BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1301

10 FEBRUARY 2017

Cyberspace

COMPUTER SECURITY (COMPUSEC)

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/CIO A6CS

Certified by: SAF/CIO A6S
(Brigader General Patrick Higby)

Supersedes: AFMAN33-282, 28 March 2012

Pages: 69

This Air Force Manual (AFMAN) implements Computer Security in support of Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management,* and Air Force Instruction (AFI) 17-130, *Air Force Cybersecurity Program Management*. Computer Security (COMPUSEC) is identified as a cybersecurity discipline in AFI 17-130 and defined within this document. This instruction applies to all AF military, civilian, and contractor personnel under contract by DoD, regardless of Air Force Specialty Code (AFSC), who develop, acquire, deliver, use, operate, or manage COMPUSEC for Air Force (AF) organizations. This instruction applies to the Air National Guard (ANG) and Air Force Reserve Command (AFRC). The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). Additional instructions and manuals are listed on the AF Publishing Website at **http://www.e-publishing.af.mil** under "Electronics Publications." Direct questions, recommended changes, or conflicts to this publication through command channels using the AF Form 847, *Recommendation for Change of Publication*, to SAF/CIO A6. Send any supplements to this publication to SAF/CIO A6 for review, coordination, and approval prior to publication. Unless otherwise noted, the SAF/CIO A6 is the waiver approving authority to policies contained in this publication. The authorities to waive wing/unit level requirements in this publication are identified with a Tier number ("T-0, T-1, T-2, and T-3") following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1, 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 Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed IAW AF Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). 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 AF.

SUMMARY OF CHANGES

This document is substantially changed, updating Public Key Infrastructure (PKI) policy, incident management, and access control as a result of a DoD and AF policy directive updates. Review this manual in its entirety.

Chapter 1

INTRODUCTION

1.1. Introduction. Computer Security (COMPUSEC) is a cybersecurity discipline identified in AFI 17-130. Compliance ensures appropriate implementation of measures to protect all AF Information System (IS) resources and information.

The COMPUSEC objective is to employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of United States (US) government information processed by AF ISs.

1.2. Applicability. This publication applies to all AF ISs and devices used to process, store, display, transmit, or protect AF information, regardless of classification or sensitivity, unless exempted.

1.2.1. This publication is binding on all military, civilian and contract employees, who develop, acquire, deliver, use, operate, or manage AF Information Technology (IT). This publication applies to all AF IT used to receive, process, store, display, transmit, or protect AF information, regardless of classification or sensitivity. AF 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).

1.2.2. More restrictive Federal, DoD, AF guidance take precedence over this publication.

1.2.3. 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*.

1.3. Exceptions. Document exceptions and deviations to guidance in this publication affecting ISs as part of the applicable IS security authorization package, IAW AFI 17-101, *The Risk Management Framework (RMF) for Air Force Information Technology (IT)*. Submit modifications, exceptions, and deviations through the system/enclave change management process.

1.3.1. Process equipment acquisition waiver requests IAW AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*.

1.3.2. See AFI 17-100, *Air Force Information Technology (IT) Service Management*, for Commercial Internet Service Provider (CISP) waiver guidance.

1.3.3. See AFMAN 17-1303, *Cybersecurity Workforce Improvement Program,* for certification requirement waiver guidance.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. AFSPC Cyberspace Support Squadron (AFSPC CYSS). Provides cyber networking expertise to HQ AFSPC for COMPUSEC activities and functions.

2.1.1. Provides COMPUSEC policy and technical subject matter expertise for the AF Enterprise.

2.1.2. Provides field support and program management for COMPUSEC to SAF CIO/A6, AFSPC, and all MAJCOMs/FOAs/DRUs. Supports SAF/CIO A6 and AFSPC cybersecurity initiatives. Reviews, evaluates, and interprets AF COMPUSEC doctrine, policy, and procedures. Develops/coordinates recommendations on implementation of the doctrine, policy, and procedures to AFSPC A2/3/6.

2.1.3. Coordinates with the AFSPC Cybersecurity Division as required and accomplishes other roles and responsibilities as directed by HQ AFSPC.

2.2. Air Force Life Cycle Management Center (AFLCMC), Cryptologic and Cyber Systems Division, Responsive Cyber Acquisition Branch, Information Assurance Section(AFLCMC/HNCYP). AF Public Key Infrastructure (PKI) System Program Office (SPO). Manages the AF PKI and carries out tasks/actions as the SAF/CIO A6 PKI Management Authority (PMA) and/or the pertinent DoD organizations direct. This includes the implementation, operation, and sustainment of PKIs and all associated enabling efforts.

2.2.1. Identifies all PKI requirements to SAF/CIO A6.

2.2.2. Integrates PKI into existing ISs as identified in the PKI implementation and program plans. Ensures future IS programs are fully compatible and interoperable with the DoD PKI, as required by DoD and Air Force policy.

2.2.3. Assists the MAJCOMs and supported Combatant Commands (COCOMs) with PK Enablement (PKE) of systems.

2.2.4. Provides PKI Helpdesk and field support to the AF.

2.2.5. Develops and sustains new PKI capabilities for the Air Force and/or for DoD.

2.2.6. Maintains and enforces the integrity of the PKI and its use.

2.3. Wing Cybersecurity Office (WCO). The WCO addresses all COMPUSEC requirements on the base, including those of tenant units (i.e., FOAs, DRUs, and other MAJCOM units), unless formal agreements exist IAW AFI 17-130. Personnel assigned to the WCO will:

2.3.1. Evaluate modifications, exceptions, and deviations to ISs for accuracy and completeness before forwarding to the appropriate agency; see **Chapter 1**. **(T-1).**

2.3.2. Train designated representatives of the Commanders Support Staff (CSS) on Air Force Network (AFNet) account management and COMPUSEC administrative processes and procedures; conduct annual or “as needed” refresher training; see **Chapter 3**. **(T-1).**

2.3.3. Consult with host or MAJCOM Foreign Disclosure Office (FDO) before authorizing Foreign National/Local National (FN/LN) access to ISs; see **Chapter 4**. **(T-1).**

2.3.4. Conduct COMPUSEC assessments; see **Chapter 7**. **(T-1).**

2.3.5. Assist with assessment or analysis supporting Vulnerability Management; see **Chapter 3** and AFI 17-100. **(T-1).**

2.3.6. Coordinate with the system/enclave ISSO/ISSM before deciding whether to sanitize media for reuse or disposal; see **Chapter 6**. **(T-0).**

2.4. Organizational Commander (or Equivalent). Maintains the COMPUSEC program IAW this publication, ensuring AF ISs operate effectively by protecting and maintaining the confidentiality, integrity, and availability of IS resources and information processed throughout the system's life cycle. Organizational commanders will:

2.4.1. Suspend access to unclassified and classified ISs when actions threaten or damage AF ISs; see **Chapter 4**. **(T-0).**

2.4.2. Ensure proper procedures are followed in response to classified information spillages affecting AF ISs; see **Chapter 5**. **(T-0).**

2.4.3. Review all approved removable media waivers semi-annually to ensure continuous validation of mission requirements; see **Chapter 5**. **(T-0).**

2.4.4. Endorse follow-up COMPUSEC assessment reports validating the status of open findings; see **Chapter 7**. **(T-1).**

2.5. Information System Security Manager (ISSM). An ISSM (formerly an Information Assurance Manager [IAM]) is responsible for the cybersecurity of a program, organization, system, or enclave and provides direction to the Information System Security Officer (ISSO) (formerly a system Information Assurance Officer [IAO]). Duties of the ISSM are outlined in DoDI 8500.01, *Cybersecurity*, AFI 17-130, and AFI 17-101. ISSMs will:

2.5.1. Obtain required training and maintain applicable cybersecurity workforce certification; see **Chapter 3**. **(T-0).**

2.5.2. Perform risk identification and assessment activities supporting the change management activities for the system/enclave; see **Chapter 3**. **(T-0).**

2.5.3. Maintain approval and inventory documentation for Authorizing Official (AO)-authorized personally-owned hardware and software; see **Chapter 5**. **(T-1).**

2.5.4. Process removable media waivers; see **Chapter 5**. **(T-1).**

2.5.5. Protect collaborative computing devices used in classified environments; see **Chapter 5**. **(T-0).**

2.5.6. Participate in remanence security (REMSEC) risk management processes; see **Chapter 6**. **(T-1).**

2.5.7. Conduct annual unit/organization COMPUSEC self-assessments using the AFMAN 17-1301 COMPUSEC Self-Assessment Communicator (SAC) located in the AF Inspector General (IG) Management Internal Control Toolset (MICT). **(T-1).**

2.5.8. Assist with AFMAN 17-1301 COMPUSEC SAC review and remediation activities; see **Chapter 7**. **(T-1).**

2.5.9. FNs/LNs are not authorized to hold ISSM positions IAW DoD 8570.01-M, *IA Workforce Improvement Program*. **(T-0).**

2.6. Information System Security Officer (ISSO). An ISSO (formerly a system IAO) is responsible for the technical implementation of a cybersecurity program. When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles. DoDI 8500.01, AFI 17-130, and AFI 17-101 outline the duties of the ISSO. ISSOs will:

2.6.1. Provide protection from threats through implementation of technical and physical security mechanisms; see **Chapter 5**. **(T-0).**

2.6.2. Maintain approval and inventory documentation for AO-authorized personally-owned hardware and software; see **Chapter 5**. **(T-1).**

2.6.3. Participate in REMSEC risk management processes; see **Chapter 6**. **(T-1).**

2.6.4. Execute procedures that identify the residual risk and risk tolerance; see **Chapter 6**. **(T-0).**

2.6.5. Conduct annual COMPUSEC self-assessments using the AFMAN 17-1301 COMPUSEC SAC located in the IG MICT; see **Chapter 7**. **(T-1).**

2.6.6. Assist with AFMAN 17-1301 COMPUSEC SAC review and remediation activities; see **Chapter 7**. **(T-1).**

2.6.7. FNs/LNs are not authorized to hold ISSO positions IAW DoDI 8500.01. **(T-0).**

2.7. Commanders Support Staff (CSS). Organizations implement and enforce AFNet account management and COMPUSEC administrative processes and procedures using the guidance within this instruction IAW AFI 17-130. Personnel performing administrative cybersecurity functions will:

2.7.1. Verify user compliance with annual CyberAwareness Challenge training; see **Chapter 4**. **(T-0).**

2.7.2. Maintain AFNet network access documentation; see **Chapter 4**. **(T-0).**

2.7.3. Assist the WCO with administrative cybersecurity functions (administrative tasking orders, in/out-processing checklists, distribute user training materials, etc.); see **Chapter 5**. **(T-0).**

2.7.4. Conduct annual unit/organization self-assessments using the AFMAN 17-1301 COMPUSEC SAC located in the IG MICT; see **Chapter 7**. **(T-1).**

Chapter 3

TRAINING AND RESOURCES

3.1. General. COMPUSEC includes all measures to safeguard ISs and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Successful implementation of COMPUSEC requires adequate training and proper application of cybersecurity/IA resources.

3.2. COMPUSEC Training Requirements

3.2.1. Military personnel in the 3D0X3 career field attend technical school training in the following courses. Upon successful completion of the final course, trainees are awarded a 3-skill level and a DoD 8570.01-M certification as an IA Management (IAM) Level I/IA Technical (IAT) Level II. . Current course identification, status, length, and prerequisite information may be found at the Education and Training Course Announcements website at **https://etca.randolph.af.mil/default1.asp** under "AETC."

3.2.1.1. E3AQR3D033, *IT Fundamentals Basic*, at Keesler AFB.

3.2.1.2. E3AQR3D033, *Cyber Surety*, at Keesler AFB.

3.2.1.3. E3ABR3D033, *Cyber Surety Security+ Certification*, at Keesler AFB.

3.2.2. All civilian, military, and contractor personnel performing ISSM duties:

3.2.2.1. Attend the Air Education and Training Command (AETC)- formal training course E3AZR3D053, *Information System Security Manager (ISSM)* at Keesler AFB within 6 months of assuming ISSM duties.

3.2.2.2. Complete the Air Force Qualification Training Package (AFQTP) 3D0X3-211RA, *Information Assurance Manager Handbook*. Use the AFQTP:

3.2.2.2.1. As an interim training measure while an individual waits for a class date for the ISSM course.

3.2.2.2.2. As refresher training for individuals that have ISSM experience but have not performed duties as an ISSM within 3 years.

3.2.2.2.3. Contractor personnel may substitute the AFQTP when contract limitations do not allow ISSM course attendance.

3.2.2.3. Follow the Cybersecurity workforce security certification requirements relative to the function, category (technical or managerial), and level of the position as specified in AFMAN 17-1303, DoD Directive (DoDD) 8140.01, *Cyberspace Workforce Management*, and DoD 8570.01-M, *Information Assurance Workforce Improvement Program*. Additional training and/or certifications may be necessary depending on specific requirements of the ISSM position. More information on DoD-approved 8570 baseline certifications is available in an extension to Appendix 3 of DoD 8570.01-M on the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) website (**http://iase.disa.mil/iawip/Pages/iabaseline.aspx**).

3.2.3. Cybersecurity Workforce. Training and certification of cybersecurity personnel depend upon the types of tasks assigned by the organizational commander. Determine the tasks performed and consult DoD 8570.01-M and AFMAN 17-1303 for training and certification requirements.

3.2.3.1. Cybersecurity Workforce categories are IAT and IAM. Specialties are Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs).

3.2.3.2. Cybersecurity Workforce personnel performing IAT/IAM level tasks require the appropriate certifications.

3.2.4. CSS Training. The WCO provides direction, oversight, and annual training for designated representatives of the CSS. The WCO locally develops the CSS cybersecurity training programs and includes the following COMPUSEC-specific items:

3.2.4.1. Authorized users, access requirements, and access documentation.

3.2.4.2. Account management and trouble reporting functions (including IAO Express/Enterprise Service Desk [ESD]).

3.2.4.3. SIPRNet token recovery actions.

3.3. Information Assurance Collaborative Environment (IACE). The AF IACE serves as the primary cybersecurity/IA support resource for WCO and managers, providing a collaborative one-stop-shop for cybersecurity/IA ideas, questions, discussions, and hosts dynamic content for information sharing (**https://cs.eis.af.mil/sites/10060**).

For classified content, the IACE- Secret Internet Protocol Router Network (SIPRNet) (IACE-S) is available at http://intelshare.intelink.sgov.gov/sites/af_cybersecurity/SitePages/Home.aspx.

3.4. Methods and Procedures Technical Orders (MPTO). MPTOs provide procedural guidance to the cybersecurity workforce to implement and manage methods and processes pertaining to COMPUSEC policy. Specific COMPUSEC-related MPTOs are MPTO 00-33B-5004, *Access Control for Information Systems;* MPTO 00-33B-5006, *End Point Security for Information Systems;* and MPTO 00-33B-5008, *Remanence Security for Information Systems.* Obtain MPTOs via the organizational Technical Order Distribution Account (TODA) on Enhanced Technical Information Management System (ETIMS) **https://www.my.af.mil/etims/ETIMS/index.jsp**).

3.5. Information Technology Asset Procurement. Comply with evaluation and validation requirements in DoDI 8500.01 for all IT services, hardware, firmware, software components, or products incorporated into DoD ISs.

3.5.1. Follow the guidance in AFMAN 17-1203 and the AF Information Technology Commodity Council (ITCC) guidance available on the AF Portal or AFWAY (**https://www.afway.af.mil/**) for procurement activities of all IT hardware, cellular, and peripheral devices (e.g., desktops, laptops, servers, commercial mobile devices [CMDs], multifunction devices [MFDs] printers, scanners, and wireless peripheral devices).

3.5.2. Comply with the evaluation and validation requirements of Committee on National Security Systems Policy (CNSSP) 11, *National Policy Governing the Acquisition of*

Information Assurance (IA) and IA-Enabled Information Technology Products, for all IA and IA-enabled products.

3.5.3. Life Cycle Management. Procure products and adopt risk-based program management IAW AFI 63-101/20-101, *Integrated Life Cycle Management.*

3.5.4. Unified Capabilities (UC). Modernizing IT capabilities while aligning with joint solutions remain two of the AF's key goals. AFMAN 17-1202, *Collaboration Services and Voice Systems Management*, and DoDI 8100.04, *DoD Unified Capabilities (UC),* provide guidance related to Voice and Video over Internet Protocol (VVoIP), Video Teleconferencing (VTC), and interoperability.

3.5.4.1. In accordance with DoDI 8100.04, use/obtain UC products certified by the DISA Joint Interoperability Test Command (JITC), JITC certifies interoperability and the UC-implementing DoD component AO or the DISA Certifying Authority (CA) certifies for Cybersecurity under RMF. Approved products are listed on the DISA UC Approved Products List (APL) (**https://aplits.disa.mil/processAPList.action**) and should be added to the enclave security authorization package and assessed for Cybersecurity through the RMF process.

3.5.4.2. As a general rule, Section 508-compatible Voice over Internet Protocol (VoIP) devices are not listed on the DISA UC APL unless the vendor has included the assistive technology (AT) end device as part of the VoIP system's evaluation package. Organizations may request that the vendor add the product to the current UC APL certification package and request a "desktop review" from the DISA Unified Capabilities Certification Office (UCCO). The DISA UCCO (Email: **disa.meade.ns.list.unified-capabilities-certification-office@mail.mil**) has a listing of all product representatives. This review ensures the product operates with the current fielded VoIP system. If the vendor is unable or unwilling to add the AT product to the UC APL certification, identify compliance with AFMAN 17-1202 in the enclave/IS security authorization package.

3.5.4.3. All Air Force VTC suites are transitioning off the Integrated Services Digital Network (ISDN)-based Defense Information System Network (DISN) Video Service-Global (DVS-G) to Global Video Services (GVS), IAW Maintenance Tasking Order (MTO) 2014-295-001. AF organizations should not expend funds on the upgrade, replacement, and acquisition of voice, video, and/or data services equipment outside of the GVS program.

3.5.5. Cloud Services. Acquire and implement private and/or public cloud computing services in support of the Air Force Information Network (AFIN) IAW AFI 17-100.

3.5.6. Foreign produced products. Under Title 10, United States Code (U.S.C.), Section 2533a (*Requirement to Buy Certain Articles from American Sources; Exceptions*) and reflected in Federal Acquisition Regulation (FAR) Subpart 25.1, *Buy American – Supplies, 25.103 Exceptions*, and Defense Federal Acquisition Regulation Supplement (DFARS) Part 225 – *Foreign Acquisition, Subpart 225.1, Buy American – Supplies, 225.103 Exceptions,* there are exceptions allowing the purchase of foreign-made commercial technology. For guidance go to **https://www.acquisition.gov/** to access the FAR and DFARS (under "Supplemental Regulations").

3.5.6.1. Use an approved importer or through a World Trade Organization Government Procurement Agreement (WTO GPA) country. AFWay, ITCC, and General Services Administration (GSA) offer foreign-made products secured from an approved importer or WTO GPA.

3.5.6.2. Countries barred from providing products and services are listed on the "Domestic Preference Restrictions" table available at the *Defense Procurement and Acquisition Policy* website under the "Restrictions on Purchasing from Non-U.S. Sources" area (**http://www.acq.osd.mil/dpap/cpic/ic/restrictions_on_purchases_from_non-us_sources.html**).

3.6. Configuration Management Resources. Securely configure and implement all IT products. Cybersecurity/IA reference documents, such as National Institute of Standards and Technology (NIST) Special Publications (SP), DISA Security Technical Implementation Guides (STIGs), DISA Security Requirements Guides (SRGs), National Security Agency (NSA) Security Configuration Guides, AF Technical Orders (TOs), and other specialized publications are used for the security configuration and implementation guidance. Apply these reference documents IAW DoDI 85xx.xx series, AFI 33-xxx series, and AFI 17-xxx series publications to establish and maintain a minimum baseline security configuration and posture. Document all configuration changes with the enclave/system ISSM in the IS security authorization package IAW AFI 17-101 and the system change management process.

Chapter 4

INFORMATION SYSTEM ACCESS CONTROL

4.1. Introduction. AF ISs connect to the DoD Information Network (DoDIN) subnetworks (e.g., SIPRNet, Non-classified Internet Protocol Router Network [NIPRNet], GVS, etc.) IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02, *Defense Information Systems Network (DISN) Responsibilities*. Every individual who has access to standalone systems, specialized/functional ISs, enterprise ISs, and/or mission systems is an IS user.

4.1.1. Access to AF ISs is a revocable privilege and is granted to individuals based on need to know and IAW National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 200, *National Policy on Controlled Access Protection;* DoD 5200.2-R, *Personnel Security Program*; and CJCSI 6510.01, *Information Assurance (IA) and Support to Computer Network Defense (CND)*. Follow procedural guidance in MPTO 00-33B-5004.

4.1.2. The Information System Owner (ISO) ensures methods are in place to verify user access requests before granting IS access. Address delegation of authority for specific system/enclave access in the system authorization package.

4.2. Authorized Users. 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. Configure authorized user account creation and administration using role-based access schemes; see AFMAN 17-1201, *User Responsibilities and Guidance for Information Systems.* Consult AFI 31-501, *Personnel Security Program Management,* for investigation requirements for access to an Automated Information System (AIS) position, as outlined in DoD 5200.2-R, Appendix 10.

4.2.1. All authorized users (e.g., military, civilian, contractor, temporary employees, volunteers, interns, key spouses, and American Red Cross personnel) will complete CyberAwareness Challenge training prior to being granted access to an IS. **(T-0).** Users annually re-accomplish CyberAwareness Challenge training; organizations maintain compliance IAW DoD 8570.01-M. Authorized user access to unclassified and classified ISs based on the assigned duties and the Automated Data Processing (ADP) position categories identified in DoD 5200.2-R, Appendix 10: Category ADP-III (also referred to as IT-III) are nonsensitive positions.

4.2.1.1. CyberAwareness Challenge training is located on the Advanced Distributed Learning Service (ADLS) accessible via the AF Portal.

4.2.1.2. A publically accessible version of the CyberAwareness Challenge training is located on the DISA website (**http://iase.disa.mil**). Users without an ADLS account may substitute this training for initial network access.

4.2.1.3. When a user requires a new/modification to his/her account (due to change of station or assignment, Temporary Duty [TDY], etc.), the gaining CSS verifies the user meets access requirements before granting access to the IS. Users are not required to retake the CyberAwareness Challenge training provided the user has a valid and current (within a year) course completion record. Verification of completion may be

accomplished using the printed or electronic copy of CyberAwareness Challenge training certificate from DISA or ADLS or confirmation by the CSS.

4.2.1.4. System access by authorized users requires PKI access methods as specified in DoDI 8520.03, *Identity Authentication for Information Systems,* and CJCSI 6510.01.

4.2.2. Privileged User. Grant privileged access to unclassified and classified ISs based on the assigned duties and the ADP position categories identified in DoD 5200.2-R, Appendix 10: Category ADP-I (also referred to as IT-I) are Privileged positions and Category ADP-II (also referred to as IT-II) are Limited Privileged positions.

4.2.2.1. Administrative and privileged accounts require PKI user authentication IAW United States Cyber Command (USCYBERCOM) Tasking Order (TASKORD) 2015-0102, *Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication*.

4.2.2.2. Privileged users should meet all the requirements of an authorized user as specified in AFMAN 17-1303 and paragraph 4.2.1.

4.2.2.3. Privileged users are established and administered with a role-based access scheme IAW the system policy and **Chapter 3** of DoD 5200.2-R and AFMAN 17-1303.

4.2.2.4. System access requires PKI access methods as specified in DoDI 8520.03 and CJCSI 6510.01.

4.2.2.5. Privileged users access only data, control information, software, hardware, and firmware that they are authorized access and fulfills the "need to know" requirement.

4.2.2.6. To maintain separation of duties and least privilege, users maintain separate accounts, a user account for day-to-day or "non-privileged" functions, and a privileged account for administrative functions IAW DoD 8570.01-M.

4.2.2.7. Prohibit sharing of privileged user accounts and credentials between users.

4.2.2.8. Configure privileged user remote access IAW the applicable DISA STIGs (i.e., Enclave, Operating System, Remote Access, Directory Services Domain, etc.) and the selected security controls within the RMF package.

4.2.2.9. Privileged users are position-certified IAW DoD 8570.01-M and qualified IAW AFMAN 17-1303.

4.2.2.10. Privileged users complete an *Information System Privileged Access Agreement and Acknowledgement of Responsibilities* IAW DoD 8570.01-M (Appendix 4).

4.2.3. Foreign Nationals/Local Nationals. A FN/LN user is anyone who is not a US citizen or permanent resident, IAW Title 8, Code of Federal Regulations, *Aliens and Nationality*.

4.2.3.1. The MAJCOM FDO determines authorized and privileged "need to know" for the administrative access and control of information, software, hardware and firmware to include controlled unclassified information (CUI) and classified information, IAW DoD Manual (DoDM) 5200.01, Volume 4, DoD *Information Security Program: Controlled Unclassified Information (CUI).*

4.2.3.1.1. WCOs consult the Host or MAJCOM FDO and applicable ISSM before authorizing access by FN/LN users to ISs processing, storing, or transmitting

classified and CUI. Note: Specific FN/LN access guidance can be found in the following publications: MPTO 00-33A-1301, *Foreign National NIPRNet Access Core Services*; MPTO 00-33B-5004; MPTO 00-33B-5006; MPTO 00-33A-1202, *Air Force Network Account Management*; MPTO 00-33D-2001, *AFNET Enterprise Services Naming Conventions*; AFI 16-107, *Military Personnel Exchange Program*; AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*; DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*; DoDD 5400.7, *DoD Freedom of Information Act (FOIA) Program*; DoD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*; AFI 33-332, *Air Force Privacy and Civil Liberties Program*; DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*; and DoDD 5230.20, *Visits and Assignments of Foreign Nationals*.

4.2.3.1.2. Pursuant to applicable host-nation agreements, FN/LN privileged users are certified to baseline computing environment (CE) IAW DoD 8570.01-M. If privileged access is required to an IS, restrict FN/LN user access to IAT I/II level positions and only under the immediate supervision of a US citizen. Furthermore, document access in the IS security assessment package.

4.2.3.1.3. At the discretion of the ISO, FN/LN system access requires PKI access methods as specified in **Chapter 8**.

4.2.3.1.4. Sanitize or configure classified ISs to restrict access by FN/LNs to only classified information authorized for disclosure to the FN/LNs government or coalition, as necessary to fulfill the terms of their assignments IAW applicable host MAJCOM FDO requirements.

4.2.3.1.5. Other Considerations. 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, as outlined in paragraph 4.2.1.

4.2.3.2. Before authorizing FN/LN access to unclassified ISs, the ISO ensures compliance with the IS access requirements in MPTO 00-33A-1301.

4.2.4. Group Accounts. The Enterprise AO (or applicable AO if entirely within their boundary) is the approving authority for group accounts and may require a Defense Information Assurance Security Accreditation Working Group (DSAWG) waiver IAW CJCSI 6510.01 and DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*. Document authorization in the system/enclave authorization package.

4.2.4.1. Requests for group accounts using individual/unique authentication should be submitted via email to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**).

4.2.4.2. Group accounts that do not use an individual/unique authenticator require DSAWG approval. To submit requests to the DSAWG for approval, contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**).

4.2.5. Temporary and Volunteer Accounts. Grant only unclassified IS access to temporary employees and volunteer personnel in support of their assigned duties.

4.2.5.1. A volunteer is any individual (including key spouses) authorized to be DoD volunteers as defined in DoDI 1100.21, *Voluntary Services in the Department of Defense*. Restrict volunteers to ADP-III/IT-III level positions IAW DoDI 5200.2-R, Appendix 10.

4.2.5.2. Temporary employees and volunteers are required to meet the requirements as specified in paragraph 4.2.1.

4.2.5.3. Temporary employees and volunteers require PKI access as outlined in **Chapter 8**.

4.3. Required Account Access Documentation

4.3.1. When required by the ISO for IS access, the CSS or ISSO ensures the DD Form 2875, *System Authorization Access Request (SAAR)*, is completed and signed. Document access requests, Annual Information Awareness (CyberAwareness Challenge) training completion, and justification for access and clearance/background investigation verification as referenced by DoD 5200.2-R and AFI 31-501. DD Form 2875 signatures can be "wet" or digitally signed. Do not combine multiple system access requests on the same DD Form 2875.

4.3.1.1. CSSs/ISSOs, in coordination with the organizational security manager, verify user background investigation requirements IAW DoD 5200.2-R.

4.3.1.2. The ISSO/ISSM (referred to as the "Information Assurance Officer" on the DD Form 2875) retains the DD Form 2875 IAW instructions outlined on the form for non-AFNet ISs. The CSS retains the DD Form 2875 according to the instructions on the form for AFNet ISs.

4.3.1.2.1. Original DD Form 2875s for unprivileged AFNet accounts may be transferred when duty assignments change; the gaining unit's CSS may use local methods to update duty information in the "IAO Express" tool and shared drive access requirements. The losing unit's CSS ensures termination of shared drive access prior to users out-processing. Changes to privileged account access requirements require a new DD Form 2875.

4.3.1.2.2. Re-accomplish DD Form 2875s for AFNet-SIPRNet (AFNet-S) accounts when access requirements change.

4.3.2. In accordance with AFMAN 17-1201, users of all authorized IS devices (to include Mobile Computing Devices) sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision,* prior to initial IS access. For wireless devices, users complete the standardized AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement.* Maintain copies of signed AF Forms 4433 within the CSS.

4.3.3. Access to classified ISs also requires a Standard Form (SF) 312, *Nondisclosure Agreement,* IAW AFI 16-1404, *Air Force Information Security Program.*

4.4. Token Access. IAW DoDI 8520.02 and DoDI 8520.03, users authenticating to DoD networks require the use of a hardware token. Follow guidance in **Chapter 8** to obtain a hardware token prior to being granted access to AFNet and AFNet-S Directory Services Domains and authenticating to NIPRNet or SIPRNet PK-Enabled websites.

4.5. Loss of Access. Access to an AF IS is a privilege and continued access is contingent on personnel actions, changes in need to know, or operational necessity; see AFMAN 17-1201. The ISO has the authority to re-instate users who have lost access.

4.5.1. Specific procedural information for account disabling is located in MPTO 00-33B-5004.

4.5.2. Failure to complete annual CyberAwareness Challenge training results in immediate suspension of access to unclassified and classified ISs.

4.5.3. Actions that threaten or damage AF ISs may result in immediate suspension of access to unclassified and classified ISs IAW CJCSI 6510.01 and DoD 5200.2-R. Deliberate inappropriate use of user accounts or systems may result in administrative disciplinary action IAW AFMAN 17-1201.

4.5.3.1. If an individual's clearance is suspended, denied, or revoked, immediately suspend access to classified ISs. Commanders should 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.

4.5.3.2. If an individual violates the IS terms of use, commanders should consider suspending access pending re-accomplishment of CyberAwareness Challenge training. Additional restrictions on reinstatements for classified ISs are determined locally and should follow the guidelines of DoD 5200.2-R.

4.6. Account Management. AF direction is to use PKI-based identification and authentication IAW DoDI 8520.02, DoDI 8520.03 and the USCYBERCOM Communications Tasking Order (CTO) 07-015, *Public Key Infrastructure (PKI) Implementation, Phase 2* (**https://www.cybercom.mil/J3/orders/Pages/CTOs.aspx**). Manage all user accounts using applicable system configuration guidance; follow TOs published by AFSPC (e.g., MPTO 00-33B-5004, MPTO 00-33A-1202 [for AFNet accounts], and the applicable DISA STIGs [enclave, application security, operating system, database, etc.]).

4.6.1. ISSM/ISSOs implement automated IS controls to check and disable IS user accounts that have been dormant more than 30 days IAW CJCSI 6510.01.

4.6.1.1. AF CIO Exception: Disable National Guard and Reserve member IS user accounts only after 90 days of inactivity.

4.6.1.2. Document system specific IS user account disabling requirements after periods of inactivity in the IS security authorization package.

4.6.1.3. ISSMs provide a monthly list of disabled SIPRNet accounts to the base Local Registration Authority (LRA) for SIPRNet hardware token recovery actions; see **Chapter 8**.

4.6.2. Delete unnecessary (to include service accounts) and/or default accounts and change all factory default or user-generated passwords included in a newly acquired system (software or hardware) IAW the configuration information in the IS security authorization package before allowing any user access to the system.

4.6.2.1. Rename default accounts that cannot be deleted, IAW applicable DISA STIGs.

4.6.2.2. Do not execute root-level access in IS applications.

4.6.2.3. Disable/deactivate user accounts (do not delete/deprovision) when users are unable to remotely access their accounts due to an extended absence or when a user is suspended from work, IS access is revoked for any reason, or the security clearance is suspended as specified in paragraph 4.5.3.

Chapter 5

END POINT SECURITY

5.1. Introduction. End point security provides the basis for overall protection of AF-controlled IT assets. Follow CJCSI 6510.01 on the use of DoD-provided, enterprise-wide automated tools/solutions (e.g., Host Based Security System [HBSS]) to ensure interoperability with DoD and AF provided enterprise-wide solutions for remediation of vulnerabilities for endpoint devices.

5.2. General Protection. All authorized users should protect networked and/or standalone ISs against tampering, theft, and loss. Protect ISs from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, AF publications, and organizationally created procedures. See AFI 31-101, *Integrated Defense*, for physical access security guidance. End point security procedures are located in MPTO 00-33B-5006.

5.2.1. Identify and authenticate users before gaining access to any government IS IAW guidance in **Chapter 4**.

5.2.2. ISSM/ISSO provide protection from threats by ensuring proper configuration of technical security mechanisms and establishing physical controls for the removal and secure storage of information from unattended ISs (e.g., Common Access Card [CAC] removal lock feature, keyboard locks, secure screen savers, add-on security software). This is done IAW the DISA Operating Systems STIGs and the system security plan (SSP) (found in the system authorization package in the Enterprise Mission Assurance Support Service [eMASS]). See NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for more information about SSPs.

5.2.3. Treat devices released to or potentially accessed by unauthorized personnel (outside DoD control) as an untrusted device until IS security policy requirements are re-established and validated IAW the DISA *Removable Media Storage and External Connections* STIG.

5.2.4. Protect devices at the applicable security classification of the information stored in the device IAW CJCSI 6510.01 and this publication.

5.2.5. Protect display devices to prevent inadvertent viewing of classified and controlled or sensitive information by unauthorized users (e.g., away from windows, doorways, public areas); for more information see the DISA *Traditional Security Checklist*.

5.2.6. Control viewing of US-Only ISs and equipment by FNs/LNs IAW CJCSI 6510.01; see the DISA *Traditional Security Checklist*.

5.2.7. Ensure transmission of sensitive information is encrypted using NIST-certified cryptography at a minimum IAW CJCSI 6510.01.

5.2.8. Ensure the transmission of classified information is encrypted using NSA-approved cryptography IAW AFMAN 17-1302, *Communications Security (COMSEC) Operations*, and CJCSI 6510.01.

5.2.9. In areas where classified information is processed, ensure ISs meet TEMPEST requirements IAW Air Force Systems Security Instruction (AFSSI) 7700, *Emission Security* (to become AFMAN 17-1305).

5.2.10. Appropriately mark and label IT devices IAW the highest level of classification processed or displayed on the device IAW DoDM 5200.01, Volume 2 *DoD Information Security Program: Marking of Classified Information*, and DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, if appropriate.

5.2.10.1. Display/peripheral devices (e.g., monitors, projectors, televisions) are required to be either physically marked or technically configured to display the classification banner.

5.2.10.1.1. Display devices located within the same classification environment or mixed environments attached to approved Keyboard, Video, Monitor (KVM) device are not required to be physically labeled if the desktop backgrounds are configured through the IS to identify the classification level.

5.2.10.1.2. Mark and label all KVM switches (regardless of classification environment) to identify the switch position and the associated classification of the connected systems IAW the DISA *Keyboard, Video, Mouse Switch Security* STIG.

5.2.10.2. Physically mark and label all mobile computing devices with the potential to be located/used in mixed environments or publically accessible areas with the highest classification level of the information approved to be processed by the device. If necessary due to mission or operating environment requirements, coordinate with WCO and Wing Information Protection (IP) Office in developing alternate marking and labeling methods.

5.2.11. Contact the organizational security manager for devices involved in data spillage or security incidents IAW AFI 16-1404. For REMSEC guidance, see **Chapter 6**.

5.3. Software Security. The ISSM ensures all software is included in the IS security authorization package IAW AFI 17-101 and CJCSI 6510.01. Comply with AFMAN 17-1203 for software accountability guidance.

5.3.1. Freeware, public domain software, shareware originating from questionable or unknown sources (e.g., World Wide Websites), and Peer-to-Peer file sharing software are highly susceptible to malicious logic and can only be used after a risk assessment (see AFI 17-101) has been conducted.

5.3.2. Prohibit use of trial or demonstration software due to its unreliability and potential source-code flaws.

5.4. Malicious Logic Protection. Protect ISs from malicious logic (e.g., virus, worm, Trojan horse) attacks by applying a mix of human and technological preventative measures IAW the DISA STIGs and CJCSI 6510.01.

5.4.1. Implement antivirus software with current signature files IAW DoD Antivirus Security Guidance (**http://www.disa.mil/cybersecurity/network-defense/antivirus**). The ISSM documents a process for updating devices that are not able to receive automatic updates (i.e., standalone systems, TDY laptops, etc.) in the SSP IAW with the NIST SP 800-53.

5.4.2. Use only security patches and antivirus tools/signature files/data files obtained from the Defense Asset Distribution Systems (DADS) hosted at the DoD Patch Repository at **https://patches.csd.disa.mil/**.

5.4.3. Configure virus scanning frequency and real-time protection IAW the applicable DISA STIG; document scanning frequency in the SSP IAW NIST SP 800-53.

5.4.4. Using additional antivirus software may be approved through the security authorization process; any additional antivirus software should be used in conjunction with DoD-approved antivirus software (**http://www.disa.mil/cybersecurity/network-defense/antivirus**).

5.4.5. Users report malicious logic intrusions or any other deviation and misconfiguration IAW AFI 16-1404.

5.4.6. Implement malicious logic protection for Mobile Code Technologies IAW the DISA *Application Security and Development* STIG and the DoD Policy Memorandum, *Mobile Code Technologies Risk Category List Update* (**http://iase.disa.mil/policy-guidance/Pages/index.aspx**).

5.5. Data Spillage/Classified Message Incidents (CMIs). Data spillage incidents occur when a higher classification level of data is placed on a lower classification level system/device (including CMDs) IAW the Committee on National Security Systems (CNSS) *Glossary 4009*. When classified information is processed or maintained on an unclassified IS, the individual discovering the incident initiates security incident procedures IAW DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* and AFI 16-1404.

5.6. Telework . Criteria for determining eligibility for telework are identified in DoDI 1035.01, *Telework Policy,* and AFI 36-816, *Civilian Telework Program*. See DoD Administration Instruction (AI) 117, *Telework Program,* for implementation guidance (**http://www.dtic.mil/whs/directives/index.html**). For detailed information on telework methods reference NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security* (**http://csrc.nist.gov/publications/PubsSPs.html**).

5.6.1. Configure all teleworking government furnished equipment (GFE) for remote access with an approved encryption solution (e.g., virtual private network [VPN], transport layer security [TLS]) IAW DISA *Remote Access Policy, Remote Endpoint,* and *Remote Access VPN* STIGs.

5.6.2. GFE, software, and communications with appropriate security measures are required for any telework arrangement that involves CUI data. See DoDI 1035.01, Enclosure 3 for additional restrictions for CUI and Personally Identifiable Information (PII) data (**http://www.dtic.mil/whs/directives/index.html**).

5.6.3. Each approved telework worksite (either the teleworker's home or a Telework Center) requires a DD Form 2946, *Department of Defense Telework Agreement*. If an alternative telework worksite is used due to a lack of resources (i.e., no electricity, ISP outage, etc.), complete a DD Form 2946 and secure the worksite IAW the DISA *Remote Access Policy* STIG.

5.7. Data Encryption. Encrypt sensitive information (e.g., CUI, For Official Use Only [FOUO], PII, Health Insurance Portability and Accountability Act [HIPAA], Privacy Act, Proprietary). Validate IA/IA-enabled products providing encryption through the Common Criteria Evaluation and Validation Scheme (CCEVS), Common Criteria Portal, or the cryptographic modules and algorithms evaluated IAW the NIST Cryptographic Algorithm Validation Program (CAVP) and of Cryptographic Module Validation Program (CMVP). The CAVP provides validation testing of Federal Information Protection Standards (FIPS)-approved and NIST-recommended cryptographic algorithms and their individual components, such as compliance with FIPS 180-4, *Secure Hash Standard (SHS),* for implementing Secure Hash Algorithm (SHA) 256, FIPS 197*, Advanced Encryption Standard (AES),* and other FIPS. Cryptographic algorithm validation is a prerequisite of the CMVP. The CMVP validates cryptographic modules to FIPS 140-2, *Security Requirements for Cryptographic Modules*. Under the *Federal Information Security Modernization Act of 2014* (Public Law 113-283), compliance with FIPS is mandatory for non-national security systems and may not be waived.

Follow additional guidance in USCYBERCOM CTO 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD),* and the CNSSP No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems.*

5.7.1. DAR and data in transit protection requires FIPS 140-2 validated cryptographic modules for securing CUI and PII and NSA approved cryptographic systems for classified data IAW CJCSI 6510.01.

5.7.1.1. Comply with any approved Enterprise DAR solution(s) for AFNet systems.

5.7.1.2. Use CCEVS-validated products or NIST-evaluated cryptographic modules that provide the minimum FIPS 140-2 validated cryptographic module implementing SHA-256 for DAR for non-Windows platform operating systems.

5.7.2. Classified Data At Rest (CDAR). Protect classified national security information at rest IAW CJCSI 6510.01 using NSA-approved cryptographic and key management systems offering appropriate protection levels and approved for protecting CDAR or approved physical security measures as identified in DoDM 5200.01, Volume 3. AFSPC CYSS Cryptographic Modernization Office (**CYSS.CYS.AFCOMSEC-CryptoMod@us.af.mil**) is the designated lead for all AF CDAR encryption use cases.

5.8. Personally -Owned Hardware and Software. Personally-owned hardware and software used to process DoD information requires mission critical justification and AO approval. The ISSO/ISSM maintains approval and inventory documentation between the user and government organization in IS security authorization package.

5.8.1. The introduction of personally-owned hardware and/or software to an IS may be a violation of the IS user agreement and subject to repercussions outlined in the IS SSP, and may result in loss of user access, see paragraph 4.5.

5.8.2. Do not introduce personally-owned/developed software or connect personally-owned media or peripheral devices with volatile or non-volatile memory (including, but not limited to, music/video Compact Disk (CD)/Digital Versatile Disk (DVD), commercial MP3 players, and Universal Serial Bus [USB] drives) to AF ISs and/or GFE.

5.8.3. Comply with TEMPEST and physical security requirements, and ensure approval for personally-owned devices prior to introduction into classified processing areas. This applies to fitness monitors, wearable smart technology devices, tablets, e-readers, recording devices (audio, video, etc.), Bluetooth, and near field communication. See paragraph 5.11.4 for more information.

5.9. Wireless Services. Comply with DoDI 8500.01 and DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, for wireless services (radio frequency [RF] and infrared [IR]) integrated with or connected to AF ISs.

5.9.1. Implement wireless peripheral devices, to include keyboard/mouse/pointer devices, IAW requirements outlined in the Wireless STIGs, the National Information Assurance Partnership (NIAP) *Mobile Device Fundamentals Protection Profile, DoD Annex* (**https://www.niap-ccevs.org/pp/**). Acquire wireless peripheral devices IAW AFMAN 17-1203.

5.9.2. Follow applicable TEMPEST guidance for all wireless capabilities. Wireless capabilities are prohibited in areas where classified information is discussed or processed without written approval from the Enterprise AO (or applicable AO if classified wireless capabilities fall entirely within their boundary and do not touch the AFIN) and the Air Force Certified TEMPEST Technical Authority (AF CTTA) IAW DoDD 8100.02.

5.9.3. Configure wireless network solutions IAW the DISA Wireless STIGs and CJCSI 6510.01; document wireless configurations in the IS security authorization package for Enterprise AO (or applicable AO if the wireless capabilities fall entirely within their boundary and do not touch the AFIN) approval IAW DoDD 8100.02. Configure mobile device wireless network solutions IAW the applicable DISA Mobility STIGs and SRGs as applicable.

5.9.4. Configure all unclassified wireless peripheral devices (e.g., keyboards, mice, pointers/forwarders, etc.) with FIPS 140-2 validated encryption modules IAW CJCSI 6510.

5.9.4.1. Implement end-to-end data encryption for unclassified information over an assured channel, and certify under the NIST CMVP to meet requirements of FIPS 140-2 IAW DoDD 8100.02. Secure classified information within NSA-approved encryption solutions IAW CJCSI 6510.

5.9.4.1.1. Individual exceptions to unclassified wireless encryption may be granted on a case-by-case basis IAW DoDD 8100.02 and this publication after a risk assessment and approval by the Enterprise AO (or applicable AO if the wireless capabilities fall entirely within their boundary and do not touch the AFIN); see boundary specific appointment letters (**https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/afcks/AFAAP/Lists/DAA_Program/AO_Public.aspx**).

5.9.4.1.2. The AF Enterprise AO has accepted the risk for not implementing FIPS 140-2 validated cryptographic modules on Bluetooth keyboard, mouse, and pointing devices used on the unclassified AFNet. Risk acceptance does not extend to non-AFNet systems/enclaves. All HIPAA-compliant medical Bluetooth devices

determined to be medically necessary or beneficial to patient care are authorized for use with AFNet and CMD with or without FIPS 140-2 certification.

5.9.4.1.3. Bluetooth headsets designed for IP-based telephones on the unclassified network do not require FIPS 140-2 validated encryption. These devices are prohibited on classified networks. Bluetooth headsets are approved for unclassified voice communication with AF-authorized mobile devices while driving a motor vehicle and for on base and mission-required communications, including VoIP headsets in unclassified work environments.

5.9.4.1.4. Bluetooth single point headsets used with UC soft phones on an unclassified network do not require FIPS 140-2 validated encryption; ISSM/ISSO annotate approval for use in the system authorization package. Multipoint headsets that allow simultaneous multiple pairing (headset-computer and headset-CMD) are prohibited.

5.9.4.2. IR wireless mice/pointers and keyboards require AO approval; for use in classified processing areas implement applicable TEMPEST countermeasures.

5.10. Mobile Computing Devices. Mobile computing devices are IS devices such as portable electronic devices (PEDs), CMDs (including enterprise activated CMDs), laptops, and other handheld devices that can store data locally and access AF-managed networks through mobile access capabilities.

5.10.1. Configure and handle all devices IAW applicable DISA Mobility STIGs, *Mobile Policy* SRG, any updated/newly released mobile operating system STIG (e.g., Apple, Android, Windows Phone), and CJCSI 6510.01. Obtain Enterprise AO approval for all non-compliant STIG configuration standards.

5.10.2. Prior to issuance of each CMD, the CSS verifies user compliance with the DISA Smartphone and Tablet training (**http://iase.disa.mil/eta/Pages/index.aspx**). CMD users complete annual training IAW DISA *CMD Policy* STIG.

5.10.3. Government-owned mobile devices connecting to DoD systems require proper approval and documentation in the IS security authorization package. The AF Enterprise AO is the approving authority for use of PKI software certificates on enterprise activated CMDs. Enterprise AO approval is required prior to provisioning CMDs with DoD PKI digital certificates as outlined in paragraph 8.13. Submit requests to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**).

5.10.4. Prohibit the introduction of government or personal cellular/personal communications system and/or RF, IR wireless devices, and other devices such as cell phones and tablets, and devices that have photographic or audio recording capabilities into areas (e.g., rooms, offices) where classified information is processed and discussed. Exceptions to this policy requires adherence to TEMPEST requirements IAW DoDD 8100.02, written approval by the AF CTTA IAW AFI 16-1404, NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, and the Enterprise AO (or applicable AO if the wireless capabilities fall entirely within their boundary and do not touch the AFIN); see boundary specific appointment letters

(**https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/afcks/AFAAP/Lists/DAA_Program/AO_Public.aspx**).

5.10.4.1. Approval by the AO is based upon the ISSM risk assessment and AF CTTA recommendation.

5.10.4.1.1. Telehealth monitoring devices (i.e., pacemakers, implanted medical devices, personal life support systems, etc.) or assistive devices (e.g., hearing aids) with Bluetooth/RF capabilities are exempt from this requirement IAW AFI 16-1404 and DoDD 8100.02.

5.10.4.1.2. Supplemental devices designed to interconnect wirelessly between telehealth/assistive devices to a VoIP handset, CMD, or similar communications device require a TEMPEST countermeasure review, AF CTTA recommendation, and AO approval prior to use in a classified area.

5.10.4.2. If approved, document AO approval within the IS security authorization package and address countermeasures in the TEMPEST assessment for classified processing areas.

5.10.5. Use only approved secure (classified) mobile computing (e.g., DoD Mobility Classified Capability-Secret [DMCC-S] replacement for Secure Mobile Environment [SME] PED) wireless devices for storing, processing, and transmitting classified information.

5.10.5.1. Encrypt classified data stored on secure (classified) mobile computing wireless devices using NSA-approved cryptographic and key management systems IAW CJCSI 6510.01.

5.10.5.2. Configure secure (classified) mobile computing wireless devices IAW the appropriate DISA Mobility STIG (e.g., SME-PED or its replacement, DMCC-S).

5.10.6. All users issued a mobile device sign a mobile device user agreement IAW AFI 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process*, using the AF Form 4433.

5.10.6.1. For all CMDs (to include Non-Enterprise Activated [NEA] CMDs), document approved changes to baseline configurations (to include software, security settings, applications) on the AF Form 4433, Part II, Block 12, *Remarks as Needed*. Annotate the date the user completed the DISA Smartphone and Tablet (**http://iase.disa.mil**) training in Block 12 of the form.

5.10.6.2. The AF Enterprise AO is the approval authority for all optional or undesignated security settings for all AF enterprise activated CMDs as defined in the appropriate DISA STIGs Configuration Tables (**http://iase.disa.mil**).

5.10.6.3. Organizations that have migrated to the Defense Enterprise Email (DEE) – NIPRNet defer to the service level agreement (SLA) with the DoD Mobility Unclassified Capability (DMUC) leased service.

5.10.7. ISSMs ensure mobile devices comply with the DAR/DIT requirements in paragraph 5.8.

5.10.8. Users immediately report any lost or stolen device to the issuing organization and system ISSO IAW AFMAN 17-1203.

5.10.8.1. Remotely wipe lost or stolen CMDs (through previously installed wiping application or by cellular carrier) and suspend the corresponding service plan, if applicable.

5.10.9. Maintain positive control over all hardware peripheral devices (i.e., portable printer devices, removable media (USB storage devices, optical media, external hard drives, power accessories, etc.) that may accompany the mobile computing device.

5.10.10. NEA CMD acquired through the AF ITCC are approved for use within the AF for any non-sensitive unclassified DoD tasks. NEA CMDs are only authorized to process/store publically available information (e.g., conducting training, monitoring meteorological data, viewing flight maps, and recruiting activities).

5.10.10.1. Prohibit NEA CMD devices from storing and/or processing classified information, CUI, HIPAA information, and other sensitive information.

5.10.10.2. Configure government-owned NEA CMDs IAW the current DISA STIG.

5.10.10.3. Track and manage all government-owned NEA CMDs IAW AFI 17-210, *Radio Management,* and AFMAN 17-1203.

5.10.10.4. Limit personal use of government-owned NEA CMDs with government-paid cellular plans to prevent excessive data charges over monthly limits (see AFMAN 17-1203).

5.10.10.5. All NEA CMDs are required to use hardware tokens via CAC readers and access any public facing DoD PKI-enabled websites; DoD-issued software certificates are not authorized for use with NEA CMDs IAW the DISA *Mobile Policy* SRG.

5.10.10.6. For purchasing NEA CMD applications, obtain licenses per the vendor's software licensing agreement. Organizations track licenses to ensure fiscal responsibility and prevent duplicate purchases IAW AFMAN 17-1203.

5.10.11. Commanders and users follow NSA Guidance, NSA MIT-005FS-2014, *Mitigations for Spillage of Classified Information onto Unclassified Mobile Devices* (**www.iad.gov** under "IA Advisories and Alerts"), for handling CMD spillages.

5.10.11.1. AF-owned NEA CMDs contaminated with CUI, PII, HIPAA, and other sensitive unclassified data may be cleared following the procedures outlined in NSA MIT-005FS-2014. Contact HQ AFSPC A2/3/6, DSN 692-9582, **afspc.a6s@us.af.mil** for CMD spillage questions.

5.10.11.2. In the event there is CUI and/or HIPAA data discovered on a personally-owned CMD, the owner of the device assumes liability for the data breach.

5.11. Peripheral Devices. A computer peripheral is any external device that provides input and output for the computer (e.g., mouse, scanners, smart boards, pointers, and keyboard devices are input devices, etc.). Output devices receive data from the desktop or laptop providing a display or printed product (e.g., monitors, projectors, printers, and MFDs).

5.11.1. Use of basic peripherals such as headsets, mice, and keyboards do not require individual authorization (i.e., in the system authorization package) as long as they are not programmable, do not contain persistent storage capabilities, or require additional software (excluding device drivers).

5.11.2. Web cam usage on any IS requires documentation in the SSP. Use of web cams in classified environments requires physical security and/or TEMPEST countermeasures.

5.11.3. Assistive Technology (AT) (Section 508). AT refers to a service or device that is used to increase, maintain, or improve functional capabilities of individuals with disabilities. AT can refer to an item, piece of equipment, software, or system that has been acquired commercially. AT solutions may include compact keyboards, breath-controlled keyboard/mouse devices, alternative pointing devices, assistive listening devices (wired, FM, and Bluetooth), video phones, screen reader software, screen magnification software, voice recognition software, etc. For more information, see AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508.*

5.11.3.1. Wounded Warrior Program. The Computer/Electronic Accommodations Program (CAP) conducts needs assessments, procures and delivers AT to Medical Treatment Facilities (MTFs) or wounded warrior program, and provides training. The MTFs record the needs assessment and document on a DD Form 2987, *CAP Accommodation Request*. DoDI 6025.22, *Assistive Technology (AT) for Wounded, Ill, and Injured Service Members,* outlines the roles and processes but does not include the local supporting communications unit.

5.11.3.1.1. DoDI 6025.22 does require that all CAP activities meet applicable acquisition, confidentiality, privacy, security, and disclosure requirements IAW DoDD 5400.11, *DoD Privacy Program*, and DoD 5400.11-R, *Department of Defense Privacy Program.* For more information, see the CAP document, *Handbook for Providing Assistive Technology to Wounded Service Members* (**http://www.cap.mil**).

5.11.3.1.2. Organizations conduct or request an assessment from the local communications unit to ensure the end point device operates properly. CAP staff members can work with the communications unit or designated assessor by discussing specific assistive technologies. Equipment can only be delivered to a Federal government facility and installed by the local communications support activity. The CAP is not responsible for the installation of AT. The enclave or system ISSM may submit any non-IA/IA-enabled software to Air Force Network Integration Center (AFNIC)/NTS for certification. Once certified (or if there is no software to certify), the ISSM conducts a risk assessment to determine the overall impact to the enclave/system security posture and adds it to the IS/enclave security authorization package.

5.11.3.2. In accordance with Public Law 109-364, Title V, Section 561, *Military Personnel Policy*, the AT is authorized by law to become the property of the wounded service member at his or her separation from active service. Therefore, the AT can and should remain with the service members as they transition to other locations or leave the military. While the service member remains on active duty, review/assess any software upgrades on a case-by-case basis.

5.11.3.3. When CAP purchases AT for a DoD civilian employee, the equipment becomes the property of the employee's organization. The individual organizations have the freedom to decide if equipment should go with the employee if they change federal jobs or stay with the agency. CAP strongly encourages organizations to transfer the AT with

the federal employee to another federal job, reducing the time waiting for replacement equipment for the employee, ensuring reuse of the technology, and saving federal funds.

5.11.4. Regardless of the classification, configure and handle peripheral devices IAW the DISA *Removable Storage and External Connections* STIG and identify in the IS security authorization package.

5.11.5. Any deviation to the configuration specified in the DISA *Removable Storage and External Connections* STIG requires approval by the AO, to include classified networks and systems.

5.11.6. Configure MFDs and networked printers IAW the *Multifunction Device and Network Printers* STIG. Only use Common Criteria-certified MFDs IAW CNSSP No. 11 and DoDI 8500.01.

5.11.6.1. Acquire all MFDs through AFWay using an ITCC blanket purchase agreement (BPA). The acquisition of any MFD device outside of the AFWay process requires MAJCOM approval. If the device is not listed on AFWay, obtain a waiver through AFWay to purchase the desired device. Guidance for obtaining a waiver may be pursued through the "Request for Quote" process at the AFWay website (**https://www.afway.af.mil/**). See AFMAN 17-1203 for more information.

5.11.6.2. Document MFDs utilizing IA-enabled functions (e.g., scan to email) in the IS security authorization package for approval by the AO IAW the DISA *Multifunction Device and Network Printers* STIG.

5.11.7. At the end-of-life, handle peripheral devices containing non-volatile memory IAW **Chapter 6**.

5.12. Removable Media. Removable media is any type of storage media designed to be removed from a computer (e.g., external hard drives, flash, USB devices, optical media, etc.).

5.12.1. Scan approved removable media devices for viruses before use.

5.12.2. Configure and handle all approved removable media devices IAW all applicable DISA STIGs and CJCSI 6510.01.

5.12.3. Protect removable media containing PII and CUI taken outside organizational networks IAW CJCSI 6510.01 and DODM 5200.01, Volume 4.

5.12.3.1. The ISSO/ISSM informs users on DAR requirements, ensuring stored information on removable media complies with the requirements outlined in paragraph 5.8 and configured IAW the DISA *Removable Storage and External Connections* STIG.

5.12.3.2. USB approved external or optical media devices should be approved by the ISO IAW AFI 33-332 prior to storing PII electronic records assigned as High or Moderate Impact.

5.12.3.3. Report any lost or stolen removable media containing CUI or PII to the privacy monitor immediately, IAW AFI 33-332.

5.12.4. Ensure the safeguarding, marking, and labeling of all media IAW the requirements for the highest level of information ever contained on the media IAW DoDM 5200.01, Volume 2.

5.12.4.1. Ensure proper classification, marking, storing, transportation, and destruction of removable flash media devices IAW DoDM 5200.01, Volumes 2 and 3, and remanence security guidelines; see **Chapter 6**.

5.12.4.2. Unless an AF Enterprise AO-approved write protection mechanism or write protection process (COMPUSEC Toolbox and/or NSA's File Sanitization Tool [FiST][or replacement tool]) is used, unclassified media introduced into a classified IS becomes classified IAW CJCSI 6510.01 and the AF Enterprise AO (AFSPC/A6) Memorandum, *Guidance for Manual Data Transfers Across Security Domains.*

5.12.4.3. Disable "write" mechanisms for all forms of removable media on SIPRNet ISs IAW USCYBERCOM CTO, *Protection of Classified Information on Department of Defense (DoD) Secret Internet Protocols Router Network (SIPRNet)* 10-133 (**https://www.cybercom.mil/default.aspx**).

5.12.4.4. Organizations with a mission requirement to write to removable media submits requests for a waiver to the AO or alternate approving authority (e.g., Group Commander) IAW the *AF DAA Combined Implementation Guidance for USCYBERCOM CTO 10-084 and CTO 10-133 Memorandum* located at (**https://cs3.eis.af.mil/sites/afao/cto10133/default.aspx**).

5.12.4.5. WCOs verify that organization commanders review all approved waivers semi-annually to validate the mission requirement. If no longer required due to a change in mission, role, or assignment, the system ISSM submits a request to remove the device/user account from the waiver and disable the USB ports/CD Drives.

5.12.4.6. Users are required to notify the approving waiver authority if the waiver requirement is no longer needed.

5.12.4.7. System ISSMs validate the approved waivers against the HBSS whitelist semi-annually, verifying the removed devices/user accounts. For systems unable to implement HBSS, manually verify the removal of write capabilities on each device.

5.12.5. Prohibit the use of removable media devices disguised to look like common items (e.g., pens, bracelets, erasers) in areas where DoD ISs are present.

5.12.6. The ISSO/ISSM ensures the proper handling of storage devices that contain classified information IAW **Chapter 6**.

5.12.7. Whitelist all external storage media (to include memory sticks, thumb drives, camera memory cards, digital cameras, smart phones, media players, external storage devices, flash media, and similar technologies) connected via USB ports to AFIN systems. Submit the whitelist waiver IAW the current TASKORD and/or MTO.

5.12.8. Removable flash media use is prohibited until organizations have identified procedures, put appropriate technologies in place, and have received approval from the AO or alternate approving authority (e.g., O-6 Group Commander or equivalent) IAW the *AF DAA Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133* memorandum. Only USB removable flash media (USB thumb drives) devices that have FIPS 140-2 certification under the NIST CMVP for encryption are authorized for purchase and use on the AFIN. View the vendor information at

http://csrc.nist.gov/groups/STM/cmvp/index.html under the "Module Validation Lists" hyperlink.

5.12.9. Account for all removable media devices in the Asset Inventory Management system or the most current, mandated AF IT inventory control system.

5.12.9.1. Report the loss of any removable media device that is whitelisted immediately to the WCO for whitelist removal actions IAW the current MTO. Treat recovered removable media devices as untrusted.

5.12.9.2. Report the loss of any removable media device containing PII to the organizational privacy monitor immediately.

5.13. Collaborative Computing. Collaborative computing provides an opportunity for a group of individuals and/or organizations to share and relay information in such a way that cultivates team review and interaction in the accomplishment of duties and attainment of mission accomplishment. Configure and control collaborative computing technologies (e.g., Defense Collaboration Services [DCS], MilSuite, SharePoint, etc.) to prevent unauthorized users from seeing and/or hearing national security information and material at another user's workstation area.

5.13.1. Follow information in paragraph 3.5.5 for cloud based collaborative computing.

5.13.2. The system ISSM ensures the use of cameras/microphones in unclassified and/or classified environments are documented and approved in the IS security authorization package. Protect collaborative computing devices used in classified environments, see paragraph 5.2.

5.13.3. Configure webcams, attached microphones, and control the projection of information viewable by webcams IAW the DISA *Voice and Video over IP (VVoIP)* and Video Services Policy STIGs. Collaborative computing mechanisms that provide video and/or audio conference capabilities need to provide a clear visible indication that video and/or audio mechanisms are operating to alert personnel when recording or transmitting IAW the DISA *VVoIP Overview* STIG.

5.14. Contractor-Owned Information Systems. Contractor-owned or operated ISs need to meet all security requirements for connection to the AFIN IAW CJCSI 6211.02, AFI 17-100, and AFI 16-1404. Interconnection with the AFIN is accomplished IAW DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* and configured IAW the appropriate DISA *Network* STIGs.

5.14.1. Authorize externally-owned IS and PIT systems that are dedicated to DoD processing and are effectively under DoD configuration control IAW DoDI 8510.01.

5.14.2. Off-base, non-DoD owned facilities require Defense Security Service (DSS) approval to process classified DoD information IAW DoD 5220.22-M.

5.14.3. On base contractors within AF-controlled facilities comply with the FAR, DFARS, and DoDI 4161.02, *Accountability and Management of Government Contract Property,* as required by contract.

5.14.4. Enclave/system ISSOs/ISSMs/CSSs maintain a listing of all contractor-owned or operated IS equipment within AF facilities.

5.14.5. Any system configuration outside the normal baseline client image requires documentation in the IS security authorization package and program contract.

5.15. Foreign-Owned Information Systems. Do not use foreign-owned or -operated (e.g., joint/coalition) IS hardware or software to process US sensitive or classified information for critical processing, unless required by international treaties or security agreements. See CJCSI 6211.02, CJCSI 6510.01, and DoDD 5230.11 for more information.

5.16. Other Service or Agency Owned Information Systems. Other service/agency-owned and operated ISs (i.e., Army, Navy, State Department, etc.) should meet all security requirements for connection to the AFIN as defined in AFI 17-101 and DoDI 8510.01. Follow reciprocity and reuse procedures IAW DoDI 8510.01.

Chapter 6

REMANENCE SECURITY

6.1. Introduction . Remanence is the residual information remaining on storage media. REMSEC actions are taken to protect the confidentiality of information on ISs (to include infrastructure devices such as routers and switches). See the IS security authorization package for system specific incident response and REMSEC procedures. Exercise risk management procedures IAW DoDI 8500.01, CJCSI 6510.01, and NIST SP 800-88, *Guidelines for Media Sanitization*.

AF policy is to safeguard classified and sensitive information, no matter what the media. Safeguarding classified and sensitive information in computer memory and media is particularly important during routine maintenance, product end of life, and reuse. ISOs, privileged users, ISSMs, ISSOs, WCOs, operations personnel, and other responsible people should know the risk factors before sanitizing ISs media and releasing them from the controlled environment. To protect against compromise allow only authorized and properly cleared persons with a need to know access to media containing classified and sensitive information.

6.1.1. Risk Assessment. Balance risk management decisions on information sensitivity, threats and vulnerabilities, and the effectiveness and potential impact of the decided action.

6.1.1.1. When assessing the risk of releasing ISs media from DoD control, the ISSO should develop procedures that identify the residual risk and risk tolerance (the acceptable level of risk as determined by the ISO). Follow the guidance in MPTO 00-33B-5008, Appendix C, and NIST SP 800-30, Revision 1, *Guide for Risk Assessments*.

6.1.1.2. The ISSO, assisted by the WCO, assesses the risks in consultation with the Wing IP Office before deciding whether to sanitize for reuse or disposal.

6.1.1.3. The ISO considers the full range of vulnerabilities and security implications to include the actual loss if an unauthorized entity extracts the residual information, the threat directed against this information, the threat of recovery, and the potential for damage. See MPTO 00-33B-5008 for risk management guidance.

6.1.2. Risk Management. Utilizing REMSEC within an organization is a risk management process that involves the information owner, ISO, ISSM, ISSO, and security manager to make a determination of potential impact prior to sanitizing media or devices for reuse or disposal. The decision is based on a complete risk analysis that involves the identification of organizational mission, mission impacts, threats, and possible compromise to the IS or information. A thorough cost benefit analysis coupled with mission priorities provides the framework for this decision.

6.1.2.1. Once the risk analysis has been completed, document the mitigations and any residual risk in the IS security authorization package SSP and Plan of Actions and Milestones (POA&M).

6.1.2.2. As the monetary cost of media decreases, the cost of sanitizing media may become impractical and destruction may become more cost effective. Costs to be considered in the sanitization and destruction decision include purchase price of sanitization software and degaussing/destruction equipment, periodic recertification of

equipment, cost of outsourcing, and time required for verification, documentation, and tracking of sanitized media.

6.2. Sanitization. REMSEC actions to sanitize medium (smartphone, Flash, random access memory [RAM] and read only memory [ROM], optical disks, solid state drives [SSDs], magnetic disks, hard disk drives [HDD], etc.) is dependent upon classification of data contained within the device.

6.2.1. Sanitization of unclassified devices follows NIST SP 800-88. The term "sanitization" is defined in SP 800-88 as a process to render access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media.

6.2.1.1. Clear – A method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

6.2.1.2. Purge – A method of sanitization that applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques.

6.2.1.3. Destroy – Renders target data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

6.2.2. Sanitization of classified devices follows the NSA/Central Security Service (CSS) Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, and involves the destruction of the media and/or data via degaussing, incineration, disintegration, shredding, embossing/knurling, chopping/pulverizing/wet pulping (paper), grinding, strip shredding/cutting, or power removal (dynamic random-access memory [DRAM], static random-access memory [SRAM], volatile Field Programmable Gate Array [FPGA]). Only products listed on the NSA Evaluated Products List (EPL) or received approval from NSA may be used to destroy classified information (to include media and devices) per NSA/CSS Policy Manual 9-12. Contact the NSA/CSS System and Network Analysis Center (SNAC) at (410) 854-6358 or via email at **SNAC@radium.ncsc.mil**, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associated materials.

6.2.2.1. Degauss (HDD/Diskettes) – Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. Classified IT storage media cannot be declassified by overwriting per DoDM 5200.01, Volume 3.

6.2.2.2. Embossing/Knurling (CDs/DVDs) – One or two rotating knurled shafts press down on the surface, elongating the focal point and making all information unreadable and inaccessible.

6.2.2.3. Grinding (CDs) – Sanitize by destroying the surface of the optical storage media; DVDs and Blu-Ray disks have information layers in the middle of the disk, making grinding ineffective for sanitization.

6.2.2.4. Disintegration (HDD/Diskettes/CDs/DVDs/SSDs) – Reduces the storage media into small fragments of a specific size, depending upon the type, using a knife mill.

6.2.2.5. Incinerate (HDD/Diskettes/CD/DVD/BluRay Disks/SSD) – Destruction using high heat/temperatures to reduce the media into ash.

6.2.2.6. Shredding (Diskettes/CD/DVD) – Physical shredding of media into small strips using two interlocking patterned drums that rotate in opposing directions.

6.2.2.7. Power Removal (DRAM/SRAM/volatile FPGA) – Clearing of volatile memory by removing power source for a specific duration.

6.2.2.8. Strip Shredding or Cutting (smart cards only) – Destruction of smart cards by cutting or shredding in small pieces.

6.2.3. When sanitization cannot be accomplished (e.g., inoperable disk), destroy the media IAW DoDM 5200.01, Volume 3.

6.2.4. Before media can be reused in a classified environment or released from organizational control, complete a separate administrative procedure for declassification. To determine the classification of the data, consult the applicable system classification guide. The Defense Technical Information Center (DTIC) maintains a repository and index of security classification guides IAW DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification,* or contact the system/enclave ISSM for a copy.

6.3. Media Reuse. Sanitize media to ensure that no data or information remains on operable media that are to be reused within the DoD.

6.3.1. Clear unclassified media before reuse; purge media containing sensitive data (e.g., PII) prior to reuse. Reference NIST SP 800-88.

6.3.2. Clear classified media before reuse and reuse only in a classified environment IAW CJCSI 6510.01.

6.4. Disposal. Disposal is the process of reutilizing, transferring, donating, selling, destroying, or other final removal of media from service. Disposal of government hardware and software is governed by DoDM 4160.21, Volume 4, *Defense Materiel Disposition Manual: Instructions for Hazardous Property and Other Special Processing Materiel*, and DoDM 4160.21, Volume 2, *Defense Materiel Disposition Manual: Property Disposal and Reclamation*.

6.4.1. Purge or destroy all unclassified IS storage media before leaving the control of the DoD, IAW NIST SP 800-88.

6.4.1.1. Dispose of unclassified electronic media IAW NIST SP 800-88. Dispose of unclassified computing systems and hard drives IAW DoDM 5200.01, Volume 3, Enclosure 7. When no longer needed, unclassified computer systems and hard drives may be disposed of outside the DoD. In some circumstances, the equipment may be provided to non-government entities for reutilization.

6.4.1.2. The Defense Logistics Agency Disposition Services (DLADS) disposes of excess property received from the military services. Turned in property is first offered for reutilization within the DoD, then transfer to other federal agencies, or donation to state/local governments and other qualified organizations. The demanufacture (DEMAN) program is the resource recovery and recycling program designed to reclaim precious metals and recycle scrap for equipment that is not usable (end of lifecycle, destroyed, etc.). For more information about the DLADS, see **http://www.dispositionservices.dla.mil**.

6.4.1.3. Track and dispose of unclassified IS storage media previously contaminated with classified data as classified media IAW CJCSI 6510.01. Reference DoDM 5200.01, Volume 3, Enclosure 3 for disposal and destruction of classified hard drives, electronic media, processing equipment components, etc. Destroy and declassify IAW NSA/CSS Policy Manual 9-12. Document destruction using guidance IAW MPTO 00-33B-5008.

6.4.2. Destroy all classified IS storage media unless being used in an IS environment at the same or higher classification level. Reuse of classified IS storage media in unclassified environments is prohibited. At the end of life, destroy IAW CJSCI 6510.01 and the sanitization/declassification procedures of NSA/CSS Policy Manual 9-12. For installations without the means to sanitize or verify sanitization, NSA does accept and destroy some classified media. Follow the guidance on the NSA Classified Materiel Conversion (CMC) for packaging, documenting, and shipping devices at **https://www.nsa.gov/cmc/**. Direct questions to the CMC Customer Service Office at 301-688-6672 or via email at **cmc@nsa.gov**.

6.5. Mixed Media Devices. Determine the sanitization requirements of mixed media devices, following MPTO 00-33B-5008, NSA/CSS Policy Manual 9-12, and NIST SP 800-88. Sanitization is complete by appropriately sanitizing all the media contained within the device. Hardware such as routers, switches, MFDs, etc., may contain multiple types of media and the sanitization methods are based on the type of media and the classification of the operational environment. Most network architecture devices have solid-state storage devices such as RAM, ROM, FPGA, smart cards, and Flash Memory. DRAM, SRAM, Ferroelectric RAM (FRAM), Magnetic RAM (MRAM), Erasable Programmable Read Only Memory (EPROM), Ultra-Violet EPROM (UVEPROM), and Electrically EPROM (EEPROM) have specific sanitization requirements.

Chapter 7

COMPUSEC ASSESSMENTS

7.1. Purpose . The COMPUSEC Assessment is designed to provide Cybersecurity personnel assistance with implementing and maintaining a cybersecurity program.

7.2. Objective . The COMPUSEC Assessment is a "find and fix" program review, essentially functioning as a staff assistance visit and therefore, the COMPUSEC Assessment is not intended to replace, but rather augment, the Air Force Inspection System (AFIS) and strengthen the AF cybersecurity program IAW AFI 17-130 and AFI 90-201, *The Air Force Inspection System*.

7.2.1. In instances where local inspection authorities (e.g., Wing Inspection Teams) are already performing inspection activities in partnership with the WCO, conduct a separate annual COMPUSEC assessment at the discretion of the WCO and organizational commander.

7.2.2. WCO assessments may be combined with MAJCOM IG inspections that assess COMPUSEC criteria.

7.2.3. Results of these inspections satisfy annual COMPUSEC assessment reporting requirements in paragraph 7.4.

7.3. Assessment Process . WCO will perform annual assessments of all units utilizing IT under the control of the base communications unit, including IT of tenant units (i.e. FOAs, DRUs, and other service units) unless formal agreements exist. **(T-1).** For Joint bases, the AF is responsible for all AF-owned IT and infrastructure. The annual period is defined as the 12-month timeframe since either the last WCO Assessment or MAJCOM IG Inspection.

7.3.1. Assessments consist of an interview and site visit with the applicable ISSO/ISSM/CSS. During the interview, the WCO reviews all responses annotated on the AFMAN 17-1301 COMPUSEC MICT SAC (**https://mict.us.af.mil/**) provided by the ISSO/ISSM/CSS during the last self-assessment. As part of the site visit, the WCO may assess organizational compliance with any COMPUSEC criteria as outlined in this manual. Sample assessment items may be found on the IACE. Additional areas for review are at the discretion of the WCO.

7.3.1.1. For geographically separated units (GSUs), remote interviews (i.e., over the phone) are acceptable in lieu of a site visit when travel costs are a concern.

7.3.1.2. In-brief, out-brief, and other formalization of assessment processes are at the discretion of the WCO and the assessed unit.

7.3.2. Assessments are not graded, but should instead provide organizational commanders an accurate COMPUSEC posture indication by itemizing the deficient COMPUSEC items and summarizing additional observations, recommendations, and best practices.

7.4. Reports. COMPUSEC Assessment Reports provide a narrative description of the deficiencies and significant trends identified during the annual COMPUSEC Assessment. Reports consist of detailed unit reports, follow-up reports, and annual executive summaries.

7.4.1. Detailed unit reports include a narrative of deficient COMPUSEC items, impacts if deficiencies are not corrected, additional areas assessed, assistance provided, recommendations, and best practices. **(T-1)**. Generate and provide detailed unit reports to organizational Commanders (or equivalent) no later than (NLT) 10 days after the COMPUSEC Assessment is completed. **(T-1).**

7.4.2. Follow-up reports addressing any open findings will be completed by the assessed unit every 30 days, endorsed by the organizational commander (or equivalent), and sent to the WCO for review. **(T-1).** Findings remain open until considered closed by the WCO that performed the assessment.

7.4.3. Annual executive summary reports reflect the status of the COMPUSEC posture of the Wing (or equivalent) and include a summary of deficient COMPUSEC items, impact if deficiencies are not corrected, assistance provided, and recommendations. **(T-1).** WCOs will generate and provide annual executive summary reports to the Wing Commander (or equivalent) NLT 31 January of each year. **(T-1).** No reply or follow-up is required on executive summary reports.

Chapter 8

PUBLIC KEY INFRASTRUCTURE

8.1. Introduction. A vital element of the DoD defense-in-depth strategy is the use of a common, integrated DoD PKI to enable network security services throughout the enterprise. 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 (email) and documents. PKI verifies identities using digital signatures and certificates.

Implementation of PKI through PK enabling is required on all IT IAW DoDI 8520.02 and DoDI 8520.03.

8.2. PKI Guidance . The DoD and the CNSS PKIs have various tokens that are used with the DoD and AF. PKI hardware tokens provide two-factor authentication IAW DoDI 8520.02, to DoD and AF ISs and access to DoD and AF Directory Services domains on NIPRNet and SIPRNet. The DoD and the CNSS PKIs use asymmetric cryptography to identify and authenticate users to systems and networks for the NIPRNet and SIPRNet.

8.2.1. DoDI 8500.01 requires the use of certificates issued by DoD-approved identity credentials to authenticate to DoD ISs.

8.2.2. The CAC is the primary hardware token for identifying individuals for access to NIPRNet assets and physical access to DoD facilities according DoDI 8520.02, DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, and AFI 31-101.

8.2.2.1. There are special instances where the CAC cannot be used. For these unique situations, the DoD CIO has approved the use of the Alternate Logon Token (ALT).

8.2.2.2. The NIPRNet Directory Services domain and SIPRNet legacy Directory Services domains are defined in the DISA STIGs as General Business Enclave LANs. All accounts and computers in Directory Services are required to use PKI.

8.2.2.2.1. Annotate smart card removal and screensaver exemptions that are allowed for very limited use cases in the enclave/system security authorization documentation IAW the applicable DISA Operating System STIG.

8.2.2.2.2. Submit Service Requests to AFSPC CYSS/CYZ PKI, (**afspc.cyss.cys.2@us.af.mil**) when a normal Directory Services-joined computer cannot fulfill the organizations requirements.

8.2.3. Identity Credential Determination. DoDI 8520.03 requires that the ISO determines the "Credential Strength" used to authenticate to the DoD IS by assessing the "Sensitivity Level" of the information contained in the DoD IS.

8.3. NIPRNet PKI. The most commonly used unclassified PKI hardware token or smart card is the CAC. The ALT can be issued in circumstances where the CAC cannot be issued to an individual. The Volunteer Logical Access Credential (VoLAC) can be issued to eligible volunteers. If there are validated circumstances where a NIPRNet token cannot be used, a NIPRNet Smart Card Logon (SCL) waiver allowing the use of username and password may be authorized. Contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) for guidance.

8.3.1. AFI 36-3026 IP, Volume 1, *Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, identifies the individuals that are eligible for CACs. Individuals should be issued a separate CAC for each persona (e.g., Active Duty Service Member, Reserve or Guard Member, Government Civilian, Contractor) IAW DoDM 1000.13, Volume 1. This role or persona is commonly referred to as a Personnel Category Code (PCC).

8.3.1.1. For uniformed services personnel and DoD civilians, all submissions to DoD Enrollment Eligibility Reporting System (DEERS) can be made electronically via an authorized data source feed (e.g., Civilian Personnel Management Service).

8.3.1.2. The Defense Manpower Data Center (DMDC), as the administrator of DEERS and the Real-Time Automated Personnel Identification System (RAPIDS), requires the use of the Trusted Associate Sponsorship System (TASS) for requesting CACs for "DoD PKI Certificate Eligible Users," IAW DoDM 1000.13.

8.3.1.2.1. DoD PKI Certificate Eligible Users are authorized DoD volunteers, State, local, or tribal government employees, or interns as defined DoDI 8520.02. To begin the process for VoLAC issuance, to include completion of DD Form 2793, *Volunteer Agreement for Appropriated Fund Activities and Non-Appropriated Fund Instrumentalities,* contact supporting TASS Trusted Agent (TA). The TA establishes sponsorship of the applicant, verifies the access requirements, and initiates the application process in TASS.

8.3.1.2.1.1. 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 Department of Defense (DoD) CAC Defense Enrollment Eligibility Reporting System (DEERS) Enrollment*.

8.3.1.2.1.2. TASS allows "DoD PKI Certificate Eligible Users" 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 (NAF) Employees, outside the continental U.S. (OCONUS) Hires, Other Federal Agency Contractors to apply for a CAC or other government credential electronically through the Internet. Government sponsors of DoD contractor personnel should contact their supporting TASS TA to request an application for an eligible contractor to receive government credentials.

8.3.1.2.1.3. Follow the guidance provided in DoDM 1000.13 and the TASS TA user manual.

8.3.1.2.2. Unfunded contract options (annotated in the contract as the period of performance [PoP]) are considered in the determination of the length of contract. For example, a contractor hired under DoD contract with a base year plus two option years should be issued a CAC with a 3-year expiration. The expiration date of the PKI certificates on the CAC should match the expiration date on the card. If contract option years are not exercised, the COR notifies the TASS TA to revoke contractor access.

8.3.1.3. Dual-role personnel have more than one role/persona (e.g., Civilian and Reservist, Contractor and Air National Guard); the individual is required to have and use the appropriate CAC for each role. At issuance, the CAC should not have the individual's PCC appended to his or her Electronic Data Interchange Personal Identifier (EDI-PI). Append PCCs at the RAPIDS Self Service Portal (**https://www.dmdc.osd.mil/self_service/rapids/unauthenticated?execution=e2s1**). Set the CAC/Directory Services account that the individual uses the most with **EDI-PI@MIL**, and set the CAC/Directory Services account that is used the least with **EDI-PI.PCC@MIL**. Each time a new CAC is issued, append the PCC.

8.3.1.4. Authorized DoD volunteers, State, local, or tribal government employees, or interns are "DoD PKI Certificate Eligible Users" IAW DoDI 8520.02. Contact supporting TASS TA to begin the process for VoLAC issuance, to include completion of DD Form 2793. The TA enters user information into TASS.

8.3.1.5. Air Force Personnel Center (AFPC) manages the issuance of CACs through DEERS/RAPIDS. On AF installations, the AF Military Personnel Section (MPS) issues the CAC. On non-AF locations, any RAPIDS can issue a CAC to any authorized Service Member, Government Civilian, or DoD Contractor. DoD Contractors contact their unit's TASS TA prior to making an appointment with their supporting MPS to have their information entered or updated in DEERS.

8.3.1.6. Turn in expired, unneeded, or found CACs or VoLACs to the nearest RAPIDS facility by the individual, Contracting Officer's Representative (COR) for DoD contractors, or TASS TA.

8.3.2. The ALT is another form of a DoD authorized PKI hardware token or smart card that can be issued to individuals for logical access to NIPRNet. Currently, there is not an ALT-like capability on SIPRNet.

8.3.2.1. Individuals who are ineligible for receiving a CAC (e.g., Italian Nationals) or the support staff serving a General Officer (GO) or Senior Executive Service (SES) (e.g., PKI Tier-1) can be issued an ALT with DoD PKI certificates. See T.O. 31S5-4-7282-1, *Alternate Logon Token (ALT) Issuance Standard Operating Procedures,* for specific issuance criteria or eligibility.

8.3.2.2. The user/requestor should contact their base ALT TA, usually assigned to the supporting base communications unit or Communications Focal Point (CFP), to begin the ALT issuance process. For a list of each base's ALT TAs, see **https://afpki.lackland.af.mil/html/b-alttokencontacts.cfm**.

8.3.2.3. Turn in expired, unneeded, or found ALTs to the nearest AF base's ALT TA.

8.3.3. Most commercially available token readers (separate device or integrated into a keyboard) can be used on the NIPRNet; there is no approved or banned product list. Only use the latest approved version of middleware on NIPRNet. Remove all other middleware products from the IS.

8.3.4. Maintain positive control over hardware token at all times IAW AFI 36-3026.

8.3.4.1. Do not leave any unclassified PKI hardware token in an unattended computer.

8.3.4.2. The person who is issued a hardware token maintains positive control of the token at all times and the embedded certificates IAW the applicable CNSS guidance, DoD *Registration Practice Statement (RPS),* or *United States Department of Defense X.509 Certificate Policy*.

8.3.4.3. Introduction of SIPRNet hardware tokens on NIPRNet ISs are not authorized. If a SIPRNet hardware token has been used on an unclassified IS, see paragraph 8.4.6 for guidance.

8.3.5. Implement SHA-256 algorithm on all DoD IT infrastructure (hardware and software) on both NIPRNet and SIPRNet IAW the *DoD Secure Hash Algorithm-256 Transition Plan*.

8.3.5.1. All DoD Components are required to support DoD-approved SHA-256 PKI credentials for digitally signing and encrypting emails, logging onto DoD networks, and authenticating to systems no later than September 30, 2017.

8.3.5.2. All NIPRNet Systems are required to be SHA-256 compliant according to SAF/CIO A6 or submit a POA&M to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**). To be compliant, all systems, websites, web capabilities, network devices, and software should be capable of utilizing the SHA-256 certificate or SHA-256 certificates when issuance on the CAC begins.

8.3.5.3. Follow FIPS 180-4, FIPS 140-2, and the validation lists available through the NIST CMVP and the CAVP sites (**http://csrc.nist.gov/groups/STM/cmvp/index.html**).

8.4. SIPRNet PKI. The SIPRNet hardware token is the primary means for logical access to SIPRNet. If there are validated circumstances where a SIPRNet token cannot be used, a SIPRNet SCL exemption allowing the use of username and password may be allowed IAW MTO 2013-077-002C (or current update of the MTO). Contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) for guidance.

8.4.1. Ensure all SIPRNet networks utilize the National Security Systems (NSS) Root Certificate Authority (CA) and are current with all PKI security patches and configuration settings IAW the applicable Certificate Practice Statement (CPS).

8.4.2. Individuals who have a SIPRNet Directory Services account are required to use SIPRNET hardware tokens IAW USCYBERCOM TASKORD J3-12-0863, Fragmentary Order (FRAGO) 2.

8.4.3. The LRA, normally residing at the supporting base normally within the base communications unit or CFP, issues the SIPRNet hardware token or smart card. The SIPRNet hardware token provides authorized users with an identity certificate, digital signature certificate, and an encryption certificate. With appropriate network configuration, the SIPRNet hardware token or smart card provides user authentication and non-repudiation for network logon.

8.4.4. The SIPRNet hardware token or smart card is a high-value unclassified item. Maintain the SIPRNet hardware token IAW CNSSI No. 1300, *National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25,* and the *National Security Systems Public Key Infrastructure, Department of Defense Registration Practice Statement (RPS).*

8.4.4.1. A SIPRNET token is classified SECRET when inserted into the SIPRNET hardware token reader and the personal identification number (PIN) is entered. It is considered unclassified when removed from the SIPRNET token reader or if it is inserted into the token reader but the PIN is not entered.

8.4.4.2. Do not leave the SIPRNet hardware token unattended in computer network resources.

8.4.4.3. Maintain the SIPRNet hardware token in the positive control of the authorized user, who is represented by the embedded certificates IAW the applicable CNSS policy or RPS. Turn-in expired, unneeded, or found SIPRNet hardware tokens to the nearest NSS LRA by the individual, COR for DoD Contractors, or TASS TA. *Note:* Do not return the found SIPRNet hardware token back to the individual. See paragraph 8.16 for key compromise guidance.

8.4.4.3.1. Positive control includes maintaining visual contact when in use, and retention on the person or secured when not in use. SIPRNET tokens are considered secured when locked or stored within a container (e.g., desk) inside a facility authorized for the protection of SECRET. Only the assigned user is authorized to use the SIPRNET token.

8.4.4.3.2. Contact the supporting LRA to revoke SIPRNet hardware token certificates when there is suspected loss of positive control or unauthorized use of the token or a certificate. Return any token determined to be temporarily out of the positive control of the assigned user to the LRA. When returned, zeroize the private keys and revoke the certificates. If zeroizing and revocation is not possible or if there is evidence of tampering with the SIPRNet hardware token, the LRA returns the token to NSA for investigation and/or destruction.

8.4.4.3.3. If the SIPRNet hardware token is lost or stolen and not recovered, immediately report this information to the LRA to initiate the revocation process IAW the applicable CPS. Issuance of a new SIPRNet hardware token is authorized after a dated and signed memorandum (wet or digital signature acceptable) on organizational letterhead by the requesters Commander authorizing the issuance, is provided to the LRA.

8.4.4.3.4. AF GO and/or SES members are authorized to retain their SIPRNet hardware token during a permanent change of station (PCS). All other AF SIPRNet users are required to turn–in their SIPRNet hardware token when undergoing a PCS or permanent change of assignment (PCA) (see paragraph 8.4.5.3.4.2).

8.4.4.3.4.1. The GO/SES or designated representative notifies the losing base LRA, either in person or through a digitally-signed e-mail stating that he/she is taking the SIPRNet hardware token to the new location and site code needs to be changed/updated. The losing base LRA changes the site code for the registration tied to the SIPRNet hardware token of the GO/SES in the Token Management System (TMS). The losing base LRA notifies the gaining base LRA of the transfer through a digitally signed e-mail.

8.4.4.3.4.2. Any user may retain their SIPRNet hardware token during PCA, if the issuing LRA remains the same.

8.4.4.3.5. Enclave or system ISSM/ISSO notifies the base LRA of expired accounts (see paragraph 4.6.1.2); the base LRA contacts users and recovers the SIPRNet hardware tokens from them.

8.4.4.3.6. Base communications unit will update their portion 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 hardware token to the base LRA prior to signing off the individual's Base Out-processing Checklist. **(T-1).** Contractors contact their unit's CSS to terminate their SIPRNet account and turn-in their SIPRNet hardware tokens to the base LRA at the end of the contract PoP.

8.4.5. Prohibit the introduction of (operational) SIPRNet hardware tokens on unclassified ISs and the introduction of unclassified tokens (e.g., CAC, ALT, Personal Identity Verification [PIV], VoLAC, and or Personal Identity Verification-Interoperable [PIV-I]) on classified ISs.

8.4.5.1. SIPRNet hardware tokens inserted into an unclassified IS may result in a security violation. Report suspected incidents to the WCO and local security manager to determine if the incident is a security violation. Follow the guidance in DoDM 5200.01, Volume 3. Note: This does not apply to SIPRNet hardware token testing cards on unclassified test beds.

8.4.5.2. The SIPRNet "90meter©" middleware configuration detects the NIPRNet token, blocks PIN entry, and blocks any service applets that do not require PIN entry.

8.4.5.3. An unclassified hardware token inserted into a SIPRNet IS may result in a security violation. Report suspected incidents to the WCO and local security manager to determine if the incident is a security violation. Follow the guidance in DoDM 5200.01, Volume 3.

8.4.6. Connect only authorized SIPRNet hardware token readers (i.e. Omnikey 3121, SCM 3310) to SIPRNet ISs. The connection of keyboards with built-in CAC readers and external USB CAC readers to classified ISs are not permitted.

8.4.6.1. Permit only the latest version of "90meter©" middleware and configure it to activate only SIPRNet hardware tokens initialized for use on the SIPRNet.

8.4.6.2. In the AF, "ActivClient©" middleware is not authorized on SIPRNet.

8.4.7. All SIPRNet Systems are required to be SHA-256 compliant according to SAF/CIO A6 or submit a POA&M to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**). To be compliant, all systems, websites, web capabilities, network devices, and software should be capable of utilizing the SHA-256 certificate or SHA-256 certificates when issuance on the SIPRNet hardware token begins. Follow FIPS 180-4, FIPS 140-2, and the validation lists available through the NIST CMVP and the CAVP sites (**http://csrc.nist.gov/groups/STM/cmvp/index.html**).

8.5. User or Administrator Password/PIN Management. Passwords may be allowed only when the AF PKI SPO has evaluated the AF Information System and has validated that the use of PKI smart cards or other approved two factor authentication is not technologically feasible; contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) for guidance. Specific procedural information for password/PIN management is located in MPTO 00-33B-5004. In addition to the AF-specific password guidance contained in the MPTO 00-33B-5004, configure IS password authentication IAW the applicable DISA Operating System STIGs. DISA STIG and/or USCYBERCOM TASKORD password requirements take precedence only if more restrictive than guidance in this publication.

8.5.1. Classify and protect passwords/PINs at the highest level of information processed on that system. As a minimum, safeguard passwords as FOUO. See DoDM 5200.01, Volume 1, for a detailed explanation of FOUO.

8.5.2. Classified passwords/PINs that are necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise) may be sealed in a properly marked envelope or annotated on a SF 700, *Security Container Information*, and stored in a GSA-approved container as specified in DoDM 5200.01, Volume 3.

8.5.3. Protect all passwords/PINs during transmission using FIPS-approved encryption IAW CJCSI 6510.01.

8.5.4. All passwords for AF ISs are required to comply with the following password management criteria.

8.5.4.1. To the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. All factory set, default or standard-user IDs and passwords are removed or changed.

8.5.4.2. Authenticators are protected commensurate with the classification or sensitivity of the information accessed, they are not shared, and they are not embedded in access scripts or stored on function keys.

8.5.4.3. Passwords are encrypted both for storage and for transmission. Store passwords in an authentication system that minimizes their exposure to disclosure or unauthorized replacement. Encryption of electronically stored passwords and password files is required.

8.5.4.4. Service Account passwords have different requirements than user passwords; see paragraph 8.21.

8.5.4.5. Case sensitive, at least 15-character mix of two upper case letters, two lower case letters, two numbers, and two special characters. For password changes, change at least four characters when a new password is created.

8.5.4.6. The ISO ensures the establishment of procedures for manual or automatic password changes by users, administrators, and machine-to-machine interfaces; password changes occur at least every 60 days or more frequently as determined by the ISO, IAW CJCSI 6510.01.

8.5.5. For systems that are not joined to the Directory Services domain and require shared/group passwords, the system ISSM requests approval from the AO IAW CJCSI 6510.01. Implement system and physical auditing procedures to support non-repudiation and accountability. For more information on waiving DoD or AF PKI requirements, see paragraph 8.22.

8.5.5.1. Unauthorized sharing of passwords/PINs is a security incident IAW CJCSI 6510.01.

8.5.5.2. Incorporate electronic or paper tracking methods to account for user activity when using AO-approved shared passwords IAW CJCSI 6510.01.

8.5.6. In the event of a compromised password/PIN, the ISO and the ISSM ensures procedures are in place to implement immediate password/PIN change activities. A compromised PKI PIN warrants probable compromise of the associated certificates. See paragraph 8.16.

8.6. PIN Caching Setting . All NIPRNet and SIPRNet DoD ISs and Directory Services domains and domain-joined computers are required to be configured for PIN caching, set to 10 minutes.

8.7. Organizational Electronic Mailbox . Disable Directory Services objects that are associated with Organizational Mailboxes. Note: Organizational Mailboxes and Organizational Accounts are two different capabilities and are not related.

8.7.1. The Organizational Mailbox Manager should grant access from the actual Organizational Mailbox. The Organizational Mailbox Manager is the person whose name appears in Directory Services as the Manager of the Organizational Mailbox. Use IAO Express to add or change the Organizational Mailbox Manager in Directory Services/Exchange.

8.7.2. The sponsor appointed for the Organizational Mailbox manages the Encryption Certificate associated with the Organizational Mailbox. The Sponsor is the person who requests, issues, and manages the Encryption Certificate. The Organizational Mailbox Sponsor should follow the procedures for managing the Organizational Mailbox Encryption Certificate found on the AF PKI SPO website (**https://afpki.lackland.af.mil/**).

8.8. Organizational Accounts. Organizational Accounts are Active Accounts that individuals use to logon using DoD-approved PKI and accesses the electronic mailbox associated with the Organizational Account (e.g., AFSPC/CC, AFSPC/CCC, AFSPC/CCF). Each individual should have a unique identifier that the system can authenticate and provide an audit trail. The Organizational Accounts are unique since a DoD approved hardware token is used to logon to the associated Directory Services account to access files or email.

8.8.1. In order for multiple users to access the same Organizational Account, each person should possess a unique DoD approved hardware token (e.g., ALT). More than one person cannot share a single DoD approved hardware token.

8.9. Group Accounts Utilizing PKI. Group accounts (not to be confused with organizational accounts) are special case accounts where more than one person may access the same account using a DoD-approved PKI credential IAW DoDI 8520.02.

8.9.1. The approval authority for group accounts is one of the applicable AOs; see boundary specific appointment letters **https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/afcks/AFAAP/Lists/DAA_Program/AO_Public.aspx**.

8.9.1.1. For AFIN group accounts, the approval authority is the Enterprise AO. To begin the AFIN approval process, contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) to determine if the appropriate solution is the use of a group account. AFSPC CYSS/CYZ PKI identifies the appropriate next step in the approval process.

8.9.1.2. For non-AFIN group accounts, the approval authority is the applicable AO for the specific boundary.

8.9.2. Authorized users request individual ALTs to access the group account; each token contains an individual identification certificate. See paragraph 8.3.2.

8.9.3. The ALT Sponsor maintains an inventory of token serial numbers and assigned users at all times.

8.9.4. Requests for group account ALTs should follow T.O. 31S5-4-7282-1.

8.10. External PKI. To begin the approval process for External PKI as authorized by DoDI 8520.02, contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**). AFSPC CYSS/CYZ PKI identifies the appropriate next step in the approval process.

8.11. Enterprise Certificate Trust Governance. Identity assurance must be applied to ensure strong identification and authentication, and to eliminate anonymity in DoD IS and PIT systems. DoD will public key-enable DoD ISs and implement a DoD-wide PKI solution that will be managed by the DoD PKI Program Management Office in accordance with DoDI 8520.02. The AF Certificate Trust baseline provides a white/black list of PKI Certificate Authorities (CAs) trust anchors (or roots) to secure AF systems from trusting unknown and/or untrusted issuing CAs. It includes a minimum number of roots required for the OS to operate and to support specific enterprise applications. The AF Certificate Trust Store Governance process exists to manage the baseline and provide a formal means to add and remove roots at the enterprise level.

8.11.1. If an AF IS user attempts to go to a website where the root CA has expired and is no longer being updated, a "Certificate Error" warning is displayed in the web browser.

8.11.1.1. For non-enterprise use (individual users), follow the procedures posted on the IACE.

8.11.1.2. For Enterprise use, the ISSM submits a request, on behalf of all users, to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) using the template found on the IACE.

8.12. Escrowed Certificates. The CA provides automatic escrow of the email encryption key IAW *United States Department of Defense X.509 Certificate Policy*. Perform recovery of escrowed encryption keys according to the CA associated practice statements. Recovery of Escrowed Certificates is required to read encrypted emails that were received by the user using the previous certificates.

8.12.1. Changing of employment roles (i.e. contractor-to-government civilian, military-to-contractor, etc.) may affect the users' need to know and requires the users to request manually the escrowed encryption certificate. For additional guidance, see the AF PKI SPO website (**https://afpki.lackland.af.mil/**).

8.13. Software Certificate Issuance and Control. The AF follows the methods for approving PKI certificates as prescribed in the DoD PKI RA/LRA CPS and DoD RPS, supported by the DoD X.509 Certificate Policy. AF RAs have overall management responsibility for certificate issuance with LRA/TA as base level points of contact. The AF Enterprise AO is the approving authority for each use of software certificates. To begin the approval process, the system/enclave ISSM should contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**).

8.13.1. AF PKI RAs, LRAs, CA Managers, CA Operators, System Administrators, and CA Security Managers comply with the detailed policy and procedures as applicable; see **https://afpki.lackland.af.mil/**.

8.13.2. Upon approval from the AO, the ISSM annotates the use in the authorization package (security control CM-6).

8.13.3. ISSMs ensure all devices are configured with an approved token reader or have AF Enterprise AO-approval to use software certificates IAW the DISA *Commercial Mobile Device (CMD) Policy* STIG. Identification, digital signature, and encryption software certificates are required for CMDs and have a designated sponsor appointed in writing; contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**). The AF Registration Authority (RA) or LRA, as appropriate, maintains a file of requirement validation documentation**.** For organizational email mailboxes on CMDs, follow the appropriate DISA STIG. For additional guidance, see the AF PKI SPO website (**https://afpki.lackland.af.mil/**).

8.13.3.1. For organizations working to comply with the mandate to use CAC readers and requiring the use of software certificates on enterprise activated CMDs, submit a POA&M and the token reader exceptions to the AF PKI for review and recommendation to the AF Enterprise AO.

8.13.3.2. Once approved by AF Enterprise AO, use PKI software certificates for the minimum time necessary to comply with the token reader requirement. The ISSM adds the approval to the system/enclave authorization package; approval may be a memorandum, letter, or included in the SSP.

8.13.3.3. Organizations update user training materials and annotate certificate usage in block 12 of the AF Form 4433.

8.13.4. DoD PKI certificates and associated private keys are stored in a *Public-Key Cryptography Standards (PKCS)* #12 file on a removal storage medium. Do not leave PKCS#12 files in on-line file systems and are properly installed into the cryptographic module on an IS for use.

8.13.5. Do not share personal software certificate passwords; protect the media containing private keys from unauthorized access at all times IAW paragraph 8.5.

8.13.6. The Network Operations Squadrons (NOS) verify removal of software certificate installation files (.p12 or .pfx) from hard drives and other online storage devices weekly.

8.13.6.1. Removal of software certificate files does not prevent usage of software certificates for web servers, group, or role-based functions. The process only requires removal of the ".p12" or ".pfx" transportable file object that contains the private key corresponding to the DoD trusted certificate from online accessibility after installation. **NOTE:** Some applications create files with extensions of ".p12" or ".pfx" that are NOT certificate installation files. Removal of non-certificate installation files from systems is not required.

8.14. LRA Guidance. LRAs perform some aspects of certificate issuance and management at the local level. Designated LRAs have certificate issuance authority for the entire installation, including Tenant organizations and GSUs supported by the installation. Training, appointment, and eligibility information is available on the AF PKI SPO website at **https://afpki.lackland.af.mil**. AF MAJCOMS/Bases/Sites and AF supported COCOMS can establish and maintain AF LRAs who are designated IAW procedures outlined in the CPS and RPS, meeting needs of all base, site, and tenant organizations. Designated LRAs will attend a DISA approved AF LRA training course after the AF RA Office has vetted and approved the submission package. Detailed procedures for submitting LRA packages are available at **https://afpki.lackland.af.mil/html/**.

8.15. CMD Hardware Token Readers. ISSMs ensure all devices are configured with an approved token readers and/or an AO-approved process for installation of PKI software certificates IAW the DISA *Mobile Policy* SRG. See paragraph 8.5 for password requirements for devices not capable of supporting PKI and the DISA Mobility STIGs/SRGs for guidance setting up token readers.

8.16. Key Compromise. The ISSO immediately notifies the supporting TA, LRA, or the AF RA (**afpki.registration@us.af.mil**) directly by encrypted email if an AF PKI certificate holder (software certificate or token) suspects a compromise of the holder's private key.

8.16.1. 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 user, changes in a user's legal name, or departure from the DoD. The AF RA revokes certificates suspected of key compromise within 24 hours or the next duty day (whichever is first) after notification.

8.16.1.1. Revoke all other certificates (e.g., encryption and digital signature) on the token if there is a revocation of a user's ID certificate.

8.16.1.2. Enter the revoked certificates into a DoD Certificate Revocation List (CRL). All applications (i.e., websites, etc.) should check validity (e.g., the trust path, expiration, and revocation status) of the presented certificate prior to allowing access based on PKI authentication.

8.17. Server Certificates. The AF RA is the approving authority for the issuance of Medium-Assurance DoD PKI or NSS (SIPRNet) server certificates based on validation of the certificate used to digitally sign the email submitting the certificate request form (AF RA Form 2842-2). The certificate request form and specific instructions to obtain and load DoD server certificates are available on the AF PKI SPO website (**https://afpki.lackland.af.mil/**).

8.17.1. Reissue a server certificate when the fully qualified domain name (FQDN) for the server changes or after three years.

8.17.2. All AF Web servers are issued a DoD X.509 PKI Server certificate and have 128/256-bit encryption; enable the certificate at all times IAW DoDI 8520.02.

8.18. Code Signing and Mobile Code Certificates. Code signing and mobile code certificates are specially formatted certificates used for digitally signing executable program code in any number of languages or formats.

8.18.1. The sponsor is required to submit the request for code signing and mobile code certificates to the Code Signing Attribute Authority (CSAA), AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**), to begin the process for issuance on a hardware token by the AF RA/AF PKI SPO. The sponsor coordinates with the ISSM for inclusion into the security authorization package. For additional guidance, see the *Air Force Developer's Guide for Obtaining DoD Code Signing Certificates* at the AF PKI SPO website (**https://afpki.lackland.af.mil/**).

8.18.1.1. Designate individuals authorized to receive code-signing certificates; ensure that such designations are kept to a minimum consistent with operational requirements.

8.18.1.2. Upon approval from the AF Enterprise AO, the ISSM annotates compliance in the enclave/system authorization package that code signing and/or mobile code certificates are being used SC18 and CM-5/SA-10/SI-7).

8.19. Certificate Reissuance Prior to Expiration. Certificate Sponsors (owners) needing continued PKI services ensures reissuance of their certificates no earlier than 60 days prior to the certificate expiration date in order to prevent disruption in service.

8.20. Network Authentication. Enable all unclassified networks to use hardware tokens, DoD PKI certificate-based authentication, and set authorized user accounts to require SCL by selecting, "Smart card is required for Interactive Logon," in Windows Directory Services environments. Obtain exceptions to this policy from the AF Enterprise AO via AFSPC CYSS/CYZ PKI, (**afspc.cyss.cys.2@us.af.mil**).

8.21. Directory Services Service Accounts. Service accounts for Directory Services Service Accounts-joined servers (e.g., AREA52 or SIPRNet legacy domain) are required to comply with the mandate for all Directory Services Service Accounts to use SCL. Follow the password complexity requirements listed in paragraph 8.5.4.

8.21.1. Interactive logon is not allowed for any Directory Services Service Account; the use of smart cards for logon is not possible. Therefore, a SCL exemption can be granted for Use Cases that meet the SCL exemption guidance; the base enclave ISSM should contact AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**) for more information.

8.21.2. Approve service accounts through the Change Request process IAW MPTO 00-33A-1100, *AFNet Operational Change Management Process*. Comply with MPTO 00-33D-2001 and populate the required Directory Services attributes. The ISSM documents service account approval in the security authorization package.

8.21.3. The ISSM ensures the Service Account passwords are changed as required and documents compliance in the security authorization package.

8.22. PKI Waivers. Technical solutions should be evaluated before pursuing a waiver. Coordinate and submit all PKI waiver requests to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**). See DoDI 8520.02 for PKI waiver guidance.

8.22.1. If AFSPC CYSS/CYZ PKI determines that a waiver is required, the ISO submits a waiver package (Authorization to Operate [ATO], DSAWG briefing package, topology diagram, and POA&M) through the system/enclave ISSM to AFSPC CYSS/CYZ PKI (**afspc.cyss.cys.2@us.af.mil**).

8.23. PKI LRA Assessments. LRAs perform annual self assessements using the *AF LRA PKI Self Assessment Checklist* (**https://afpki.lackland.af.mil/html/lra_trg.cfm**) and submit assessment results to the RAs.

8.24. Biometric Management. Biometrics should be fully integrated to conduct the AF mission in support of joint military operations IAW DoDD 8521.01E, *DoD Biometrics*. Configure biometric programs IAW the DISA *Biometric Security Checklist for the Access Control STIG*.

8.24.1. At the discretion of the installation commander, the collection and use of biometrics may occur at any time when a person requests or requires access to systems, facilities, and networks under the responsibility of the AF or according to host nation and Status of Forces Agreement (SOFA) agreements.

8.24.1.1. When used, biometrics are collected, matched, transmitted, stored, shared, archived, and received IAW AFI 33-332.

8.24.1.2. All biometrics data and associated information collected as a result of DoD operations or activities should be maintained or controlled by the DoD, unless otherwise specified by Defense Forensics and Biometrics Agency (DFBA) for DoD Biometrics at a later date.

8.24.2. All biometrics activities are coordinated via the sponsoring AF functional organization through the DFBA at **http://www.biometrics.dod.mil/** and approved by DoD Biometrics Executive Committee (EXCOM) before acquisition.

WILLIAM J. BENDER, Lt Gen, USAF
Chief of Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 5 United States Code (U.S.C.), § 552a, *Privacy Act,* updated December 19, 2014

Title 8 Code of Federal Regulations (CFR), *Aliens and Nationality*, January 1, 2016

Title 10, U.S.C., § 2533a, *Requirement to Buy Certain Articles from American Sources; Exceptions*, January 2, 2013

Public Law 109-364, *Title V*, Section 561, *Military Personnel Policy*, October 17, 2006

Public Law 113-283, *Federal Information Security Modernization Act of 2014,* December 18, 2014

Federal Acquisition Regulation (FAR) Subpart 25.1, *Buy American – Supplies*, *25.103 Exceptions*, June 15, 2016

Defense Federal Acquisition Regulation Supplement (DFARS) Part 225 – *Foreign Acquisition*, *Subpart 225.1, Buy American – Supplies*, *225.103 Exceptions*, June 30, 2016

CNSSI No. 1300, *National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25,* December 2014

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

CNSSP No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 10, 2013

CNSSP No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems,* October 1, 2012

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 200, *National Policy on Controlled Access Protection*, July 15, 1987

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, *Guide for Risk Assessments*, September 2012

NIST SP 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security,* June 2009

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013; Includes updates as of January 22, 2015

NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, December 2014; Includes updates as of December 18, 2014

NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization,* December, 2014

NIST Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001; Includes updates as of December 3, 2002

NIST FIPS 180-4, *Secure Hash Standard (SHS),* August 2015

NIST FIPS 197, *Advanced Encryption Standard (AES),* November 2001

NSA/CSS Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual,* December 15, 2014

NSA MIT-005FS-2014, *Mitigations for Spillage of Classified Information onto Unclassified Mobile Devices (FOUO),* August 2014

NIAP, *Mobile Device Fundamentals Protection Profile,* June 10, 2016

Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,* September 15, 2008; *Technical Amendment,* July 21, 2015

CJCSI 6211.02, *Defense Information System Network (DISN): Policy and Responsibilities,* January 24, 2012

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

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010; As Amended Through February 15, 2016

National Security Systems Public Key Infrastructure, Department of Defense Registration Practice Statement, Version 8, December 19, 2014

DoD Policy Memorandum, *Mobile Code Technologies Risk Category List Update,* March 14, 2011

DoD Secure Hash Algorithm-256 Transition Plan, June 11, 2013

DoD 5200.2-R, *Personnel Security Program,* January 1987, Administrative Reissuance Incorporating Through Change 3, February 23, 1996

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* February 28, 2006; Incorporating Change 2, May 18, 2016

DoD 5400.11-R, *Department of Defense Privacy Program,* May 14, 2007

DoD 8570.01-M, *IA Workforce Improvement Program*, December 19, 2005; Incorporating Change 4, November 10, 2015

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

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

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, November 6, 1984; Incorporating Change 1, August 18, 1995

DoDD 5400.7, *DoD Freedom of Information Act (FOIA) Program*, January 2, 2008

DoDD 5400.11, *DoD Privacy Program*, October 29, 2014

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

DoDD 8140.01, *Cyberspace Workforce Management,* August 11, 2015

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

DoDI 1035.01, *Telework Policy,* April 4, 2012

DoDI 1100.21, *Voluntary Services in the Department of Defense*, March 11, 2002; Incorporating Change 1, December 26, 2002

DoDI 4161.02, *Accountability and Management of Government Contract Property,* April 27, 2012

DoDI 6025.22, *Assistive Technology (AT) for Wounded, Ill, and Injured Service Members*, January 30, 2015

DoDI 8100.04, *DoD Unified Capabilities (UC),* December 9, 2010

DoDI 8500.01, *Cybersecurity*, March 14, 2014

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* March 12, 2014; Incorporating Change 1, May 24, 2016

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

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

DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* January 23, 2014

DoDM 4160.21, Volume 2, *Defense Materiel Disposition Manual: Property Disposal and Reclamation*, October 22, 2015

DoDM 4160.21, Volume 4, *Defense Materiel Disposition Manual: Instructions for Hazardous Property and Other Special Processing Materiel*, October 22, 2015

DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification, February 24, 2012*

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information*, February 24, 2012; Incorporating Change 2, March 19, 2013

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012; Incorporating Change 2, March 19, 2013

DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI),* February 24, 2012

United States Department of Defense X.509 Certificate Policy Version 10.5, January 23, 2013

DoD Administration Instruction (AI) 117, *Telework Program*, March 31, 2015

USCYBERCOM CTO 07-015, *Public Key Infrastructure (PKI) Implementation, Phase 2,* December 11, 2007

USCYBERCOM CTO 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD),* January 8, 2008

USCYBERCOM TASKORD J3-12-0863, FRAGO 2, FOUO Title (U), July 1, 2013

USCYBERCOM TASKORD 2015-0102, *Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication,* July 6, 2015

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

AFI 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process,* December 17, 2015

AFI 16-107, *Military Personnel Exchange Program (MPEP),* February 2, 2006

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* June 2, 2015

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

AFI 16-1404, *Air Force Information Security Program,* May 29, 2015

AFI 17-100, *Air Force Information Technology (IT) Service Management,* September 16, 2014

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology,* February 2, 2017

AFI 17-130, *Air Force Cybersecurity Program Management,* August 31, 2015

AFI 17-210, *Radio Management,* May 26, 2016

AFI 31-101, *Integrated Defense*, October 8, 2009; Incorporating Change 3, February 3, 2016

AFI 31-501, *Personnel Security Program Management,* January 27, 2005; Incorporating Change 2, November 29, 2012

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, January 12, 2015

AFI 33-360, *Publications and Forms Management*, December 1, 2015

AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508,* April 10, 2013; Incorporating Change 2, June 3, 2016

AFI 36-816, *Civilian Telework Program*, November 13, 2013

AFI 36-3026_IP, Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel,* June 17, 2009

AFI 63-101/20-101, *Integrated Life Cycle Management,* March 7, 2013; Incorporating Change 3, February 23, 2015

AFI 90-201, *The Air Force Inspection System,* April 21, 2015; Incorporating Change 1, February 11, 2016

AFMAN 17-1201, *User Responsibilities and Guidance for Information Systems*, June 1, 2012

AFMAN 17-1202, *Collaboration Services and Voice Systems Management,* September 6, 2012

AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM),* March 19, 2014; Incorporating Change 1, August 28, 2014

AFMAN 17-1302, *Communications Security (COMSEC) Operations, (U//FOUO),* September 3, 2014; Incorporating Change 1, June 4, 2015

AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, March 20, 2015; Incorporating Change 1, May 26, 2016

DoD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program,* October 21, 2010; Incorporating Through Change 3, May 16, 2016

AFMAN 33-363, *Management of Records*, March 1, 2008; Incorporating Change 2, June 9, 2016

AFSPC/A6, *AF DAA Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133 Memorandum*, December 16, 2013

AFSPC/A6 Memorandum, *Guidance for Manual Data Transfers Across Security Domains*, January 10, 2012

Air Force Systems Security Instruction (AFSSI) 7700, *Emission Security*, October 24, 2007; Incorporating Change 1, April 14, 2009

MPTO 00-33A-1100, *AFNet Operational Change Management Process*, December 2, 2014

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

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

MPTO 00-33B-5004, *Access Control for Information Systems*, July 23, 2015

MPTO 00-33B-5006, *End Point Security for Information Systems,* December, 19, 2012

MTPO 00-33B-5008, *Remanence Security for Information Systems,* December 19, 2012

MPTO 00-33D-2001, Active *Directory Naming Conventions,* April 17, 2015

MTO 2013-077-002C, FOUO Title (U), FOUO Date (U)

MTO 2014-295-001, FOUO Title (U), FOUO Date (U)

T.O. 31S5-4-7255-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon / Next Generation Using Personal Identity Verification (PIV) Certificate*, August 13, 2012

T.O. 31S5-4-7256-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon / Next Generation Using Alternate Security Identification (ALTSECID),* December 13, 2011

T.O. 31S5-4-7282-1, *Alternate Logon Token (ALT) Issuance Standard Operating Procedures,* August 28, 2012, Incorporating Change 2, September 11, 2015

Air Force Developer's Guide for Obtaining DoD Code Signing Certificates, August 2014

Computer/Electronic Accommodations Program, *Handbook for Providing Assistive Technology to Wounded Service Members*, Version 1.1, November 9, 2010

AFQTP 3D0X3-211RA, *Information Assurance Manager's Handbook,* March 11, 2010

Prescribed Forms

AF RA Form 2842-2, *Air Force (AF) Registration Authority (RA) Public Key Infrastructure (PKI) Non Person Entity (NPE) Acceptance and Acknowledgement of Responsibilities*

AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement*

Adopted Forms

SF 312, *Nondisclosure Agreement*

SF 700, *Security Container Information Form*

DD Form 1172-2, *Application for Department of Defense (DoD) CAC Defense Enrollment Eligibility Reporting System (DEERS) Enrollment*

DD Form 2793, *Volunteer Agreement for Appropriated Fund Activities and Non-Appropriated Fund Instrumentalities*

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

DD Form 2946, *Department of Defense Telework Agreement*

DD Form 2987, *CAP Accommodation Request*

AF Form 847, *Recommendation for Change of Publication*

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

Abbreviations and Acronyms

ADLS—Advanced Distributed Learning Service

ADMIN-I—Admin Identity

ADP—Automated Data Processing

AETC—Air Education and Training Command

AES—Advanced Encryption Standard

AF—Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFIS—Air Force Inspection System

AFLCMC—Air Force Life Cycle Management Center

AFMAN—Air Force Manual

AFNET—Air Force Network

AFNET-S—Air Force Network-SIPRNet

AFNIC—Air Force Network Integration Center

AFPC—Air Force Personnel Center

AFPD—Air Force Policy Directive

AFQTP—Air Force Qualification Training Package

AFRIMS—Air Force Records Information Management System

AFSC—Air Force Specialty Code

AFSPC—Air Force Space Command

AFSSI—Air Force System Security Instruction

ALT—Alternate Logon Token

AO—Authorizing Official

APL—Approved Products List

ATO—Authorization to Operate

BPA—Blanket Purchase Agreement

CA—Certificate Authority

CA—Certifying Authority

CAA—Controlled Access Areas

CAC—Common Access Card

CAP—Computer/Electronic Accommodations Program

CAVP—Cryptographic Algorithm Validation Program

CCEVS—Common Criteria Evaluation and Validation Scheme

CD—Compact Disk

CDAR—Classified Data at Rest

CE—Computing Environment

CE—Continuing Education

CFP—Communications Focal Point

CFR—Code of Federal Regulation

CIO—Chief Information Officer

CISP—Commercial Internet Service Provider

CJCS—Chairman of the Joint Chiefs of Staff

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CMC—Classified Materiel Conversion

CMD—Commercial Mobile Device

CMI—Classified Message Incident

CMVP—Cryptographic Module Validation Program

CND—Computer Network Defense

CND-SP—Computer Network Defense Service Providers

CNSSI—Committee on National Security Systems Issuances

CNSSP—Committee on National Security Systems

COCOM—Combatant Command

COMPUSEC—Computer Security

COMSEC—Communications Security

COR—Contracting Officer's Representative

CPS—Certificate Practice Statement

CRL—Certificate Revocation List

CSAA—Code Signing Attribute Authority

CSS—Central Security Service

CSS—Commanders Support Staff

CST—Client Support Technician

CTTA—Certified TEMPEST Technical Authority

CTO—Communications Tasking Order

CUI—Controlled Unclassified Information

CYSS—Cyberspace Support Squadron

DAA—Designated Accrediting Authority

DAR—Data at Rest

DCS—Defense Collaboration Services

DEE—Defense Enterprise Email

DEERS—Defense Enrollment Eligibility Reporting System

DEMAN—Demanufacture

DFARS—Defense Federal Acquisition Regulation Supplement

DFBA—Defense Forensics and Biometrics Agency

DISA—Defense Information Systems Agency

DISN—Defense Information Systems Network

DLADS—Defense Logistics Agency Disposition Services

DMCC-S—DoD Mobility Classified Capability-Secret

DMDC—Defense Manpower Data Center

DMUC—DoD Mobility Unclassified Capability

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

DRAM—Dynamic Random-Access Memory

DRU—Direct Reporting Unit

DSAWG—Defense Information Assurance Security Accreditation Working Group

DSS—Defense Security Service

DTIC—Defense Technical Information Center

DVD—Digital Versatile Disc

DVS-G—DISA Video Service-Global

EDI-PI—Electronic Data Interchange Personal Identifier

EEPROM—Electrically Erasable Programmable Read Only Memory

eMASS—Enterprise Mission Assurance Support Service

EPL—Evaluated Products List

EPROM—Erasable Programmable Read Only Memory

ESD—Enterprise Service Desk

ETIMS—Enhanced Technical Information Management System

EXCOM—Executive Committee

FAR—Federal Acquisition Regulation

FDO—Foreign Disclosure Office

FIPS—Federal Information Processing Standards

FISMA—Federal Information Security Modernization Act

FiST—File Sanitization Tool

FN/LN—Foreign National/Local National

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FPGA—Field Programmable Gate Array

FQDN—Fully Qualified Domain Name

FRAGO—Fragmentary Order

FRAM—Ferroelectric RAM

GFE—Government Furnished Equipment

GIG—Global Information Grid

GO—General Officer

GSA—General Services Administration

GSU—Geographically Separated Unit

GVS—Global Video Services

HBSS—Host Based Security System

HDD—Hard Disk Drive

HIPAA—Health Insurance Portability and Accountability Act

HQ—Headquarters

IA—Information Assurance

IACE—Information Assurance Collaborative Environment

IACE-S—Information Assurance Collaborative Environment-SIPRNet

IAM—Information Assurance Management

IAM—Information Assurance Manager

IAO—Information Assurance Officer

IASAE—Information Assurance System Architects and Engineer

IASE—Information Assurance Support Environment

IAT—Information Assurance Technical

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directive

ID—Identification

IG—Inspector General

IP—Information Protection

IR—Infrared

IS—Information System

ISDN—Integrated Services Digital Network

ISO—Information System Owner

ISP—Internet Service Provider

ISSM—Information Systems Security Manager

ISSO—Information Systems Security Officer

IT—Information Technology

ITCC—Information Technology Commodity Council

JPAS—Joint Personnel Adjudication System

JTIC—Joint Interoperability Test Command

JWICS—Joint Worldwide Intelligence Communications System

KVM—Keyboard, Video, Monitor

LAN—Local Area Network

LRA—Local Registration Authority

MAJCOM—Major Command

MICT—Management Internal Control Toolset

MFD—Multifunction Device

MPS—Military Personnel Section

MPTO—Methods and Procedures Technical Order

MRAM—Magnetic RAM

MTF—Medical Treatment Facilities

MTO—Maintenance Tasking Order

NAF—Non-Appropriated Fund

NEA—Non-Enterprise Activated

NIAP—National Information Assurance Partnership

NIPRNet—Non-classified Internet Protocol Router Network

NISPOM—National Industrial Security Program Operating Manual

NIST—National Institute of Standards and Technology

NLT—No Later Than

NOS—Network Operations Squadron

NSA—National Security Agency

NSS—National Security Systems

NSTISSP—National Security Telecommunications and Information Systems Security Policy

OCONUS——Outside the Continental U.S.

OPR—Office of Primary Responsibility

OS—Operating System

PCA—Permanent Change of Assignment

PCC—Personnel Category Code

PCS—Permanent Change of Station

PED—Portable Electronic Device

PII—Personally Identifiable Information

PIN—Personal Identification Number

PIT—Platform Information Technology

PIV—Personal Identity Verification

PIV-I—Personal Identity Verification-Interoperable

PKE—Public Key Enablement

PKI—Public Key Infrastructure

PMA—PKI Management Authority

POA&M—Plan of Actions and Milestones

PoP—Period of Performance

RA—Registration Authority

RAM—Random Access Memory

RAPIDS—Real-time Automated Personnel Identification System

RDS—Records Disposition Schedule

REMSEC—Remanence Security

RF—Radio Frequency

RMF—Risk Management Framework

ROM—Read Only Memory

RPS—Registration Practice Statement

SAAR—System Authorization Access Request

SAC—Self-Assessment Communicator

SAF—Secretary of the Air Force

SCI—Sensitive Compartmented Information

SCL—Smart Card Logon

SES—Senior Executive Service

SF—Standard Form

SHA—Secure Hash Algorithm

SHS—Secure Hash Standard

SII—Special Interest Item

SIPRNet—Secret Internet Protocol Router Network

SLA—Service Level Agreement

SME PED—Secure Mobile Environment PED

SOFA—Status of Forces Agreement

SPO—System Program Office

SP—Special Publication

SRAM—Static Random Access Memory

SRG—Security Requirements Guide

SSD—Solid State Drive

SSL—Secure Sockets Layer

SSP—System Security Plan

STIG—Security Technical Implementation Guide

TA—Trusted Agent

TASKORD—Tasking Order

TASS—Trusted Associate Sponsorship System

TDY—Temporary Duty

TLS—Transport Layer Security

TMS—Token Management System

TO—Technical Order

TODA—Technical Order Distribution Account

UC—Unified Capabilities

USB—Universal Serial Bus

U.S.C—United States Code

USCYBERCOM—United States Cyber Command

UCCO—Unified Capabilities Certification Office

US—United States

UVEPROM—Ultra-Violet EPROM

VAR—Visit Authorization Request

VoIP—Voice over Internet Protocol

VoLAC—Volunteer Logical Access Credential

VVoIP—Voice and Video over Internet Protocol

VPN—Virtual Private Network

VTC—Video Teleconferencing

WCO—Wing Cybersecurity Office

WTO GPA—World Trade Organization Government Procurement Agreement

Terms

Air Force Information Network (AFIN)—AF provisioned portion of the DoDIN.

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)

Assistive Technology (AT)—AT refers to a service or device that is used to increase, maintain, or improve functional capabilities of individuals with disabilities. AT solutions may include compact keyboards, breath-controlled keyboard/mouse devices, alternative pointing devices, assistive listening devices (wired, FM, and Bluetooth), video phones, screen reader software, screen magnification software, voice recognition software, etc.

Authorized User—Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function. Authorized users include DoD employees, contractors, and guest researchers. (DoD 8570.01-M).

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 and DoDD 8521.01)

Certification Authority (CA)—An entity authorized to create, sign, and issue public key certificates. (CNSSI No. 1300)

Certification Authority System (CAS)—The collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to subscribers. (CNSSI No. 1300)

Classified Message Incident (CMI)—A higher classification level of data is transferred to a lower classification level system/device via messaging systems, e.g., email, instant messaging, etc. (AFI 16-1404)

Classified Information Spillage—Security incident that occurs whenever classified data is spilled either onto an unclassified IS or to an IS with a lower level of classification. (CNSSI 4009)

Collaborative Computing—Applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. (CNSSI 4009)

Common Criteria—Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (CNSSI 4009)

Commercial Mobile Device (CMD)—A subset of PED 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 PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers.

Computer Security—Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (CNSSI 4009)

Countermeasures—Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. (CNSSI 4009)

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoDI 8500.01)

Cybersecurity Workforce—Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. (DoDD 8140.01).

Data Spillage—Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. (CNSSI 4009)

Declassification—An administrative decision/action, based on a consideration of risk by the owner, whereby the classification of a properly sanitized storage device is downgraded to UNCLASSIFIED. (NSA Policy Manual 9-12)

Degaussing (or Demagnetizing)—Process for reducing the magnetization of a storage

device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. (NSA Policy Manual 9-12)

Destroy—A method of Sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data. (NIST SP 800-88)

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). (JP1-02)

Flash Media—Devices or products that maintain stored data without any external power source. Data can be electro-magnetically written, erased, and/or reprogrammed. General storage and example devices used for data transfers between ISs and other digital products are items such as memory cards, USB flash drives, and solid-state drives. (CNSS 4009)

Foreign Disclosure Office (FDO)—A U.S. Government official designated in writing whose primary responsibilities are to authorize disclosure of classified military information or CUI and manage and implement a disclosure program for their command or organization. (AFI 16-201)

Foreign National (FN)—Any person other than a U.S. citizen, U.S. permanent or temporary legal resident alien, or person in U.S. custody. (JP 1-02)**High Impact Personally Identifiable**

Information (PII)—Any Defense-wide, organizational (e.g., unit or office), program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act. Any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII. (DoD Memorandum, *Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)*)

IA-Enabled Product—Product whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities. **Note:** Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security enabling messaging systems. (CNSSI 4009)

IT Position Category—Applicable to unclassified DoD ISs, a designator that indicates the level of IT access required to execute the responsibilities of the position. It is based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. IT Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as outlined in DoD 5200.2-R, Appendix 10. Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national, as outlined in DoD 5200.2-R in **Chapter 3**.

Note:—The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position outlined in DoD 5200.2-R. (DoD 5200.2-R)

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

Management Internal Control Toolset (MICT)—the AF program of record to communicate a unit's current status of SAC, HAF Self-Assessment Communicator Fragmentary Order (SAC FRAGO) and Special Interest Item (SII) compliance. (AFI 90-201)

Moderate Impact PII—Any electronic records containing PII not identified as High Impact (DoD Memorandum, *Department of Defense [DoD] Guidance on Protecting Personally Identifiable Information (PII)*).

Mobile Code—Software programs or parts of programs obtained from remote ISs, 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, etc. (CNSSI 4009)

Non-Enterprise Activated (NEA) CMD—A non-enterprise activated (NEA) device is any DoD mobile handheld device that is not connected at any time to a DoD network or enterprise, and does not process sensitive or classified DoD data or voice communications. Sensitive data or

information is defined as any DoD data or information that has not been deemed as publicly releasable by a DoD Public Affairs Officer. (Mobile Policy SRG Overview)

Nonrepudiation—Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (CNSSI 4009)

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. (NIST 800-53)

Overwriting—The process of writing data on top of the physical location of data stored on the media. (NIST SP 800-88)

Periods Processing—The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next. (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)

Have the same requirements as an authorized user, but have additional permissions to configure IA-enabled software products and systems. These uses must hold baseline commercial certifications IAW DoD 8570.01-M and be placed in unit manning documented positions that require privileged access. (DoDI 8500.01)

Public Key Enable—The incorporation of the use of certificates for people, networks, systems and applications to provide security services such as strong identification, authentication, confidentiality, data integrity, and non-repudiation. (DoDI 8500.01, DoDI 8520.02, and DoDI 8520.03).

Public Key Infrastructure (PKI)—The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (CNSSI 4009)

Registration Authority (RA)—An entity (hardware, software, and individual) authorized by the (Certification Authority System) CAS to collect, verify, and submit information provided by potential subscribers that is to be entered into public key certificates. (CNSSI No. 1300)

Registration Practice Statement (RPS)—A document representing a statement of practices a RA employs when performing RA duties for a CAS. (CNSSI No. 1300)

Remanence—Residual information remaining on data media after clearing. (CNSSI 4009)

Removable Media—Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device for the purpose of storing text, video, audio, and image information. Such devices lack independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices. (CNSSI 4009)

Sanitization—The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, etc. (NSA Policy Manual 9-12)

Sanitize—A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media. (NIST SP 800-88)

Self-Assessment Communicator (SAC)—A SAC is a two-way communication tool designed to improve compliance with published guidance and communicate risk and program health up and down the chain of command in near real-time. Compliance with a SAC does not relieve individual Airmen from complying with all statutory and regulatory requirements in AFIs and directives at the local, state, or federal level. (AFI 90-201)

Sensitive Information—Information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under *Title 5 U.S.C.* Section 552a (Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy. **Note:** Systems that are not national security systems, but contain sensitive information are subject to be protected IAW the requirements of the Computer Security Act of 1987 (Public Law 100-235). (CNSSI 4009)

Sensitivity Level—Sensitivity levels relate the relative importance of information residing in a system or on a network to the potential impact that could be caused by unauthorized access or modification of that information. There are four sensitivity levels for unclassified information and three sensitivity levels for classified as Secret or Confidential. (DoDI 8520.03)

Telehealth Monitoring Devices—Electronic monitoring devices (pacemakers, implanted medical devices, personal life support systems, etc.)

Two-Factor Authentication—A method of authenticating a user's identity using a combination of something the user has (private key) and something the user knows (PIN). (NIST Interagency Report 7849)

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