant. **(T-0).** The DoD PKI provides the ability for issuance of a software-based certificate. Protection of this PKI certificate must be in an approved crypto module**. (T-0).** Software-based PKI certificates are:

4.4.2.1. Used by both Person and Non-Person Entities. **(T-0).**

4.4.2.2. For authentication, digital signature, and encryption.

4.4.2.3. Used by mobile devices when a hardware-based PKI is not feasible.

4.4.3. Other multifactor tokens may include one-time passwords, time-based one-time passwords, biometrics, behavioral analytics, fast identity online or "FIDO" claims, or other technical factors. Approval of other multifactor tokens follow the process outlined in the DoD CIO memorandum, *Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems*.

4.5. CAC token management. DAF ISs and subscribers shall only rely on certificates issued by a DoD or AF PKI (e.g., LTMA, Internal Basic Assurance (IBA)) that are approved for use. **(T-3).** Relying parties will authenticate approved external PKI certificates using either a direct trust mechanism or using a cross-certification mechanism. **(T-3).** All external PKI certificates presented from an approved external PKI must be validated via either download of the PKI certificate revocation list associated with the external PKI or use of an online certificate status protocol (OCSP) query. **(T-3).** The DoD maintains a repository for posting CA certificates and policy object identifiers for approved external PKIs, in accordance with DoDI 8520.02. **(T-3).**

4.5.1. DAF must use TASS for requesting CACs for DoD PKI certificate eligible users. **(T-0).**

4.5.2. TASS allows the following personnel to apply for a CAC or other government credential: affiliated volunteers (requiring DoD Network access), DoD and uniformed service contractors, foreign affiliates, non-DoD civil service employees, non-Federal agency civilian associates, non-US non-appropriated fund employees, outside the Continental US hires, and other Federal agency contractors.

4.5.3. Government sponsors approve the applications for government credentials.

4.5.3.1. Government sponsors of DoD contractor personnel will contact their supporting TASS TA to request an application for an eligible contractor. **(T-3).**

4.5.3.2. The locally appointed TASS TA (e.g., organizational security manager) verifies contractor access against Visit Authorization Requests in the Joint Personnel Adjudication System, ensuring there is a valid contract in the TASS before approving the request for a CAC.

4.5.4. Unfunded contract options annotated in the contract as the period of performance are considered in the determination of the length of contract, (e.g., a contractor hired under DoD contract with a base year plus two option years shall be issued a CAC with a 3-year expiration). **(T-3).** The expiration date of the PKI certificates on the CAC shall match the expiration date on the card. **(T-3).**

4.5.4.1. DoD Contractors contact their unit TASS TA prior to making an appointment with their supporting Military Personnel Section to have their information entered or updated in DEERS.

4.5.4.2. If contract option years are not exercised, the COR notifies the TASS TA to revoke contractor access.

4.5.5. DoD PKI certificate eligible users include authorized DoD volunteers, state, local, or tribal government employees, or interns, as defined in DoDI 8520.02.

4.5.6. The TASS application replaced the Contractor Verification System (CVS) and was designed to replace the paper application process using DD Form 1172-2, *Application for Identification Card/DEERS Enrollment,* in accordance with DoDM 1000.13 and the *Trusted Associate Sponsorship System (TASS) Overview Guide*

4.6. SIPRNET token management . DoD issues SIPRNET Tokens to uniformed services personnel, to include DAF, ANG, AFR. All recipients must be approved by the Office of the Undersecretary of Defense for Personnel and Readiness. **(T-0).**

4.6.1. SIPRNET account users are required to use SIPRNET tokens in accordance with Maintenance Tasking Order (MTO) 2018-283-001, *Two-Factor Authentication (2FA) for Privileged User Accounts.*

4.6.2. SIPRNET tokens are issued by designated LRA personnel.

4.6.3. SIPRNET tokens must be handled in accordance with CNSS-015-2016, *National Security Systems Public Key Infrastructure Member Governing Body* and SAF/CN Memo, *Secure Internet Protocol Routed Network (SIPRNET) Token Guidance*. **(T-0).**

4.6.4. Positive control includes maintaining visual contact when in use and retention or secured on the person when not in use. Only the assigned subscriber is authorized to use the SIPRNET token. **(T-3).**

4.6.4.1. Do not leave the SIPRNET token unattended in computer network resources.

4.6.4.2. Turn in expired, found, or no longer required SIPRNET tokens to the nearest LRA, or COR for DoD Contractors. Do not return the found SIPRNET token back to the individual.

4.6.4.3. If the SIPRNET token is lost or stolen, immediately report this information to the LRA to initiate the revocation process, in accordance with NSS PKI DoD RPS. **(T-0).**

4.6.4.4. Contact the supporting LRA to revoke SIPRNET token certificates when suspected loss of positive control or unauthorized use of the token or a certificate. **(T-3).**

4.6.4.5. Return any token determined to be temporarily out of the positive control of the assigned subscriber to the LRA.

4.6.4.6. Issuance of a new SIPRNET token is authorized after a dated and signed memorandum (wet or digital signature acceptable) on organizational letterhead by the requester's commander authorizing the issuance is provided to the LRA. **(T-3).**

4.6.4.7. When out-processing for a permanent change of station (PCS), SIPRNET tokens must be returned to the LRA. **(T-3).**

4.6.4.7.1. Applies to all personnel with the exception of General Officers (GOs) and Senior Executive Service (SES) personnel.

4.6.4.7.2. GOs and SES personnel who PCS with tokens should notify the losing base LRA. The losing base LRA then:

4.6.4.7.2.1. Changes the site code for the SIPRNET token in TMS.

4.6.4.7.2.2. Notifies the gaining base LRA of the transfer through a digitally signed email.

4.6.4.7.3. Base communications unit updates their section of the base out-processing checklist to ensure that all individuals have contacted their unit's CSS to terminate their SIPRNET account and have turned in their SIPRNET token to the base LRA prior to signing off the individual's Base Out-processing Checklist. **(T-3).**

4.6.4.7.3.1. Upon receipt, LRAs shall reformat the token and store it with other issuance card stock to be reissued. **(T-3).**

4.6.4.7.3.2. Contractors contact their unit's CSS to terminate their SIPRNET account and turn in their SIPRNET tokens to the base LRA at the end of the contract period of performance. **(T-3).**

4.6.4.8. Any subscriber can retain his or her SIPRNET token during a move, while they reside on the same station or base. SIPRNET tokens are required to be turned in when leaving a station or base.

4.6.4.9. Exception or exemption validated circumstances, where a SIPRNET token cannot be used, refer to SIPRNET smart card logon below.

4.7. Virtual Smart Card (VSC).

4.7.1. VSC is a multi-factor technology that emulates the functionality of traditional X.509-based smart cards. Smart card-based PIV cards cannot be readily used with most mobile devices (e.g., smartphones, tablets); however, VSCs use derived PIV Credentials (DPCs), which can be used instead to PIV-enable these devices and provide multifactor authentication for mobile device subscribers.

4.7.2. DPCs are only used on FIPS 140-2, level 2, trusted platform module 1.2 and greater.

4.7.2.1. A DPC is issued for which the corresponding private key is stored in a cryptographic module that is an alternative form factor to the PIV Card. **(T-3).**

4.7.2.2. A DPC shall be issued following verification of the applicant's identity using the PIV authentication key on their existing PIV card by demonstrating possession and control of the related PIV card via the PKI-AUTH authentication mechanism, in accordance with FIPS 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*. **(T-0).**

4.7.2.3. A DPC cannot be used for network logon without the explicit approval of the AF Enterprise AO and the AF CISO. **(T-3).**

4.8. NIPRNET Enterprise Alternate Token System (NEATS). Implemented by the DISA. NEATS Alternate TAs will be appointed at every base. **(T-3).** They will receive token stock, set up a workstation, and issue NEATS tokens to local administrators, Very Important Persons (VIP), group or role sponsors, and end subscribers. **(T-3).**

4.8.1. NEATS Alternate TAs shall be appointed by appointment letter submitted to the AF RA, approved, and trained via DISA web-based training. **(T-3).** Go to the following link for the Alternate TA Designation Letter and Acknowledgement of Responsibilities: **https://intelshare.intelink.gov/sites/usafpki/_layouts/15/start.aspx#/SitePages/Alternate%20Logon%20Token%20(ALT)%20Trusted%20Agents%20(TAs).aspx**; once there, click on the third link for AF Alternate TA Designation Letter and Acknowledgement of Responsibilities.

4.8.2. TAs are required to submit the request for VIP, Group, Code Signing, and Role sponsor to ACC HQ CCC/CYX ICAM

(**https://cs2.eis.af.mil/sites/13015/_layouts/15/start.aspx#/SitePages/Home.aspx**), to begin the process for NEATS token issuance.

4.8.3. The NEATS Alternate TA shall be assigned permissions to register and issue NEATS tokens for administrator and personal user accounts. **(T-3).**

4.9. Role Based Attribute Authority (RBAA). The commander or director of the organization no lower than Division Chief in the grade of Lieutenant Colonel (O-5), or in small detachments, the Unit/Organizational Commander. He or she is responsible for requesting a group or role certificate.

4.9.1. Appoints the PKI sponsor to receive either group or role certificate. Go to: **https://intelshare.intelink.gov/sites/usaf-pki/ReferenceDocs/CI-09-03-002_Role-Based_Certificate_Request_Procedures_v1.3.0.pdf**; open the standard operating procedure, then go to Appendix A for the appointment letter template.

4.9.2. Validates the need for a certificate and then requests the certificate.

4.9.3. Provides the AF RA the necessary information for the creation of the group and role certificates. Each distinguished name (DN) must be unique within DAF domains. **(T-3).**

4.9.4. The RBAA is the verifying official (VO) for group tokens in accordance with DoD PKI RA/LRA CPS and the NSS PKI DoD RPS.

4.10. PKI Sponsors. A subscriber representing and managing role-based certificates (e.g., organizational email account, mobile code signing) or NPEs (e.g., workstations, IT systems, applications, physical or virtual devices requiring authentication). More information is available regarding sponsor training and roles and responsibilities at **https://intelshare.intelink.gov/sites/usafpki/_layouts/15/start.aspx#/SitePages/Help%20and%20Training%20for%20Organizational%20E-Mail%20Account%20Sponsors.aspx**.

4.10.1. Appointed by the RBAA. Go to **https://intelshare.intelink.gov/sites/usaf-pki/ReferenceDocs/CI-09-03-002_Role-Based_Certificate_Request_Procedures_v1.3.0.pdf**; open the Standard Operating Procedure, then go to Appendix A for the appointment letter template.

4.10.2. Appoints a new sponsor before departing the command, or the certificate will be marked as compromised and revoked. **(T-3).**

4.10.3. Manages certificates in accordance with CNSSI 1300 and NSS PKI DoD RPS.

4.10.4. Keeps a list of applicable personnel up to date and sends updated copies to the LRA. Go to **https://intelshare.intelink.gov/sites/usaf-pki/ReferenceDocs/CI-09-03-002_Role-**

Based_Certificate_Request_Procedures_v1.3.0.pdf; open the Standard Operating Procedure, then go to Appendix C to obtain the list of applicable personnel template.

4.10.5. Responsible for the installation and use of the certificate once it has been created.

Chapter 5

ACCESS MANAGEMENT

5.1. Introduction. Access management covers subscribers' authentication and authorization to a relying party, providing verification and ensuring non-repudiation. DAF authentication will align and comply with the Deputy Secretary of Defense DoD Cybersecurity Discipline Implementation Plan, DoD cybersecurity policies and privilege management initiatives, in accordance with DoDI 8520.03 and NIST SP 800-63B. **(T-0).**

5.1.1. Subscriber. Subscribers are entities defined by their affiliation within the DoD. Common affiliations include: Uniformed Service Members, DoD Civilians, Contractor Employees, Foreign Nationals (FNs), NPEs, and Organizational Roles.

5.1.1.1. Entities (e.g., role, person, equipment) must possess an attribute to be bonded and allowed to be identified, verified, and authenticated for access. **(T-0).** System or device subscribers will use system or device authenticators containing a unique system or device identifier as the subject and are responsible for maintaining and managing access to the activation key, code, or token associated with the authenticator. **(T-0).**

5.1.1.2. Credential Responsibilities. Identities are critical to securing network traffic. Tokens are used to store credentials by definition. The subscriber must possess and control assigned tokens at all times. **(T-0).**

5.1.1.2.1. Once the token is activated and in-use, it must not be left unattended at any time. **(T-0).** All active tokens must be secured when not in use. **(T-0).**

5.1.1.2.2. After use, the token must be deactivated with a manual logoff in accordance with DoD X.509 *Certificate Policy v10.6,* Section 6.2.9. **(T-0).**

5.1.2. Relying Party (RP). An entity that relies upon the subscriber's authenticator(s) and credentials, or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system. Examples of an RP include websites or applications where a subscriber must be authenticated using digital certificates before granting access. **(T-0).** This includes the AF Portal where the AF Portal is the RP the subscriber is requesting access using the authentication certificate to validate his or her digital identity. In the case of network logon, the Domain Controller is the RP.

5.1.2.1. Devices can be both an RP and a subscriber when in a device-to-device communication session.

5.1.2.2. Applications like Outlook™ or Adobe™ also act as an RP when validating digital signatures of emails and forms to verify the digital certificate is valid in accordance with X.509 Certificate Policy. **(T-0).**

5.1.3. Authentication is the process used to confirm a claimed identity, through the use of a valid credential during identity proofing in accordance with DoDI 8520.03, for unclassified systems. All DAF relying parties are required to authenticate using certificates by approved credentials in accordance with NIST SP 800-63-3 and DoDI 8500.01. **(T-0).**

5.1.4. Authorization is the enforcement of access policies to ensure that the correct individuals and entities are granted access to only the resources and information that they require and for

which they possess the requisite permissions (or attributes). Authorization is often done directly through compliance with local policy governing the resource or indirectly through a separate authorization service, which is sometimes termed a "policy decision point." Typically, decisions involve some type of lookup of the requester's identity attribute data or use of local access control lists. Decisions may depend upon an individual's role (e.g., system administrator, database administrator) or the permissions and attributes associated with a specific group. Access to DAF ISs is a revocable privilege and is granted to individuals based on need to know and in accordance with CJCSI 6211.02D, CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)* and National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 200, *National Policy on Controlled Access Protection*.

5.2. Authentication. The authentication of subscribers and the granting of logical and physical access is a combination of enterprise-wide and local functions (e.g., DEERS, global directory services, or DoD PKI services) in real-time whenever possible in accordance with DoDI 1000.25, DoD 5200.08-R, *Physical Security Program*, DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, DoDI 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)*, DoDI 8500.01, and DoDI 8520.03. **(T-3).**

5.2.1. Factors. Authentication Factors fall within three categories, knowledge, possession, and inherence. Multiple categories combined form the basis of a multi-factor authentication process. This process is to ensure a stronger, more secure method of authenticating an identity.

5.2.1.1. Knowledge is something known (e.g., username/password, PIN).

5.2.1.2. Possession is something physical a PE has (e.g., smart token).

5.2.1.3. Inherence is a biological trait an entity has (e.g., fingerprint).

5.2.1.4. Biometrics. A biometric identifier (e.g., a fingerprint, an iris scan, or a hand geometry template) registered in a DoD-approved authoritative source that is used as an enabler (e.g., as one factor of an approved multi-factor identity authentication process) enhances strength of the identity credentials. For additional information and management processes refer to DoD Directive (DoDD) 8521.01E, *DoD Biometrics*, DoDI 8520.03 and AFI 33-332, *Air Force Privacy and Civil Liberties Program* unless otherwise specified by Defense Forensics and Biometrics Agency.

5.2.2. Process.

5.2.2.1. PE Authentication. For person authentication, all subscribers will have an AAL-2 or AAL-3 authenticator in accordance with NIST SP 800-63-3. **(T-3).**

5.2.2.2. NPE Authentication. Authentication of NPEs is accomplished by securely-installed DoD-approved PKI digital certificates whenever possible. Alternate certificates types must be approved by CISO. **(T-0).**

5.3. IS Access. Requests for access to resources located on the AFIN are vetted through identity and authentication steps prior to receiving an authorization decision. Follow guidance in **paragraph 4.2** to obtain a token prior to being granted access. **(T-3).**

5.3.1. Authorized access to DAF resources.

5.3.1.1. CAC eligible subscriber. Individuals eligible for CACs are identified in accordance with DoDM 1000.13. Individuals will be issued a separate CAC for each persona (e.g., DoD uniformed and civilian personnel and eligible contractors; DoD volunteers or interns; selected reserve personnel; executive department and agency personnel; ANG members; state or local or tribal government employees; foreign government and foreign organization personnel, and foreign contractors) in accordance with DoDI 8520.02, AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, DoDI 8520.03, CJCSI 6510.01F, and DoD 8570.01-M, *IA Workforce Improvement Program*. **(T-0).**

5.3.1.1.1. Dual-role personnel have more than one role or persona (e.g., civilian and reservist, contractor and ANG); the individual is required to have and use the appropriate CAC for each role.

5.3.1.1.2. System and application owners must make a decision if the information the individual is accessing is restricted by the persona expressed in the certificate. **(T-3).** Some applications must ensure that the correct persona is used to authenticate personnel with dual persona roles (e.g., Reservist persona for military related actions, or Contractor persona for contract related actions) **(T-3).**

5.3.1.2. Applications can use information in the credential provided (Federal Agency Personal Identifier in the User Principal Name of the PIV cert) or the application can establish an information exchange with a DoD approved identity provider.

5.3.2. Temporary and volunteer access.

5.3.2.1. Grant only unclassified IS access to temporary employees and volunteer personnel in support of their assigned duties in accordance with AFI 36-3026V2.

5.3.2.2. Individuals (including key spouses) authorized to be DoD temporary and/or volunteer must meet access requirements in accordance with AFI 36-3026V2. **(T-3).**

5.3.3. Mission Partners, (e.g., Five Eyes, allies, coalition partners) the ISO shall establish procedures for assigning or determining the unique attribute to use and for securely binding the attribute to the account. **(T-3).** This attribute must be included on an authorized PKI credential or an authorized token in accordance with DoDI 8520.02, and MPTO 00-33A-1300, *SIPRNET Releasable (SIPR REL) Enclave Implementation Core Service*. **(T-0).**

5.3.4. Non-DoD individuals and organizations that support or are supported by DoD missions and operations. Mission partners include allies, coalition partners, host nations, international and multinational organizations, civilian government agencies and departments (Federal, State, local, and tribal), law enforcement agencies, non-governmental agencies and organizations (private volunteer organizations, commercial businesses, academic institutions, etc.), and other non-adversaries in accordance with DoDI 8520.02.

5.3.5. Foreign National (FN)/Local National (LN).

5.3.5.1. WCOs consult the Host or MAJCOM foreign disclosure officer and applicable ISSM before authorizing access by FN or LN subscribers to ISs processing, storing, or transmitting classified and controlled unclassified information (CUI), in accordance with AFMAN 17-1301, MPTO 00-33A-1301, *Foreign National NIPRNET Access Core Service*, MPTO 00-33A-1202, *Air Force Network Account Management*, MPTO 00-33D-2001, AFI

16-107, *Military Personnel Exchange Program*, DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and DoDD 5230.20, *Visits and Assignments of Foreign Nationals*. **(T-0).**

5.3.5.2. Pursuant to applicable host-nation agreements, FN or LN privileged subscribers are certified to access the baseline computing environment. If privileged access is required to an IS, restrict FN or LN subscriber access to Information Assurance Technical I/II level positions and only under the immediate supervision of a United States (US) citizen. **(T-3).** Furthermore, document access in the IS security assessment package in accordance with AFMAN 17-1301.

5.3.5.3. Sanitize or configure classified ISs to restrict access by FNs or LNs to only classified information authorized for disclosure to the FNs or LNs government or coalition, as necessary to fulfill the terms of their assignments in accordance with applicable host MAJCOM foreign disclosure officer requirements.

5.3.5.4. FNs or LNs requiring system access must use PKI access methods in accordance with DoDI 8520.03 and CJCSI 6510.01F. **(T-0).** The application and data the FN or LN is accessing must be approved for release to the country of the FN/LN. **(T-0).** If a system cannot accept a PKI certificate, follow guidance for other approved two-factor authentication capabilities for establishing the identity of the FN and/or LN.

5.3.5.5. Non-US citizens, who are permanent legal residents, are required to meet the same requirements of any US citizen for access to the unclassified network or system. **(T-0).**

5.4. Authorization.

5.4.1. Authorized User. An authorized user is any appropriately cleared individual required to access a DoD IS to carry out or assist in a lawful and authorized governmental function. The DCSA Position Designation Tool may be used to determine the position sensitivity and corresponding investigative requirement in accordance with DoDI 1400.25V731, *DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees*. Configure authorized user account creation and administration, consult Executive Order (EO) 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust*, for investigation requirements. **(T-0).**

5.4.2. Non-Privileged. Also known as subscribers requiring basic access to unclassified and classified IS based on the assigned duties. Non-privileged subscribers authenticate with an authenticator that meets the proper AAL/IAL combo, depending on the information being accessed.

5.4.3. Privileged. Authorized (and, therefore, trusted) to perform functions on an unclassified and classified IS based on the assigned duties and the Automated Information System position-certified, in accordance with DoDM 5200.02_AFMAN16-1405, *Air Force Personnel Security Program*, DoD 8570.01-M, and AFMAN 17-1303. Privileged subscribers are required to authenticate with a hardware-based PKI credential or via IFS method (**see paragraph 4.2**). **(T-3).** Privileged subscribers are separated into a tier system, in accordance with DoDD 5205.16, *The DoD Insider Threat Program.*

5.4.3.1. Tier 1 is the lowest level of privileged access and network rights. Includes subscribers who service and maintain single endpoint devices; cannot access or modify networks; can install software; can modify network settings; and enable or disable services on individual computers. Tier 1 privileged subscribers include local-system administrators and client support team members.

5.4.3.2. Tier 2 includes subscribers who can access more than the local system but have restrictions and are generally responsible for upgrading, installing, or repairing systems. Tier 2 privileged subscribers include most AFNET administrators who have an administrator account and subscribers who have the responsibility to secure information systems.

5.4.3.3. Tier 3 includes individuals who have access rights across most areas of the infrastructure. Members of this group often have full administrative control of domains within the enterprise. Tier 3 privileged subscribers include domain administrators, enterprise administrators, and network administrators.

5.4.4. Required Documentation. The DAF is moving toward an automated account provisioning process. The process uses attributes managed by the enterprise attribute manager, and authorization is enforced through the service provider. It remains the service provider's or relying party's responsibility for which attributes ensure proper authorization occurs.

5.4.4.1. When required by the ISO for IS access, in accordance with *Title 10 United States Code Section 9013,* AFI 33-332, and EO 9397, *Numbering System for Federal Accounts Relating to Individual Persons,* users of all authorized DAF information system devices (to include mobile computing devices) the CSS or ISSO will ensure:

5.4.4.1.1. Users sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision,* prior to initial access. **(T-3).**

5.4.4.1.2. Users complete Cyber Awareness Challenge training prior to being granted access to an IS. **(T-0).** Subscribers must re-accomplish Cyber Awareness Challenge training annually; organizations maintain compliance in accordance with DoD 8570.01-M. **(T-0).**

5.4.4.1.3. Failure to complete annual Cyber Awareness Challenge training results in immediate suspension of access to unclassified and classified information systems. **(T-0).** Access can be restored upon satisfying the annual retraining requirement, in accordance with DoD 8570.01-M. **(T-0).**

5.4.4.1.4. If an individual violates the information system terms of use, commanders should consider suspending access pending re-accomplishment of Cyber Awareness Challenge training. Violations identified by the AFNET Mission Assurance Center result in automatic account suspension. Additional restrictions on reinstatements for classified information systems are determined locally and should follow the guidelines of DoD 8570.01-M.

5.4.4.2. DD Form 2875, *System Authorization Access Request (SAAR),* is completed and digitally signed by the user. The Government sponsor verifies the justification and need for access and digitally signs the form before routing to the Security Manager. The Security Manager performs a security clearance and background investigation verification and

digitally signs the form before routing for account creation, in accordance with DoDM 5200.02_AFMAN 16-1405 and AFMAN17-1301.

5.4.4.2.1. Original DD Forms 2875 for unprivileged AFNET accounts may be transferred when duty assignments change. The gaining unit may use local methods to update duty information in the Information Assurance Officer (IAO) Express tool and shared drive access requirements. The losing unit ensures termination of shared drive access prior to user's out-processing. **(T-3).**

5.4.4.2.2. Changes to privileged account access requirements require a new account access request. **(T-3).**

5.4.4.2.2.1. Re-accomplish the account request for AFNET-Secured Internet Protocol Network (SIPRNET) (AFNET-S) accounts when access requirements change (e.g., duty position, permanent change of station). **(T-3).**

5.5. Account Management.

5.5.1. Manage all subscriber accounts using applicable system configuration management guidance; follow Technical Orders (TOs) published by DAF (e.g., MPTO 00-33B-5006, MPTO 00-33A-1202 for AFNET accounts) and the applicable DoD Security Technical Implementation Guides (STIGs) (e.g., enclave, application security, operating system, database). **(T-3).**

5.5.2. Account Provisioning. Logically moving a new subscriber account from the placeholder Organizational Unit (OU) to the requested Base OU in the AFNET. Enables the new account, and if the CSS requests, provides the account email.

5.5.2.1. Contact the Unit CSS to provision the new account.

5.5.2.2. CSS provisions account via IAO Express Tier Zero.

5.5.3. Password management.

5.5.3.1. Specific procedural information for password management is provided in DoD STIGs and PIN management requirements in accordance with DoD PKI RA/LRA CPS.

5.5.3.2. USCYBERCOM tasking order password requirements take precedence only if more restrictive than guidance in this publication.

5.5.3.3. Unauthorized sharing of passwords/PINs is a security incident, in accordance with CJCSI 6510.01F.

5.5.3.4. In the event of a compromised password/PIN, the ISO and the ISSM ensure procedures are in place to implement immediate password/PIN change activities. **(T-3).** A compromised PKI PIN warrants probable compromise of the associated certificates.

5.5.4. Pin management. All NIPRNET and SIPRNET DoD ISs and Directory Service domains and domain-joined computers, per local security policy, are required to be configured for PIN caching, set to 10 minutes. **(T-3).**

5.5.5. Loss of Access. Access to a DAF IS is a privilege, and continued access is contingent on personnel actions, changes in need to know, or operational necessity, in accordance with CJCSI 6510.01F.

5.5.5.1. Actions that threaten or damage DAF ISs can result in immediate suspension of access to unclassified and classified ISs.

5.5.5.2. If an individual's clearance is suspended, denied, or revoked, immediately suspend access to classified information systems. **(T-3).** Commanders review circumstances surrounding the suspension, denial, or revocation to determine if continued access to unclassified systems is warranted and if revocation of the hardware token is required. Commanders may provide recommendations regarding user access to the ISO.

5.5.6. Subscriber account. Also known as user accounts, require basic access to unclassified and classified ISs based on the assigned duties. A subscriber account is established for a single named individual based on his or her identity and access needs. AFNET accounts are created through an automated method by AFDS based on information obtained by DMDC. Applications generate the accounts in an automated method when possible. **(T-3).**

5.5.7. Group Account. A special case account where more than one person can simultaneously access the same account using a DoD-approved PKI credential, in accordance with DoDI 8520.02. Tier-1 ALT (NIPRNET) and VIP ALT (SIPRNET) are for Flag Officers or SES personnel only. The AO is the approving authority for group accounts, in accordance with CJCSI 6510.01F and DoDI 8520.02. The AO approval letter must be part of the system or enclave authorization package. **(T-3).** Approval authority for group accounts is identified in the boundary specific IT inventory spreadsheets at **https://usaf.dps.mil/sites/10440/InfoAcc/SitePages/Home.aspx**.

5.5.7.1. Executive staff support personnel use ALTs to log on to the executive's network account to perform system testing, workstation configuration, read and answer routine email on behalf of the executive.

5.5.7.2. ALTs have unique identifiers that do not allow the staff support personnel to digitally impersonate the Executive.

5.5.7.3. Request a group account via email to ACC HQ CCC/CYZ ICAM at **acc.cyss.cyz.pki@us.af.mil**.

5.5.8. Role Account. A role account is used in control center or similar positions, assigned to the particular position, not to an individual, to fulfil the mission requirements. The mission continues, without interruption, during personnel changes (e.g., shift changes, swap-outs). A role account is issued to an individual authorized to fill a specific organizational role or function and does not contain the individual's name. Role certificates are the credentials which role account users use to authenticate.

5.5.8.1. One individual accesses the account at a time. Identity control and monitoring is maintained by the individual in charge through assignment of individuals and tracked with a log. The mission continues, without interruption, during personnel changes (e.g., shift changes, swap-outs).

5.5.8.2. Each person would access the organizational email mailbox for any email requirement (e.g., Air Operation Center stations, Command Center stations, information displays and Remotely Piloted Aircraft positions).

5.5.8.3. Request a role account via email to ACC HQ CCC/CYZ ICAM at **acc.cyss.cyz.pki@us.af.mil**.

5.5.9. Administrative Account. An information system account which is used by a privileged subscriber to install and maintain an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established cybersecurity policy and procedures. AFNET accounts must always designate an administrative account using ".ad+Level Code" at the end of the account name in accordance with MPTO 00-33D-2001. **(T-0).**

5.5.10. Service Account. A service account is used in a system-to-system or application-to-system process to provide "ownership" of a process or system service. Any account without interactive login that is for device-to-device; system-to-system; system-to-device; or system-to application authentication is considered a service account. Service account passwords must be changed at a minimum every 60 days per AD STIG. **(T-0).**

5.5.10.1. All AFNET Enterprise Service/Application Accounts will follow MPTO 00-33D-2001; all other Service/Application Accounts will have their own naming convention or follow MPTO 00-33D-2001. **(T-3).**

5.5.10.2. A service account belongs to the operating system or application instead of an administrator or end user (individual). Such an account is forbidden to be used for interactive login. **(T-3).** All connectivity to other systems or applications should be blocked. **(T-3).**

5.5.10.3. Passwords shall be created that will restrict human interaction. **(T-3).** All external connectivity not defined in the service account approval must be logically blocked. **(T-3).** Each service account must be identified in the Enclave/System Assessment and Authorization package. **(T-3).** Interactive logon is prohibited for any Directory Services Service Account; the use of smart tokens for logon is not possible. **(T-3).**

5.5.10.4. Service accounts are not just applicable to the Windows™ Server environment, but are also used in UNIX/Linux™, Mac OS™, CISCO™, IBM™, and others. Other related terms are "system account", "system process owner", "computer/machine account", and "application account". Each account is created to provide services which include, Active Directory™ Connector or Microsoft™ SQL Server Express; other Windows™ Services on Windows™ Servers; Oracle Database™ services; UNIX system™ services: UNIX Spooler account, process scheduler; etc. Service accounts can be a non-domain joined system to or from a domain joined system.

5.5.10.5. ACC HQ CCC/CYX ICAM validates the intended use of service accounts via the change management process with Remedy change requests.

5.5.11. Organizational electronic mailbox. Disable DS objects that are associated with organizational mailboxes. **Note:** Organizational mailboxes and organizational accounts are two different capabilities and are not related.

5.5.11.1. The organizational mailbox manager grants access from the actual organizational mailbox. The organizational mailbox manager is the person whose name appears in DS as the manager. Use IAO Express to add or change the organizational mailbox manager in DS/Exchange.

5.5.11.2. The sponsor appointed for the organizational mailbox manages the associated encryption certificate. The sponsor is the person who requests, issues, and manages the

encryption certificate. The organizational mailbox sponsor will follow the procedures for managing the organizational mailbox encryption certificate found on the AF PKI SPO website. **(T-3).** (**https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/AF%20Public%20Key%20Infrastructure%20System%20Program%20Office.aspx**).

5.5.11.3. Encryption certificates for organizational email mailboxes, to include portable electronic devices (PEDs), must have a designated sponsor appointed in writing using the template available on the AF PKI SPO website. **(T-3).** Go to: **https://intelshare.intelink.gov/sites/usaf-pki/ReferenceDocs/** browse for CI-09-03-002_Role-Based_Certificate_Request_Procedures_v1.3.0.pdf and open it; once the Standard Operating Procedure is open, go to Appendix A for the appointment letter template. The AF RA or LRA, as appropriate, will maintain a file of requirement validation documentation. **(T-3).** For organizational email mailboxes on PEDs, follow the appropriate DoD STIG. For additional guidance, consult the *DoD PKI Registration Authority/Local Registration Authority Certification Practice Statement* (RA/LRA CPS) which can be found under the Resources/Policy tab of the AF PKI System Program Office website at (**https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/AF%20Public%20Key%20Infrastructure%20System%20Program%20Office.aspx**).

5.5.12. System/Enclave ISSM is responsible for requesting the removal of any stale or not required accounts in accordance with CJCSI 6510.01F. **(T-3).**

5.6. Account Life Cycle. The full life cycle of identity and access for a subscriber on a given system.

5.6.1. Creation. For subscriber accounts, AFDS enables discovery of new identities from DMDC, DAF Human resource systems and other authoritative sources. The identity may be augmented with data from additional authoritative sources and an account created in a subscriber management system. AFDS establishes new account upon CAC issue via a data driven process initiated by DMDC. Group, Executive Support Staff, Role, Admin Service and Organizational mailbox accounts follow the established procedures and document requirements in the previous sections. These accounts are only activated once all documents are completed and signed by the user, sponsor and supervisor and sent to ACC HQ CCC/CYX ICAM for processing.

5.6.2. Maintenance. Unique attributes within a local context generally do not change over time, with minor exceptions such as name changes for both PEs and NPEs. For PEs, non-unique attributes may change occasionally or even frequently, (e.g., office symbols, phone numbers, rank, positions). ISOs shall establish procedures for maintaining and updating any locally gathered or assigned attributes and also designates acceptable sources such as AFDS for externally managed PE attributes. **(T-3).** AFDS obtains updated information from authoritative data sources and replicates that data to the AFNET for subscriber accounts. If an individual identifies errors in the data, a help desk ticket is generated for resolution. All other accounts require a help desk ticket for account maintenance.

5.6.3. Termination. For subscriber accounts, AFDS detects removal of identities from DMDC and initiates the decommissioning process of the digital identity of a PE. This initiation may

cascade to account removal in subscriber management systems. Sponsors of all other account types should request account termination when the account is no longer required.

5.7. Access Control. Access control is the resulting convergence of identity management, credential management, authentication, and authorization. Access control represents enforcement of the authorization decision and is often referred to as the policy enforcement point. Methods and mechanisms are used to restrict physical and logical access based on verified identity, valid credentials, and policies governing the accessibility of a given resource. Attributes required for access to a resource must be allocated to subscribers as part of the identity account provisioning process based on a policy of least privilege as well as need-to-know. **(T-3).**

5.7.1. Physical Access. DoD IS, DoD networks or DoD facilities shall authenticate all entities prior to granting access. **(T-0).** DAF installations and facilities shall utilize a DoD PIV credential (e.g., CAC) for personal identification and authentication to Physical Access Control Systems (PACS) in accordance with NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS).* **(T-0).**

5.7.1.1. The identifier is the Cardholder Unique Identifier.

5.7.1.2. Any new DAF PACS procurements require the use of the DoD CAC (Contactless or Chip+PIN) exclusively in accordance with DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control*. **(T-0).**

5.7.2. Logical Access. Access to an IT network, system, service, or application. DoD IS or DoD networks hosting information not previously approved for public release shall authenticate all entities prior to granting access in accordance with DoDD 5230.09, *Clearance of DoD Information for Public Release* and DoDI 5230.29, *Security and Policy Review of DoD Information for Public Release.* **(T-0).**

5.7.2.1. For network authentication, enable all unclassified networks to use tokens, (AAL-2 or AAL-3), DoD PKI certificate-based authentication, and set authorized subscriber accounts to require smart card logon by selecting, "Smart card is required for Interactive Logon," in Windows™ AD environments.

5.7.2.2. Primary identifier for logical access shall be the EDIPI which can be represented in various ways such as the user principal name in the PIV certificate for active directory smart token logon or the distinguished name for authentication to non-windows systems. **(T-3).** Other identifiers shall not be used without approval by the SAF/CN CTO or SAF/CNZ CISO in cases where the aforementioned methods are technically infeasible except for Systems specifically exempted from PKI and two-factor authentication, **see paragraph 1.3.1**. **(T-3).**

5.7.3. Role-Based Access Control or Attribute Based Access Control. Either are acceptable as long as the attributes come from an authorized source (e.g., AFDS, AFNET AD).

5.7.3.1. Method used within DoDIN for administering an Access Control List. It provides an authorization mechanism that links rights and privileges with subscriber roles, which correspond to job functions within the enterprise.

5.7.3.1.1. Roles are defined based on job functions, instead of individual member accounts and groups.

5.7.3.1.2. Permissions are defined based on job authority and responsibilities within a job function.

5.7.3.1.3. Operations on an object are invocated based on the permissions.

5.7.3.1.4. Object is concerned with the subscriber's role and not the subscriber.

5.7.3.2. Targets different levels of a system or application to provide any degree of access control that is necessary.

5.7.4. Attribute-Based Access Control (ABAC).

5.7.4.1. Logical access control methodology where authorization is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environmental conditions against policy, rules, or relationships that describe the allowable operations in accordance with NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*.

5.7.4.2. Enterprise ABAC allows applications and devices within the DoD to support current and emerging identity and access management requirements in a standards-based manner in accordance with NIST SP 800-162.

5.7.4.3. Enterprise ABAC allows organizations to meet the requirements of NIST SP 800-63-3, *Digital Identity Guidelines*, while simultaneously providing the capability to grant and deny access to resources based on current access policy, resource and subscriber security attributes, and threat conditions in accordance with NIST SP 800-162.

5.8. Accountability. Components used for tracing (e.g., event monitoring, auditing, logging and reporting) an entities (PE/NPE) actions on a system, back to the unique entity will ensure non-repudiation. **(T-3).** These components, while not an ICAM-specific capability, enable accountability across ICAM.

Chapter 6

CERTIFICATE MANAGEMENT

6.1. Introduction . The AF ensures its internal PKI CAs and the digital certificates they issue are trustworthy using the trust governance method. It also ensures external roots and associated certificates can be trusted by AF relying parties. The process of trusting a PKI involves the acceptance of its root (also known as a Trust Anchor) certificate and placing it in a trust store. The enterprise certificate trust governance process exists to manage the baseline and provide a formal means to add and remove roots at the enterprise level. AF ISs and subscribers shall only rely on certificates issued by a DoD and/or AF PKI that are approved for use. **(T-3).** Relying parties authenticate approved external PKI certificates using either a direct trust mechanism or cross-certification mechanism. All external PKI certificates presented from an approved external PKI must be validated via either download of the PKI certificate revocation list associated with the external PKI or use of an on-line certificate status protocol query. **(T-3).** The DoD maintains a repository for posting CA certificates and policy object identifiers for approved external PKIs.

6.2. Identity credential strength determination . The ISO will determine the "Credential Strength" used to authenticate to the DoD IS by assessing the "Sensitivity Level" of the information contained in the DoD IS in accordance with DoDI 8500.01 and DoDI 8520.03. **(T-0).**

6.3. Type of certificates.

6.3.1. NPE. Provide the capability to set up secure communications between relying parties and devices, prevent the connection of unauthorized devices to the Department's networks, and secure existing connections between network devices.

6.3.1.1. All private AF Web servers must be issued a DoD X.509 PKI Server certificate. **(T-3).** 6.3.1.2 A server certificate must be reissued when the fully qualified domain name for the server changes or after three years. **(T-3).**

6.3.2. DoD. These certificates are required for external facing AF server and domains and are issued by the AF RA.

6.3.3. DAF. These certificates are allowed for internal facing AF server (e.g., web servers, domain name servers), issued by the AF LTMA Sub-CA on NIPRNET.

6.3.4. Mobile code signing certificate. Code signing and mobile code certificates are specially formatted certificates used for digitally signing executable program code in any number of languages or formats. The code signing certificate binds the identity attributes of the owning organization and the hash of the executable code to the credential to provide assurance that the code has not been altered during distribution.

6.3.4.1. Code signing attribute authority (CSAA) is authorized to appoint individuals to receive and use code-signing certificates.

6.3.4.2. For the AF Developer's Guide for Obtaining DoD Code Signing Certificates and additional guidance, go to the AF PKI website **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/Mobile%20Code%20and%20Code%20Signing%20Certificates.aspx**.

6.3.4.3. The CSAA ensures that code-signing designations are kept to a minimum consistent with operational requirements.

6.3.4.4. The ISSM annotates compliance in the enclave or system authorization package. The code signing and/or mobile code certificates are approved for use by the AF AO.

6.4. Online certificate status protocol (OCSP). Primary method used in the DoD to validate certificate revocation statuses. The DoD's Robust Certificate Validation Service provides this capability on both NIPRNET and SIPRNET enclaves. **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/Certificate%20Validation.aspx**.

6.5. Certificate reissuance prior to expiration. Certificate sponsors (owners) needing continued PKI services can request reissue of their certificates no earlier than 60 days prior to the certificate expiration date in order to prevent disruption in service, and to alleviate not having to process a certificate revocation. Reissuance is not allowed prior to 60 days before expiration without the current certificate being revoked first. **(T-3).** Reissue a server certificate when the fully qualified domain name for the server changes or after three years.

6.6. Certificate Revocation.

6.6.1. Certificate revocation is necessary to terminate a certificate's use before its normal expiration date. Examples of reasons for revocations include private key compromise (e.g., lost or stolen token), loss of trust in a subscriber, changes in a subscriber's legal name, or departure from the DoD. Examples of reasons for NPE device certificate revocation are (e.g., changes to IP, loss of private key, compromise or, for Domain Controllers, a rebuild of the device).

6.6.2. The request must be submitted in a digitally signed email to the AF RA/\LRA/TA. **(T-3).**

6.6.2.1. Revoke certificates suspected of key compromise within 24 hours or the next duty day (whichever is first) after notification. **(T-3).**

6.6.2.2. Enter the revoked certificates into a DoD CRL. All applications (e.g., web sites) must check validity (e.g., the trust path, expiration, and revocation status) before granting access. **(T-3).**

6.6.2.3. CAs are responsible for indicating the revocation status of the certificates they issue. **(T-3).** Revocation status information is provided using the OCSP, CRLs, or some other mechanism in accordance with Internet X.509 PKI Certificate and CRL Profile, Request for Comments (RFC) 5280, DOI 10.17487/RFC5280, **https://doi.org/10.17487/RFC5280**.

6.7. Revocation Repositories. A system or collection of distributed systems that stores certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

6.8. Certificate management on Mobile Technology.

6.8.1. For appropriate use of mobile devices see **https://cs2.eis.af.mil/sites/10060/Wiki/Commercial%20Mobile%20Devices.aspx**.

6.8.2. Each MAJCOM must maintain a list of all subscribers that have installed derived certificates in the event of device loss, theft or compromise. **(T-3).**

6.8.3. ISSMs ensure all devices are configured with an approved token reader or have AF AO-approval to use software certificates in accordance with the *DoD Commercial Mobile Device (CMD) Policy STIG*. **(T-0).**

6.8.4. Derived Credentials.

6.8.4.1. A Derived PIV Credential is an additional X.509 certificate, issued in accordance with the requirements specified in the NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* and DoD *Interim Guidance on the Use of DoD Personal Identity Verification Derived PKI Credentials on Unclassified Commercial Mobile Devices.* When the PIV authentication certificate on an applicant's PIV Card, it serves as an additional common identity credential under Homeland Security Presidential Directive (HSPD) 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* and FIPS 201-2, and is used with mobile devices.

6.8.4.2. The PIV cardholder may request a derived PIV credential.

6.8.4.3. Derived credentials cannot be stored on workstations. **(T-3).** They must be deleted after issuance to the subscriber. **(T-3).**

6.8.4.4. In the event of device loss, theft or compromise, subscriber shall follow all current incident/loss processes and inform their LRA or TA to revoke all the derived credentials. **(T-3).**

6.8.4.5. Purebred. A key management interface for DoD PKI to distribute device and derived subscriber credentials over the air to CMD. More information can be found at **https://iase.disa.mil/pki-pke/Pages/purebred.aspx**.

6.8.4.5.1. Securely issues approved CMD DoD PKI device certificates and allows DoD PKI subscribers to request and receive subscriber credentials onto their CMDs.

6.8.4.5.2. Purebred Agent. Purebred Agent performs the necessary steps to establish cryptographic keys that can be used to authenticate the device and encrypt configuration data for use by the device.

6.8.5. CMD. PKI credential storage and use on classified CMDs is not authorized.

6.8.5.1. The *DoD Mobile Policy STIG* prohibits the use of personally owned or contractor owned CMDs to access DoD information or connect to DoD networks.

6.8.5.2. Device management is governed by local organizations to meet mission requirements.

6.8.5.3. The use of software certificates on CMDs must be approved by the applicable AO and documented in the system Assessment and Authorization package in accordance with the DISA Mobile Policy Security Requirements Guide (SRG). **(T-0).**

6.8.5.4. For CMDs that are certified in accordance with the National Information Assurance Partnership (NIAP) Protection Profile Mobile Device Fundamentals V3.1, derived credentials are permitted to be stored in the CMD's native keystore. Consult the NIAP Product Compliant List at **https://www.niap-ccevs.org/Product/** for a listing of certified devices.

6.8.5.5. For CMDs that are not certified in accordance with the Protection Profile for Mobile Device Fundamentals, derived credentials shall be stored in FIPS 140-2 level 2 validated cryptographic modules with FIPS 140-2 level 3 physical security in accordance with the DoD PKI Certificate Policy and NIST SP 800-63-3. **(T-0).**

6.8.5.6. Once derived credentials are stored on a CMD, it shall be handled as if it were the CAC from which they were derived. **(T-3).** Subscribers must report it as missing immediately after it is discovered as missing. **(T-3).**

6.8.5.7. For organizational e-mail mailboxes on CMDs, follow the appropriate DoD STIG.

Chapter 7

AIR FORCE DIRECTORY SERVICES

7.1. Air Force Directory Services (AFDS) . Provides authoritative identity and attribute management for the DAF through an end-to-end life-cycle process that includes generation, provision, maintenance, and termination of individual digital identity records. AFDS harvests, standardizes, aggregates, and presents data attributes to organizations and customers through identity management products and services. AFDS serves as the DAF enterprise-level directory service and identity management attribute store. AFDS leverages multiple authoritative data sources to enable secure, accurate, and timely identity data attributes that reduce the need for redundant USAF directory services and security stores core capabilities. These core capabilities include: AF enterprise identity data directory (IDD), account provisioning and user self service, and Exchange contact information synchronization (ECIS). It also provides the Air Force Email for Career (E4C) capability in the form of "@us.af.mil" email addresses for all DAF subscribers. The program is the Authoritative Data Source for the E4C address and makes it available to other authoritative data sources, as requested.

7.1.1. Enterprise IDD (unclassified or classified): Retrieves data from multiple, disparate USAF and DoD data sources to create a single consolidated digital identity record.

7.1.1.1. Provides a common repository known as authoritative attribute store of role-based identity data for warfighters that can be used by systems, applications, and devices. This simplifies the management of core identity data elements about warfighters within individual systems by giving systems access to near real-time data about their subscribers. This capability is designed to be used in strategic and tactical environments.

7.1.1.2. No other identity attribute source (local store) will be established in the DAF without coordinating with ACC HQ CCC/CYX ICAM, AFLCMC, and SAF/CN. **(T-3).**

7.1.2. Account provisioning and user self service (unclassified or classified): Provides administrators and warfighters an automated business process to manage accounts across multiple systems based on authoritative identity records.

7.1.2.1. A single interface is provided to the warfighter to allow automated management of subscribers profiles associated with directory and non-directory enabled applications, including the creation, vetting, modification, updating, and disabling or deletion of accounts process triggered by changes in authoritative data source records.

7.1.2.2. User-Self Service capability gives warfighters the ability to verify or update personal attributes, request publication to the Global Address List publication, and select alternate delivery points for E4C email traffic. User Self Service is found at: **https://imp.afds.af.mil/default.aspx**.

7.1.2.3. DAF users may use AFDS User Self Service to update and/or verify personal attributes.

7.1.3. ECIS. Conduct daily synchronization of email Global Address Lists daily for NIPRNET and SIPRNET environments. This service includes a broader Lightweight Directory Access Protocol directory capability containing over 3.4 million contacts DoD-wide.

7.1.3.1. Supports geographically disparate exchange sites and is a key enabler for email communications for the warfighter.

7.1.3.2. Conducts daily synchronization of several million contacts across DoD, MAJCOMs, CCMDs, and DRUs.

7.1.3.3. DAF organizations will use AFDS Exchange Contact Information Synchronization service to populate all Global Address Lists. **(T-3).**

7.1.4. Requirements Process. ACC HQ CCC/CYX ICAM serves as Lead Command Support and Requirement Lead (RL) for AFDS program. Primary duties include capturing, evaluating, validating, and prioritizing customer requirements. To receive any of the identity management services offered by AFDS, review the AFDS requirements process and workflow at the AFDS Requirements website.

7.1.4.1. To help the customer shape the requirement for submission, visit AFDS Safe Download website **https://epi.afds.af.mil/Onboarding** webpage and review/download the pertinent documents.

7.1.4.2. AFDS Service Catalog. Describes the different services offered by AFDS.

7.1.4.3. Identity Management (IdM) Form 3215, *Requirements Document*. Requirement request form.

7.1.4.4. IdM 3215 Form Instructions. Helps requester properly fill out IdM 3215 Form.

7.1.4.5. AFDS External Data Dictionary. Describes data elements available in the AFDS IDD repository.

7.1.5. AFDS Interface Developers Guide. Gives a high-level explanation of the process of connecting to the virtual directory and sending a query. Provides necessary background information to incorporate the information provided in the virtual directory into an application. Gives a developer the necessary background information to connect to the AFDS web service and incorporate the information returned from the web service into an application.

7.1.6. ACC HQ CCC/CYX ICAM, AFDS requirements lead (RL). Receives properly completed requirements form from customer and determines if requirement is in scope and within current Lead Command direction. If not in scope but in AFDS area of expertise, or has DAF Enterprise level impact, AFDS seeks approval from ACC A6I, AFDS Lead Command, to accept and work the requirement. If RL requires external coordination on a requirement (Air Force Network Integration Center, 561/83 Network Operations Support Center, ANG 299 Network Operations Security Squadron), RL notifies the requester that coordination is needed prior to AFDS Requirements Review Board acceptance.

7.2. Operational Use of Identity Attributes. When performing actions that require the gathering, usage, or presentation of digital identity data, the system will use the associated attributes from the AFDS digital identity store. **(T-3).** Systems that require disconnected operations or other forms of limited connectivity situations may maintain a local copy of the associated attributes of the AFDS digital identity. These systems will not act as a secondary proxy or re-deliver the AFDS identity data attributes to other systems. **(T-3).** First, the system must perform routine periodic updates of the identity record by pulling data from AFDS on a recurring basis of no less frequently that weekly. **(T-3).** Second, the system must use the real time data available from AFDS to the greatest extent possible, as dictated by mission needs. **(T-3).** DAF systems and

organizations will use AFDS IDD (DAF attribute store) service to populate directories with DAF enterprise attributes. **(T-3).**

7.2.1. AFNET NIPRNET attribute binding. For NIPRNET subscriber accounts on AFNET, unique identity attribute binding for individual (non-administrative or non-group accounts) is the responsibility of AFDS on behalf of the AFNET. AFDS is responsible for obtaining the subscriber identity information directly from DMDC to ensure subscriber accounts are established with the subscriber's matching identity attributes. The correct assignment of the identity attributes enables subscribers to use the PKI credentials on their CAC to authenticate to their network account.

7.2.2. Non-AFNET NIPRNET and SIPRNET attribute binding. These network accounts must be configured with a unique identifier for each subscriber. **(T-0).** SIPRNET accounts may use the EDIPI or FASCN with the addition of the Personnel Category Code as the unique identifier. Administrators of non-AFNET NIPRNET and SIPRNET accounts should use an automated tool, such as SIPRNET Lightweight Extensible Authentication Protocol, when possible to populate the account attributes directly from the CAC or SIPRNET token to avoid potential entry errors and unauthorized access.

Chapter 8

PUBLIC KEY INFRASTRUCTURE (PKI) AND PUBLIC KEY ENABLEMENT (PKE)

8.1. PKI/PKE

8.1.1. DoD Defense-in-Depth Security Strategy (e.g., Trust Governance). A vital element of this strategy integrates DoD PKI/PKE to enable network security services throughout the enterprise. **(T-3).** AF PKI System Program Office web site is at **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/AF%20Public%20Key%20Infrastructure%20System%20Program%20Office.aspx/html**. Provides information on the implementation and enablement of PKI and ICAM for Air Force networks, desktops, and personnel and provides comprehensive ICAM solutions to satisfy end subscriber needs. Information Assurance Collaborative Environment (IACE). The AF IACE serves as the primary cybersecurity support resource providing a collaborative one-stop-shop for cybersecurity ideas, questions, discussions, and hosts dynamic content for information sharing.

8.1.1.1. Unclassified IACE content is available at: **https://cs2.eis.af.mil/sites/10060**.

8.1.1.2. ICAM specific SharePoint site **https://cs2.eis.af.mil/sites/13015/_layouts/15/start.aspx#/SitePages/Home.aspx**.

8.1.1.3. Classified content, the IACE-SIPRNET (IACE-S) is available on SIPRNET at **http://intelshare.intelink.sgov.gov/sites/af_cybersecurity/SitePages/Home.aspx**.

8.1.2. PKI includes a combination of hardware, software, policies, and procedures, as well as the ability to authenticate, protect, digitally sign, and when necessary, encrypt electronic mail (e-mail) and documents. It also is able to verify identities, digital signatures and encryption mechanisms by using X.509 certificates for public-key cryptography.

8.1.3. PKE incorporates the use of certificates for people, networks, systems and applications to provide security services such as authentication, confidentiality, data integrity, and non-repudiation. DoD ISs are required to use these certificates to support authentication of identity, access control, information confidentiality, data integrity, and non-repudiation in accordance with DoDI 8520.02 and DoDI 8520.03. **(T-0).**

8.1.4. Certificate Trust. DAF non-person entities (NPEs)s and person entities (PEs) shall only use certificates that are issued by the DoD PKI or with specific CISO approval. **(T-0).** DAF NPEs (e.g., standard desktop configuration trust store) can establish trust with PKIs as described in **paragraph 6.1** Alternate 2FA technologies are described in **paragraph 4.4** External PKIs are approved for use by the Assistant Secretary of Defense for Networks & Information Integration (NII)/DoD CIO in accordance with DoD CIO Memo Update to Department of Defense Chief Information Officer Memorandum on Commercial Public Key Infrastructure Certificates on Public-Facing DoD Website. DoDI 8520.02 defines the process for recommending approval for external PKIs.

8.1.5. DoD PKI Interoperability Root. DAF ISs and subscribers must only trust certificates issued by a DoD and/or a DAF PKI. **(T-0).**

8.1.5.1. DoD mission partners shall use certificates issued by the DoD external certification authority (ECA) program or a DoD approved PKI when interacting with the

DoD in unclassified domains in accordance with DoD External Certification Authority X.509 Certificate Policy Version 4.4. **(T-0).**

8.1.5.2. DoD mission partners shall establish PKI authentication when interacting with the DoD in classified domains in accordance with DoDI 8520.02. **(T-0).**

8.1.5.3. No other PKIs will be established in the AF without coordinating with ACC HQ CCC/CYX ICAM, AF PKI SPO, and SAF/CN. **(T-3).** Contact the AF PKI SPO Helpdesk at **afpki.helpdesk@us.af.mil** to begin the process of adding non preapproved Certificate Trusts.

8.1.5.4. Certificates, by themselves, provide an identity. That identity is gained from an identity manager and can also be leveraged to obtain additional attributes from the identity manager.

8.1.6. Identity manager for attributes (e.g., certificates issued by the DoD PKI, AF PKI, or by a DoD-approved PKI for authentication, digital signature, or encryption). DAF non-DoD mission partners use certificates issued by the DoD ECA program or a DoD-approved PKI. **(T-0).** DoD ECA PKI and External PKI certificates are not used in the DoD and DAF classified domains in accordance with DoDI 8520.02.

8.1.7. Access management uses those attributes provided in making an authorization decision.

8.1.7.1. ICAM Certificate Policy Authority.

8.1.7.2. Unclassified information and information systems.

8.1.7.3. US DoD X.509 Certificate Policy defines the creation and management of X.509 public key certificates for use in applications requiring communication between networked computer-based systems including email, transmission of data, digital signature, and authentication of infrastructure components. Assurance level credential strengths include Level C for Medium Assurance, Level D for Medium Hardware, and Level E for Personal Identity Verification (PIV)-A in accordance with DoDI 8520.02. **(T-0).**

8.1.7.4. Specifications for Medium Assurance credential strength for NPEs, software, and hardware are provided in US DoD X.509 Certificate Policy. **(T-0).**

8.1.8. Classified information and information systems.

8.1.8.1. Establish instructions for the implementation of PKI for SECRET-high collateral classified networks in accordance with CNSSI 1300. **(T-0).**

8.1.8.2. Specifications and instructions for the issuance of certificates issued to named individuals, roles, systems, or devices that are part of NSS SECRET-high systems are provided in NSS PKI DoD Registration Practice Statement (RPS). **(T-0).**

8.1.9. Air Force Internal. Less than medium assurance (LTMA) and internal basic assurance (IBA) certificates. These certificates are used to sign the subordinate CAs operated in the AFNET and at DAF-supported CCMDs, in turn, and issue device identity certificates to internally facing NPEs within the AFIN in accordance with IBA X.509 Certificate Policy Internal LTMA X.509 Certificate Policy. **(T-3).**

8.1.10. DoD PKI Interoperability Root. DAF ISs and subscribers, by policy, are only supposed to trust certificates issued by a DoD and/or AF PKI. **(T-0).**

8.1.10.1. Situations where subscribers and applications must be able to trust commercial providers (e.g., Microsoft™ operating systems) require trust in Verisign commercial certificates in order to operate. **(T-3).**

8.1.10.2. DoD mission partners shall use certificates issued by the DoD External Certification Authority (ECA) program or a DoD approved PKI, when interacting with the DoD in unclassified domains. **(T-0).**

8.1.10.3. DoD mission partners shall establish PKI authentication when interacting with the DoD in classified domains in accordance with DoDI 8520.02. **(T-0).**

8.1.10.4. No other PKIs will be established in the DAF without coordinating with ACC HQ CCC/CYX ICAM, AF PKI SPO, and SAF/CN. Contact the AF PKI SPO Helpdesk at **afpki.helpdesk@us.af.mil** to begin the process of adding non preapproved Certificate Trusts.

8.1.10.5. Certificates, by themselves, provide an identity. That identity is gained from an identity manager and can also be leveraged to obtain additional attributes from the identity manager.

8.1.11. Identity manager for attributes (e.g., certificates issued by the DoD PKI, AF PKI, or by a DoD-approved PKI for authentication, digital signature, or encryption). DAF non-DoD mission partners use certificates issued by the DoD ECA program or a DoD-approved PKI. DoD ECA PKI and External PKI certificates are not used in the DoD and DAF classified domains in accordance with DoDI 8520.02. **(T-0).** Access management uses those attributes provided in making an authorization decision.

8.1.12. ICAM Certificate Policy Authority.

8.1.12.1. Unclassified information and information systems.

8.1.12.1.1. US DoD X.509 Certificate Policy defines the creation and management of X.509 public key certificates for use in applications requiring communication between networked computer-based systems including email, transmission of data, digital signature, and authentication of infrastructure components. Assurance level credential strengths include Level C for Medium Assurance, Level D for Medium Hardware, and Level E for PIV-Authentication in accordance with DoDI 8520.02. **(T-0).**

8.1.12.1.2. Specifications for Medium Assurance credential strength for NPEs, software, and hardware are provided in US DoD X.509 Certificate Policy. **(T-0).**

8.1.12.2. Classified information and information systems.

8.1.12.2.1. Establishes instructions for the implementation of PKI for SECRET-high collateral classified networks in accordance with CNSSI 1300. **(T-0).**

8.1.12.2.2. Specifications and instructions for the issuance of certificates issued to named individuals, roles, systems, or devices that are part of NSS SECRET-high systems are provided in NSS PKI DoD Registration Practice Statement (RPS). **(T-0).**

8.1.13. Air Force Internal. LTMA and IBA Certificates. These certificates are used to sign the Subordinate CAs operated in the AFNET and at DAF-supported CCMDs, in turn, and issue device identity certificates to internally-facing NPEs within the AFIN. **(T-3).**

8.1.13.1. IBA X.509 Certificate Policy.

8.1.13.2. Internal LTMA X.509 Certificate Policy.

Chapter 9

AUDIT CHECKLIST

9.1. Auditing. Auditing associate's identity data with events for monitoring, saving activity to audit logs for automated and human review. This ensures that behaviors involving the access and utilization of resources comply with established guidance. It also provides for the capability to set thresholds for system alerts when activity falls outside accepted norms. Such activity can then be investigated to determine the nature of the behavior and apply the proper remediation. Monitoring data or their detected patterns can also be used to reconstruct activity profiles to facilitate performance and forensic investigations. The event data contained in audit logs, along with the logs themselves, must be protected from unauthorized access, modification, or deletion. **(T-3).**

9.2. Compliance Audits. The purpose of a compliance audit is to verify that the audited party has in place a system to assure the quality of the services that it provides and that it complies with all the requirements of the Certificate Policy and its CPS. NIPRNET and SIPRNET RAs and LRAs will be audited annually. **(T-3).**

9.2.1. RAs/LRAs must attach a risk assessment to all audit submissions. **(T-3).**

9.2.2. All RAs and LRAs will be audited periodically in accordance with DoD RA/LRA CPS. **(T-3).**

9.2.2.1. RAs will audit the LRAs' audit results and checklists annually. **(T-3).**

9.2.2.2. RAs will provide updates to the AF CISO every 6 months. **(T-3).**

9.2.2.3. DoD PKI PMO has the responsibility to audit the RAs. **(T-3).**

9.2.3. LRA self-assessment audit checklists are located on the AF PKI LRA Training website: **https://intelshare.intelink.gov/sites/usaf-pki/_layouts/15/start.aspx#/SitePages/AF%20Public%20Key%20Infrastructure%20System%20Program%20Office.aspx/html/lra_trg.cfm** under the Help & Training/Local Registration Authority.

9.2.3.1. Items are arranged in four sections: General LRA responsibilities; physical controls; system administrator responsibilities and ISSO responsibilities.

9.2.3.2. A completed LRA self-assessment checklist signed by the LRA's commander may serve as the LRAs annual or periodic audit requirement.

9.2.4. RAs/LRAs will maintain a file of requirement validation documentation for organizational account certificates, as appropriate. **(T-3).**

Lauren Knausenberger, SES, USAF
DAF Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AF Developer's Guide for Obtaining DoD Code Signing Certificates, 5 July 2017

AFI 16-107, *Military Personnel Exchange Program,* 29 August 2018

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, 18 February 2014

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 06 February 2020

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 31-101, *Integrated Defense (ID),* 25 March 2020

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFI 36-3026V1_IP, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 04 August 2017

AFI 36-3026V2, *Common Access Card (CAC),* 17 May 2018

AFMAN 17-1301, *Computer Security (COMPUSEC),* 12 February 2020

AFMAN 17-1303, *Air Force Cybersecurity Workforce Improvement Program*, 12 May 2020

AFPD 17-1, *Information Dominance Governance and Management,* 12 April 2016

CJCSI 6211.02D, *Defense Information System Network (DISN) Responsibilities*, 24 January 2012

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* 9 February 2011

CNSS-015-2016, *Memorandum for the National Security Systems Public Key Infrastructure Member Governing Body*, 14 June 2016

CNSSI 1300, *Instruction for National Security Systems (NSS) Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25,* October 2009

CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015

DAFI 33-360, *Publications and Forms Management,* 7 August 2020

DHS ICAM 101 Briefing for Public Safety Officials

DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information,* 1 June 2005

DoD 5200.08-R, *Physical Security Program,* 9 April 2007

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

DoD CIO Memorandum, Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems, 20 August 2018

DoD External Certification Authority X.509 Certificate Policy v4.4, 1 October 2015

DoD PKI RA/LRA CPS, DoD PKI Registration Authority/Local Registration Authority Certification Practice Statement, Version 5, 10 April 2019

DoD Security Technical Implementation Guides (STIGs)

DoD X.509 Certificate Policy v10.6, 20 May 2018

DoDD 5205.16, *The DoD Insider Threat Program*, 30 September 2013

DoDD 5230.09, *Clearance of DoD Information for Public Release*, 25 January 2019

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* 16 June 1992

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, 22 June 2005

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure,* 6 November 1984

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),* 14 April 2004

DoDD 8521.01E, *DoD Biometrics*, 13 January 2016

DoDI 1000.25, *DoD Personnel Identity Protection (PIP) Program*, 2 March 2016

DoDI 1400.25V731, *DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees,* 24 August 2012

DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, 10 December 2005

DoDI 5200.46, *DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC),* 1 May 2018

DoDI 5200.48, *Controlled Unclassified Information (CUI),* 6 March 2020

DoDI 5230.29, *Security and Policy Review of DoD Information for Public Release,* 13 August 2014

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, 24 May 2011

DoDI 8520.03, *Identity Authentication for Information Systems,* 13 May 2011

DoDM 1000.13V1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, 23 January 2014

DoDM 5200.02, *Procedures for the DoD Personnel Security Program (PSP),* 3 April 2017

DoDM 5200.02 AFMAN 16-1405, *Air Force Personnel Security Program,* 1 August 2018

DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control,* 23 August 2018

EO 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, 22 November 1943

EO 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust,* 16 January 2009

FIPS 140-2, *Security Requirements for Cryptographic Modules,* 25 May 2001

FIPS 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors,* August 2013

HAFMD 1-26, *Chief, Information Dominance and Chief Information Officer,* 5 February 2015

HSPD 12: *Policy for a Common Identification Standard for Federal Employees and Contractors,* 27 August 2004

ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* 15 September 2008

Memorandum on Commercial Public Key Infrastructure Certificates on Public-Facing DoD Website, 4 October 2018

MPTO 00-33A-1202, *Air Force Network Account Management,* 18 March 2014

MPTO 00-33A-1300, *SIPRNET Releasable (SIPR REL) Enclave Implementation Core Service,* August 1, 2017

MPTO 00-33A-1301, *Foreign National NIPRNet Access Core Services,* 4 April 2016

MPTO 00-33B-5006, *Computer Security (COMPUSEC),* 15 December 2017

MPTO 00-33D-2001, *AFNET Enterprise Naming Conventions,* 31 August 2018

MTO 2018-283-001, *Two-Factor Authentication (2FA) for Privileged User Accounts,* 10 October 2018

NIST SP 800-63-3, *Digital Identity Guidelines,* June 2017

NIST SP 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*, June 2017

NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*, June 2017

NIST SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI),* July 2015

NIST SP 800-116 Rev. 1, Guidelines for the Use of PIV Credentials in Facility Access, June 2018

NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials,* 19 December 2014

NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations,* January 2014

NSS PKI DoD Registration Practice Statement, Version 8, 19 December 2014

NSTISSP 200, *National Policy on Controlled Access Protection,* 15 July 1987

TASS Overview Guide, December 2014

Title 8 Code of Federal Regulations, *Aliens and Nationality*, 1 January 2018

Title 10 United States Code Section 9013, 14 January 2019

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision*

DD Form 1172-2, *Application for Identification Card/DEERS Enrollment*

DD Form 2875, *System Authorization Access Request (SAAR)*

Identity management (IdM) Form 3215, *requirements document*.

Abbreviations and Acronyms

2FA—Two-factor authentication

AAL—Authenticator Assurance Level

ABAC—Attribute Based Access Control

ACC—Air Combat Command

AD—Active Directory

AF—Air Force

AFDS—Air Force Directory Services

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFLCMC—Air Force Life Cycle Management Center

AFMAN—Air Force Manual

AFNET—Air Force Network

AFNET-S—Air Force Network-Secure Internet Protocol Network

AF PKI SPO—Air Force Public Key Infrastructure System Program Office

ALT—Alternate Logon Token

ANG—Air National Guard

AO—Authorizing Official

CA—Certification or Certificate Authority

CAC—Common Access Card

CAVP—Cryptographic Algorithm Validation Program

CCC—Cyberspace Capabilities Center

CCMD—Combatant Command

CCRB—Change Control Requirements Board

CIO—Chief Information Officer

CISO—Chief Information Security Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CMA—Certificate Management Authority

CMD—Commercial Mobile Device

CNSS—Committee on National Security Systems

CNSSI—Committee on National Security Systems Instruction

COG—Cyber Operations Group

COMPUSEC—Computer Security

COR—Contracting Officer Representative

CPR—CAC Pin Reset

CPS—Certification Practice Statement

CRI—Certificate Registration Instructions

CRL—Certificate Revocation List

CSAA—Code Signing Attribute Authority

CSP—Credential Service Provider

CSS—Commanders Support Staff

CTO—Chief Technology Officer

CUI—Controlled Unclassified Information

CVS—Contractor Verification System (superseded by TASS)

CW—Cyber Wing

CYZ—Cyberspace Security Flight

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DEERS—Defense Enrollment Eligibility Reporting System

DHS—Department of Homeland Security

DISA—Defense Information Systems Agency

DMDC—Defense Manpower Data Center

DN—Distinguished Name

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDIN—Department of Defense Information Network

DoDM—Department of Defense Manual

DPC—Derived PIV Credentials

DRU—Direct Reporting Unit

E4C—Email for Career

ECA—External Certification Authority

ECIS—Exchange Contact Information Synchronization

EDIPI—Electronic Data Interchange Personal Identifier

ETIMS—Enhanced Technical Information Management System

FASCN—Federal Agency Smart Credential Number

FIPS—Federal Information Processing Standards

FN—Foreign National

FOA—Field Operating Agency

GO—General Officer

HAF—Headquarters Air Force

HQ—Headquarters

HTTPS—Hypertext Transfer Protocol Secure

IA—Information Assurance

IACE—Information Assurance Collaborative Environment

IACE—S—IACE-SIPRNET

IAL—Identity Assurance Level

IAO—Information Assurance Officer (IAO) Express

IBA—Internal Basic Assurance

IC—Intelligence Community

ICAM—Identity, Credential, and Access Management

ICD—Intelligence Community Directive

IDD—Identity Data Dictionary

IdM—Identity Management

IFS—Identity Federation Services

IS—Information System

ISO—Information System Owner

ISSM—Information Systems Security Manager

ISSO—Information Systems Security Officer

IT—Information Technology

ITIPS—Information Technology Investment Portfolio Suite

LN—Local National

LRA—Local Registration Authority

LTMA—Less Than Medium Assurance

MAJCOM—Major Command

MPTO—Methods and Procedures Technical Order

MTO—Maintenance Tasking Order

NEATS—NIPRNET Enterprise Alternative Token System

NIAP—National Information Assurance Partnership

NII—Network & Information Integration

NIPRNET—Non-classified Internet Protocol Router Network

NIST—National Institute of Standards and Technology

NOSC—Network Operations and Security Center

NPE—Non-Person Entity

NSS—National Security Service or National Security System

NSTISSP—National Security Telecommunications and Information Systems Security Policy

OCSP—Online Certificate Status Protocol

OID—Object Identifiers

OPR—Office of Primary Responsibility

PACS—Physical Access Control Systems

PCS—Permanent Change of Station

PE—Person Entity

PED—Portable Electronic Device

PIN—Personal Identification Number

PIP—Personnel Identity Protection

PIT—Platform Information Technology

PIV—Personal Identity Verification

PKE—Public Key Enabling

PKI—Public Key Infrastructure

PMO—Program Management Office

P&R—Personnel & Readiness

RA—Registration Authority

RAPIDS—Real-time Automated Personnel Identification System

RBAA—Role Based Attribute Authority

RFC—Request for Comments

RL—Requirement Lead

RMF—Risk Management Framework

RP—Relying Party

RPS—Registration Practice Statement

SAAR—System Authorization Access Request

SCI—Sensitive Compartmented Information

SES—Senior Executive Service

SIPRNET—Secret Internet Protocol Router Network

SP—Special Publication

SPO—System Program Office

SRG—Security Requirements Guide

STIG—Security Technical Implementation Guide

TA—Trusted Agent

TASS—Trusted Associate Sponsorship System (superseded CVS)

TMS—Token Management System

TO—Technical Order

US—United States

USAF—United States Air Force

USB—Universal Serial Bus

USCYBERCOM—United States Cyber Command

USSF—United States Space Force

VIP—Very Important Person

VO—Verifying Official

VSC—Virtual Smart Card

WCO—Wing Cybersecurity Office

Terms

Access—Ability to make use of any information system (IS) resource. (CNSSI 4009)

Accountability—The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (CNSSI 4009)

Accreditation—Formal declaration by an AO that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (CNSSI 4009)

Alternate Logon Token (ALT)—A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions. (DoDI 8520.02)

Application—A software program hosted by an information system. (CNSSI 4009)

Assurance—The grounds for confidence that the set of intended security controls in an information system are effective in their application. (CNSSI 4009)

Asymmetric Cryptography—Also referred to as public-key cryptography, asymmetric cryptography incorporates two cryptographic keys to implement data security, a public key and a private key. The public key is used for encryption and may be given to anyone, trusted or not. The private key is used for decryption and must be kept secret. **(T-0).**

Audit—Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. (CNSSI 4009)

Audit Trail—A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period. (CNSSI 4009)

Authentication—Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information (CNSSI 4009)

Authorized User—User must: possess a valid U.S. security clearance commensurate with the classification level of system accessed, possess a mission need to know, and complete DoD IA training. **(T-0).**

Authorizing Official (AO)—A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI 4009)

Availability—Timely, reliable access to data and information services for authorized users. (CNSSI 4009)

Biometrics—Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (CNSSI 4009 & DoDD 8521.01)

Certification Practice Statement—A statement of the practices that a Certificate Authority, Registration Authority, or other PKI component employs in issuing, revoking, and renewing certificates and providing access to them, in accordance with specific requirements specified in a Certificate Policy. (DoDI 8520.02)

Claimant—An entity whose identity is to be verified using an authentication protocol. (CNSSI 4009)

Clearance—A formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of classified information (TOP SECRET, SECRET, or CONFIDENTIAL). (CNSSI 4009)

Commercial Mobile Device (CMD—)—A subset of portable electronic devices as defined in DoDD 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (touch screen, miniature keyboard, etc.) and exclude portable electronic devices running a multi-user operating system (Windows™ operating system, Mac™ operating system, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers. (AFMAN 17-1301)

Common Access Card (CAC)—Standard identification/smart card issued by the DoD that has an embedded integrated chip storing PKI certificates. **Note:** As per DoDM 1000.13, the CAC, a form of DoD ID card, serves as the Federal PIV card for DoD implementation of Homeland Security Presidential Directive 12. (CNSSI 4009) It is the primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. (DoDI 8520.02)

Computing Environment—Workstation or server (host) and its operating system, peripherals, and applications. (CNSSI 4009)

Confidentiality—Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (CNSSI 4009)

Controlled Access Protection—Minimum set of security functionality that enforces access control on individual users and makes them accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. (CNSSI 4009)

Controlled Unclassified Information(CUI)—Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. (DoDI 5200.48) The designation CUI replaces the term "sensitive but unclassified" (SBU). (CJCSI 6510.01F)

Countermeasures—Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (CNSSI 4009)

Credential—An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token processed and controlled by a subscriber. (NIST SP 800-79-2)

Cryptographic Token—A portable, user-controlled, physical device (e.g., smart card or PC card) used to store cryptographic information and possibly also perform cryptographic functions. (See also Token) (CNSSI 4009)

Department of Defense Information Network (DoDIN)—The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or standalone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Formerly known as the Global Information Grid (GIG). (CNSSI 4009)

Enclave—A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI 4009)

Encryption—The cryptographic transformation of data to produce ciphertext. (CNSSI 4009)

Foreign National—Anyone who is not a United States (US) citizen. (Title 8, Code of Federal Regulations (CFR), "Aliens and Nationality")

Five Eyes (FVEY)—FVEY is an intelligence alliance between the U.S., Canada, United Kingdom, Australia and New Zealand. (DIA.MIL)

Information—Facts and ideas which can be represented (encoded) as various forms of data. Knowledge -- e.g., data, instructions -- in any medium or form that can be communicated between system entities. (CNSSI 4009)

Information Assurance—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. **Note:** DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms. (CNSSI 4009)

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. **Note:** Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (CNSSI 4009)

Information System Security Manager (ISSM—)—Individual responsible for the information assurance of a program, organization, system, or enclave. (CNSSI 4009)

Information System Security Officer (ISSO)—Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information

system owner for maintaining the appropriate operational security posture for an information system or program. (CNSSI 4009)

Information System Owner (ISO)—Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (CNSSI 4009).

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (CNSSI 4009)

Integrity—Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (CNSSI 4009)

Key—A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. Usually a sequence of random or pseudorandom bits used initially to set up and periodically change the operations performed in cryptographic equipment for the purpose of encrypting or decrypting electronic signals, or for determining electronic counter-countermeasures (ECCM) patterns, or for producing other keys.(CNSSI 4009)

Key Pair—A public key and its corresponding private key used with a public key algorithm. (CNSSI 4009)

Least Privilege—The principle that a security architecture will be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (CNSSI 4009) **(T-0).**

Media—Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, large scale integration memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (CNSSI 4009)

Mission Partners—Non-DoD individuals and organizations that support or are supported by DoD missions and operations. Mission partners include allies, coalition partners, host nations, international and multinational organizations, civilian government agencies and departments (Federal, State, local, and tribal), law enforcement agencies, non-governmental agencies and organizations (private volunteer organizations, commercial businesses, academic institutions) and other non-adversaries.

Mobile Code—Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. **Note:** Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript. (CNSSI 4009)

Mobile Computing Device—Mobile computing devices are information system devices such as portable electronic devices, smartphones, commercial mobile devices (including enterprise activated commercial mobile devices), laptops, tablets, broadband aircard devices, and other handheld devices that can store data locally and/or access Air Force-managed networks through mobile access capabilities. (AFMN 17-1301)

Need-to-know—A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified

information in order to perform or assist in a lawful and authorized governmental function. (E.O. 13526)

Non-repudiation—Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (CNSSI 4009)

Personal Identification Number—A secret number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (CNSSI 4009)

Personal Identity Verification—A physical artifact (e.g., identity card, "smart" card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an

automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201. (CNSSI No. 1300)Personally Identifiable Information (PII)—Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (CNSSI 4009)

Platform Information Technology (PIT—)—Information technology (IT), both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. (CNSSI 4009)

Portable Electronic Device (PED)—Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to, pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders. (CNSSI 4009)

Privileged User—A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (CNSSI 4009)

Public Key Infrastructure—The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. (CNSSI 4009)

Relying Party—An entity that relies on the validity of the binding of the subscriber's name to a public key to verify or establish the identity and status of an individual, role, system or device; the

integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the subscriber. (CNSSI 4009)

Role-Based Access Control—Access control based on subscriber roles (e.g., a collection of access authorizations a subscriber receives based on an explicit or implicit assumption of a given role). Role permissions can be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (CNSSI 4009)

Safeguards—The protective measures prescribed to meet the security requirements (e.g., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. (CNSSI 4009)

Security Controls—The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (CNSSI 4009)

Sensitive Compartmented Information—A subset of Classified National Intelligence concerning or derived from intelligence sources, methods, or analytical processes, that is required to be protected within formal access control systems established by the Director of National Intelligence. (CNSSI 4009)

Special Access Program—A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (CNSSI 4009)

Subscriber—An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. (CNSSI 4009)

Threat—Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (CNSSI 4009)

Token—A portable, user-controlled, physical device (e.g., smart card or PC card) used to store cryptographic information and possibly also perform cryptographic functions. (Also known as Cryptographic Token) (CNSSI 4009)

Two-Factor Authentication—A method of authenticating a subscriber's identity using a combination of something the subscriber has and something the subscriber knows. (DoD Access Control STIG)

Unauthorized Access—Any access that violates the stated security policy. (CNSSI 4009)

Very Important Person (VIP)—GOs and/or SESs are eligible to receive ALTs. This use case covers issuing an ALT to members of a support staff of senior executives so the staff can log onto the VIP's account, author/send email on behalf of a VIP, and read current VIP encrypted email. (MTO 2018-283-001)

Vulnerability—Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (CNSSI 4009)

X.509 Public Key Certificate—The public key for a subscriber (or device) and a name for the subscriber (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate. (CNSSI 4009)