DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

**OFFICE OF THE SECRETARY**

AFMAN33-282_AFGM2015-01

19 March 2015

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1720

SUBJECT: Air Force Guidance Memorandum to AFMAN 33-282, Computer Security (COMPUSEC), 28 March 2012, Incorporating Change 1, 15 January 2015

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes AFMAN 33-282, *COMPUSEC*. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails, in accordance with AFI 33-360, Publications and Forms Management.

Enterprise activated Commercial Mobile Devices (CMDs) in the Air Force are government-issued smart phones and tablets IAW DoD Commercial Mobile Device Interim Policy, 17 Jan 2012 and DoD Commercial Mobile Device Implementation Plan, 15 February 2013. The following policy is added to AFMAN 33-282, paragraph 6.18 clarifying Enterprise Activated CMD use in the Air Force:

6.18.1. Air Force organizations using Defense Enterprise Email (DEE).

6.18.1.1. CMDs must use DoD Enterprise Mobility (DEM) solutions **(T-0)**.

6.18.1.2. CMDs must be purchased utilizing the Network Enterprise Technology Command Blanket Purchase Agreement (BPA) and be on the DISA Approved Products List **(T-0)**.

6.18.1.3. CMDs must be managed by DISA's approved Mobile Device Management (MDM), Mobile Content Management (MCM) or Mobile Application Management (MAM) system **(T-0)**.

6.18.2. Air Force organizations not using DEE.

6.18.2.1. CMDs must use Air Force Enterprise Mobility Solutions **(T-1)**.

6.18.2.2. CMDs must be purchased utilizing the Network Enterprise Technology Command Blanket Purchase Agreement (BPA) and be on the Air Force Approved Products List **(T-0)**.

6.18.2.3. CMDs must be managed by an AF-approved MDM, MCM, or MAM system **(T-1)**.

Customers requiring other new IT services, to include Non-enterprise Activated CMDs, (see para. 6.17 of this manual) or with questions regarding procedures for non-program office fielded systems may forward requirements/questions to HQ AFSPC/A2/3/6 A6CI, Network/Infrastructure Branch, a6.wf@us.af.mil or via memorandum (see AFI 33-115, para 4.10.3.1).

Questions regarding this policy may be forwarded to the SAF/CIO A6SS Strategy and Policy Division, usaf.pentagon.saf-cio-a6.mbx.a3cs-a6cs-strategy-and-policy@mail.mil. This memorandum becomes void after one year has elapsed from the date of this memorandum, or upon publication of an Interim Change or rewrite of AFMAN 33-282, whichever is earlier.

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

***BY ORDER OF THE SECRETARY OF THE AIR FORCE***

***AIR FORCE MANUAL 33-282***

***28 MARCH 2012***

*Incorporating Change 1, 15 January 2015*

***Communications and Information***

***COMPUTER SECURITY (COMPUSEC)***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

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

**RELEASABILITY:** There are no releasability restrictions on this publication.

OPR: SAF/A6OI

Certified by: SAF/A6O
(Mr. Kenneth Brodie)

Pages: 62

Supersedes: AFSSI 8502, 18 September 2008;
AFSSI 8520, 18 June 2009;
AFSSI 8522, 9 June 2008; and
AFSSI 8580, 17 November 2008

This Air Force Manual (AFMAN) implements Computer Security in support of Air Force Policy Directive (AFPD) 33-2, *Information Assurance (IA) Program* and Air Force Instruction (AFI) 33-200, *Information Assurance (IA) Management*. Computer Security (COMPUSEC) is defined within the Information Assurance (IA) portion of AFI 33-200. This publication applies to Air Force military, civilian and contractor personnel under contract to the Department of Defense (DoD), who manage COMPUSEC for Air Force organizations. This publication applies to the Air National Guard and Air Force Reserve Command. Additional instructions and manuals are listed on the Air Force 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 AF Form 847, *Recommendation for Change of Publication*, to SAF/CIO A6SS. Unless otherwise noted, the SAF/CIO A6 is the waivering authority to policies contained in this publication. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See 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 AFMAN 33-363, *Management of Records*, and disposed of according to Air Force 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 Air Force.

***SUMMARY OF CHANGES***

This interim change revises AFMAN 33-282 by (1) eliminating the use of the Air Force Communications Quality Control Checklists (CQCC) to perform annual COMPUSEC self-assessments, (2) mandating SHA-256 compliance, (3) adding policy pointers for the AF Internal Basic Assurance (IBA) Certificate Policy and the Certificate Practice Statement (CPS), and (4) adding security policy on the use of Blackberry® and other DoD-approved smartphones, Bluetooth®, and commercial mobile devices (CMDs). References, Acronyms, and Terms have also been updated. A margin bar ( | ) indicates newly revised material.

# Chapter 1

## INTRODUCTION

**1.1. Introduction.** Computer Security (COMPUSEC) is an IA discipline identified in AFI 33-200, *Information Assurance (IA) Management.* Compliance ensures appropriate implementation of measures to protect all Air Force Information System (IS) resources and information.

1.1.1. The framework of the AF COMPUSEC IA program consists of a cyclic sequential security management model for risk management. This model is specific to information processed on AF computing systems and incorporates strategy, policy, awareness/training, implementation, assessment, remediation, and mitigation controls.

**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 in Para 1.2.3 or 1.2.4.

1.2.1. AF ISs and devices include but are not limited to: Stand-alone systems, Platform IT (PIT) systems, IS components of systems where PIT interconnections (PITI) exist, Modeling and simulation systems/networks, ISs connected to external networks via authorized internet service providers (ISPs), ISs providing the management infrastructure, Connections/interfaces with other ISs

1.2.2. This publication is binding on all users, military, civilian and contract employees, that operate, connect, or interact with the ISs owned, maintained, and controlled by the AF.

1.2.3. More restrictive Federal, DoD, and Director of Central Intelligence Agency directive requirements governing Special Access Program information take precedence over this publication. The latest version of all publications (e.g., Federal, Joint, DoD, AF) referenced within this publication must be utilized.

1.2.4. This publication and implementation guidance identified within are not applicable to Sensitive Compartmented Information (SCI) ISs. For SCI systems, refer to the Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.*

1.2.5. Compliance with IA controls will be assessed, documented, and mitigated according to DoD Instruction (DoDI) 8500.2, *Information Assurance (IA) Implementatio*n, and DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP),* for inclusion in the AF IS Certification and Accreditation (C&A) package.

**1.3. Objective.** The objective of COMPUSEC is to ensure the employment of countermeasures to protect and secure United States (US) government information processed by AF ISs by protecting the confidentiality, integrity, availability, authentication, and non-repudiation of ISs.

## Chapter 2

## ROLES AND RESPONSIBILITIES

**2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6).** Develops, implements, and oversees all cybersecurity disciplines.

**2.2. Air Education and Training Command (HQ AETC).** Conducts and integrates IA education and training into initial military training courses, Air Force accession programs, formal schools, professional military education courses, and specialized training in Air Force Specialty Code-awarding courses according to AFI 36-2201, *Air Force Training Program*, and the specific IA education and training requirements of DoD 8570.01-M, *IA Workforce Improvement Program.*

**2.3. Designated Accrediting Authorities.** Executes Designated Accrediting Authority (DAA) duties according to AFI 33-210 *Air Force Certification and Accreditation (C&A) Program (AFCAP).* Reference AFI 33-210 for DAA appointment, assignment, delegation, training requirements, and key roles and responsibilities.

**2.4. Air Force Senior Information Assurance Officer (AF SIAO).** Reference AFI 33-200 and AFI 33-210 for AF SIAO assignment, roles, and responsibilities.

**2.5. Air Force Space Command.** Designated as the lead command for cyberspace and related subject matter experts in support of policy development for the Air Force future goal of one Air Force Network (the AFNet).

**2.6. 24th Air Force.** Directs Air Force Network Defense (NetD) in accordance with AFPD 10-7, *Information Operations*.

**2.7. Air Force Network Integration Center (AFNIC).** Designated by HQ AFSPC as the organization for IA policy subject matter expertise in support of HQ AFSPC's future goal of one Air Force Network (AFNet).

**2.8. Information System Owners (ISO).** Reference AFI 33-210 for ISO assignment, roles, and responsibilities.

**2.9. System Information Assurance Officer/Manager (IAO/IAM).** Reference AFI 33-200, AFI 33-210 and DoDI 8510.01 for system IAO/IAM roles and responsibilities.

**2.10. Wing Information Assurance Office (WIAO) (To become Wing Cybersecurity Office (WCSO)).** Responsible for the development, implementation, oversight and maintenance of host wing cybersecurity programs.

**2.11. DELETED.**

**2.12. Organizational IAO (To be called Cybersecurity Liaison).** Conducts annual COMPUSEC self-assessments using the COMPUSEC Self-Assessment Checklist (SAC) located in the Inspector General's Management Internal Control Toolset (MICT).

**2.13. Information System Users.** Authorized IS users must comply with the guidance within AFMAN 33-152, *User Responsibilities and Guidance for Information Systems* **(T-1)**.

## Chapter 3

## COMPUSEC

**3.1. General.** Safeguard ISs and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons.

**3.2. Notice and Consent to Monitoring.** Configure all DoD telecommunications devices according to AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP).*

**3.3. Security Configuration Specifications.** Securely configure and implement all Information Technology (IT) products. IA reference documents, such as National Institute of Standards and Technology (NIST) Special Publications (SP), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), National Security Agency (NSA) Security Configuration Guides, AF specialized publications (AF System Security Instructions, AF Technical Orders [TO], etc.), and other relevant publications are used for the security configuration and implementation guidance. Apply these reference documents according to AFI 33-200 and AFI 33-210 to establish and maintain a minimum baseline security configuration and posture. References to various documents are cited throughout this publication, where applicable.

3.3.1. Document all configuration requirements within this publication in the IS C&A package according to AFI 33-210.

3.3.2. Document any deviation to guidance within this publication as part of the applicable IS C&A package. If the DAA has not been delegated the approval authority for the deviation, then the deviations must be submitted, on an AF Form 4169, through IA channels to the OPR of the governing publication prior to DAA approval.

**3.4. IA Community of Practice (CoP).** The AF IA CoP serves as the primary IA support resource for Wing IA officers and managers, providing a collaborative one-stop-shop for IA ideas, questions, discussions, and hosts dynamic web content for information sharing (**https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-SC-IA-01**).

**3.5. Information Technology Asset Procurement.** All IT hardware, firmware, and software components or products incorporated into DoD ISs must comply with evaluation and validation requirements in DoDI 8500.01, *Cybersecurity* **(T-0)**.

3.5.1. Procurement activities of all IT hardware, cellular, and peripheral devices (e.g., desktops, laptops, servers, BlackBerry® devices, cell phones, printers, scanners, and Bluetooth® peripheral devices) must follow the guidance in AFMAN 33-153, *Information Technology Asset Management*, and the AF Information Technology Commodity Council (ITCC) guidance available on the AF Portal.

**3.6. COMPUSEC Methods and Procedures Technical Orders (MPTO).** MPTOs present procedural guidance to the IA workforce to implement and manage methods and processes pertaining to COMPUSEC directed by this policy.

3.6.1. This publication directs the use of the implementation guidance and procedures as identified in the MPTOs for the COMPUSEC program.

3.6.2. Obtain MPTOs via your organizational Technical Order Distribution Account (TODA).

**3.7. Operations Security (OPSEC).** Follow OPSEC measures according to AFI 10-701, *Operations Security (OPSEC),* when using IT assets. OPSEC training and guidance can be obtained from the Installation OPSEC Program Manager or Signature Management Officer.

**3.8. IAO Functions.** Within this publication where both organizational and system IAO functions overlap, the "IAO" term is all inclusive. In all other specific situations, the terms "organizational" or "system" will be indicated. Furthermore, the new term for organizational IAO will become "Cybersecurity Liaison" in the rewrite of AFI 33-200. The term "cybersecurity" has replaced the term "information assurance" in future policy updates and rewrites.

**3.9. Risk Management Framework (RMF) Roles.** With the publishing of DoDI 8510.01, *RMF*, many role designations have been replaced with new terminology. Designated Accrediting Authority (DAA) has been replaced with Authorizing Official (AO); Information Assurance Manager (IAM) has been replaced with Information System Security Manager (ISSM); System Information Assurance Officer (IAO) has been replaced with Information System Security Officer (ISSO); the AF Senior Information Assurance Officer (SIAO) has been replaced with the AF Senior Information Security Officer (SISO). Future policy rewrites will change the old terms to match DODI 8510.01.

## Chapter 4

## INFORMATION SYSTEM ACCESS CONTROL

**4.1. Introduction.** Every individual who has access to the Non-Classified Internet Protocol Router Network (NIPRNET) or Secret Internet Protocol Router Network (SIPRNET), standalone systems, specialized ISs, and/or mission systems is an IS user.

4.1.1. Access to AF ISs is a revocable privilege and will be granted to individuals based on need-to-know and according to DoDI 8500.2, *Information Assurance (IA) Implementation*; NSTISSP No. 200, *National Policy on Controlled Access Protection;* DoD 5200.2-R, *Personnel Security Program*; and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01, *Information Assurance (IA) and Support to Computer Network Defense (CND)*.

**4.2. Authorized Users.** Authorized user account creation and administration must be configured with role-based access schemes according to system policy requirements in DoDI 8500.2.

4.2.1. All authorized users (e.g., military, civilian, contractor, temporary employees, volunteers, interns, key spouses, and American Red Cross personnel) complete DoD IA training prior to being granted access to an IS. IA training will be re-accomplished annually by the user and compliance maintained by the IAO according to DoD 8570.01-M.

4.2.1.1. DoD IA training is located on Advanced Distributed Learning System (ADLS) accessible via the AF Portal. A publically accessible version of the DoD IA training is located on the Information Assurance Support Environment (IASE) website (**http://iase.disa.mil/eta/ProductDownload/awareness_download.html**).

4.2.1.2. When a user requires a new/modification to his/her account (due to change of station or assignment, Temporary Duty [TDY], etc.), the gaining IAO will verify the user meets access requirements before granting access to the IS. Users are not required to retake the DoD IA training provided the user has a valid and current (within a year) course completion record. In emergency or deployment situations, the IAO may rely on a training record review or ADLS to validate course completion.

4.2.2. For IS access, the IAO ensures the DD Form 2875, *System Authorization Access Request (SAAR),* is completed and signed. Document access requests, DoD IA training completion, and justification for access and clearance/background investigation verification as referenced by DoD 5200.2-R and AFI 31-501, *Personnel Security Program.* DD Form 2875 signatures can be "wet" or digitally signed.

4.2.2.1. All authorized IS (to include Mobile Computing Devices) users will sign the standardized AF Form 4394, *Air Force User Agreement Statement-Notice and Consent Provision* (See AFI 33-100, to become AFMAN 33-152) prior to initial IS access. See paragraph **6.12** for wireless mobile device requirements.

4.2.2.2. Access to classified ISs also requires a Standard Form 312, *Nondisclosure Agreement,* according to AFI 31-401, *Information Security Program Management.*

4.2.2.3. IAOs, in coordination with the organizational security manager, verify user background investigation requirements according to DoD 5200.2-R.

4.2.3. A user must obtain an approved hardware token according to current processes prior to obtaining NIPRNET (and SIPRNET when tokens are available) access.

4.2.3.1. The locally appointed Contractor Verification System (CVS) Trusted Agent (TA) individual (e.g. organizational security manager) verifies contractor access against a valid contract in the CVS before approving the request for a contractor to be issued a Common Access Card (CAC).

4.2.4. The ISO ensures methods are in place to verify user access requests before granting IS access.

4.2.5. All user accounts are created using applicable TOs published by the 24 AF (e.g. MPTO 00-33D-2001, *Active Directory Naming Conventions)*.

4.2.6. Privileged User. A privileged user is an authorized user who has access to IS control, monitoring, or administration functions. Grant privileged access to unclassified and classified ISs based on the assigned duties and the position categories identified in DoDI 8500.2: Category IT-I (Privileged) and Category IT-II (Limited Privileged).

4.2.6.1. Privileged users must meet all the requirements of an authorized user as specified in paragraphs **4.2.1 – 4.2.3**.

4.2.6.2. Privileged users are established and administered with a role-based access scheme according to the system policy and DoDI 8500.2.

4.2.6.3. System access requires Public Key Infrastructure (PKI) access methods as specified in **Chapter 5**, Public Key Infrastructure**.**

4.2.6.4. Privileged users access only data, control information, software, hardware, and firmware that they are authorized access and still have a requirement for "need to know."

4.2.6.5. 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 according DoD 8570.01-M and DoDI 8500.2.

4.2.6.6. The system IAM tracks and maintains visibility over all privileged users according to AFI 33-200 and DoDI 8500.2.

4.2.6.7. Prohibit sharing of privileged user accounts between users.

4.2.6.8. Configure privileged user remote access according to the DISA *Enclave* STIG.

4.2.6.9. Privileged users must be position-certified according to DoD 8570.01-M and qualified according to AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program*.

4.2.6.10. Privileged users must complete a Privileged Access Agreement according to DoD 8570.01-M.

4.2.7. Foreign Nationals/Local Nationals. A Foreign National/Local National (FN/LN) user is anyone who is not a US citizen or permanent resident, according to Title 8, Code of Federal Regulations, "Aliens and Nationality." Before authorizing FN/LN access to unclassified and/or classified ISs, the ISO ensures compliance with the IS access requirements in paragraphs **4.2.1**-**4.2.3** and the following constraints:

4.2.7.1. Constraints. MAJCOM Foreign Disclosure Office (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, in accordance with DoD Manual (DODM) 5200.01, Volume 4, *Controlled Unclassified Information* (CUI).

4.2.7.1.1. Base or Wing IA offices must consult the Host or MAJCOM FDO before authorizing access by FN/LN users to ISs processing, storing, or transmitting classified and controlled unclassified information. Note: Specific FN/LN access guidance can be found in the following publications: 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 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*.

4.2.7.2. Administrative Controls. Establish a process between ISOs, system IAMs, and the applicable MAJCOM FDO to determine classified or unclassified access. Direct conflicts in FN/LN access requirements to the MAJCOM FDO for resolution.

4.2.7.2.1. Base or Wing IA offices maintain a list of FN/LN users from each subordinate organization within their assigned organizations. Provide specific documentation indicating FN/LN usage to the system IAM for inclusion in the IS C&A.

4.2.7.2.2. The IAO tracks and maintains visibility over all FN/LN billets assigned to an IS and/or organization.

4.2.7.2.3. Restrict FN/LN IS user access to IT levels defined in DoDI 8500.2.

4.2.7.2.4. If privileged access is required to an IS, FN/LN user access must be restricted to IT II-level positions only and directly supervised by a U.S. Citizen according to DoDI 8500.2 and CJCSI 6510.01. Furthermore, document access in the IS C&A package. Pursuant to applicable host-nation agreements, FN/LN privileged users must be baseline computing environment (CE) certified according to DoD 8570.01-M.

4.2.7.3. IS Controls. System IAMs in coordination with privileged users ensure that applicable IA technical safeguards and controls are established and maintained according to CJCSI 6510.01 and DoDI 8500.02.

4.2.7.3.1. Prohibit unlimited FN/LN access to ".mil" websites until specific host FDO and the MAJCOM FDO approval is accomplished.

4.2.7.3.2. ISOs direct privileged users to setup permissions on ISs that allow for FN/LN account management in accordance with this publication.

4.2.7.3.3. Establish proper messaging naming conventions (e.g., <**john.smith.uk@af.mil**>) of FNs as non-US citizens according to CJCSI 6510.01.

4.2.7.3.4. At the discretion of the ISO, system access requires PKI access methods as specified in **Chapter 5**, Public Key Infrastructure. See paragraph **4.2.6.3** MAJCOMs handle token requirements according to host nation agreements.

4.2.7.3.5. IAOs validate implementation of appropriate safeguards (e.g. PKI, email accounts). Employ safeguards that adhere to DoD, Joint, and AF, and if applicable, locally created information security publications.

4.2.7.3.6. 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 according to applicable host MAJCOM FDO requirements.

4.2.7.3.7. For SIPRNET RELEASABLE (SIPR REL) IS specific configuration requirements, follow guidance in the DISA Embedded REL User Enclave Technical Implementation Instruction (TII) (**http://iase.disa.mil/stigs/net_perimeter/enclave_dmzs/rel.html**).

4.2.7.3.8. SIPR REL users do not need FDO approval to access .mil sites. DISA controls website access at the REL DMZ proxy.

4.2.7.4. Other Considerations. Non-US citizens who are permanent legal residents and/or full time permanent employees of the DoD meet the requirements of any US citizen for access to the unclassified network or system.

4.2.8. Grant only unclassified IS access to temporary employees and volunteer personnel in support of their assigned duties.

4.2.8.1. A volunteer is any individual authorized to be DoD volunteers as defined in DoDI 1100.21, *Voluntary Services in the Department of Defense*. Restrict volunteers to IT-III level positions.

4.2.8.2. Temporary employees and volunteers (including key spouses) must meet the requirements as specified in paragraphs **4.2.1** through **4.2.3**.

4.2.8.3. Temporary employees and volunteers require PKI access at the discretion of the ISO and according to IS requirements as outlined in **Chapter 5**, Public Key Infrastructure. See paragraph **4.2.6.3**

4.2.8.3.1. Eligible volunteers should contact their CVS TA to get their Volunteer Logical Access Credential (VoLAC).

4.2.8.3.2. The VoLAC is used for logical access (network) and is replacing the Alternative Token for volunteers.

4.2.9. Public users that access an IS intermittently (i.e. vendors, morale support, technical support, etc.) have only non-privileged access.

4.2.9.1. The system ISO ensures adherence to applicable DISA STIGs (e.g., Web Server STIG) for private/public IS separation.

4.2.10. All IS users have the responsibility to report suspected inappropriate use, both by authorized and unauthorized personnel, to supervisory chain of command, security manager, organizational IAO, or commander.

**4.3. 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 AFI 33-100, to become AFMAN 33-152).

4.3.1. Specific procedural information for account disabling is located in MPTO 00-33B-5004, *Access Control for Information Systems*.

4.3.2. Failure to maintain DoD IA training results in immediate suspension of access to unclassified and classified ISs.

4.3.3. Unintentional and/or intentional actions that threaten or damage AF ISs will result in immediate suspension of access to unclassified and classified ISs according to CJCSI 6510.01.

4.3.3.1. According to CJCSI 6510.01, suspend access to classified ISs if the user's security clearance is suspended, denied, or revoked. If an individual's clearance is suspended, denied, or revoked, the ISO coordinates with the organization commander and determines if unclassified network access can be maintained according to paragraph 4.3.3.3.

4.3.3.2. The IAO notifies the ISO and/or the organizational commander upon discovery or notification of user activity that is inconsistent with the terms of DoD IA training or inconsistent with approved IS security usage.

4.3.3.3. At the direction of the organizational commander, the IAO suspends user access and the ISO provides reason for the suspension. The ISO identifies requirements required for account reinstatement (at a minimum, DoD IA remedial training, MAJCOM required, or USCYBERCOM CTO-directed requirements). Upon satisfactorily completing retraining and any other requirements, the IAO, on behalf of the ISO and/or organizational commander initiates reinstatement.

4.3.3.4. The ISO reviews all pertinent documentation relating to the justification for the suspension, the risk to the network, and operational requirements. The organizational commander makes a determination as to whether or not to suspend the individual's network access. See Table 4.1, *Network Access Suspension Matrix,* as guidance for when an individual's security clearance is suspended, denied, or revoked, for whatever reason.

4.3.4. If the user disputes IS access suspension, follow local command level legal guidance.

**Table 4.1. Network Access Suspension Matrix.**

| RULE | A | B | C |
|---|---|---|---|
| | **If the system is** | **and the clearance is** | **then** |
| **1** | Classified | Suspended, denied, or revoked | The individual's access is immediately suspended. See AFI 31-501, *Personnel Security Program Management,* and CJCSI 6510.01 |
| **2** | Unclassified | Denied or revoked | The IAO will immediately suspend the individual's access |
| **3** | Unclassified | Suspended | Organizational commanders may make a |

| | | | |
|---|---|---|---|
| | | | recommendation for access reinstatement based on the circumstances surrounding the suspension, threat to the network, and operational requirements |
| **4** | Unclassified with privileged access | Suspended, denied, or revoked | Suspend privileged access immediately. Organizational commanders may make a recommendation for user access suspension depending on the circumstances surrounding the suspension and operational requirements |

**4.4. Account Management.** AF direction is to use PKI-based access control according to DoDI 8520.03, *Identity Authentication for Information Systems* and the USCYBERCOM, *Public Key Infrastructure (PKI) Implementation* Communications Tasking Order (CTO) 07-015 (**https://www.cybercom.mil/J3/orders/default.aspx**) for unclassified systems. See Chapter 5, Public Key Infrastructure.

4.4.1. IAO Account Actions. Specific procedural information is located in MPTO 00-33B-5004, IAOs/IAMs will:

4.4.1.1. Maintain the group account configurations according to the IS C&A documentation and according to DoDI 8500.2.

4.4.1.2. Ensure assignment of individual accounts to privileged users. Group or shared accounts do not support nonrepudiation and least-privilege access controls.

4.4.1.3. Notify privileged users to de-provision all user accounts from an IS whenever the user no longer requires access to the IS within 24 hours of notification (e.g., whenever the user is permanently transferred to another location, termination of employment, retirement).

4.4.1.4. Substitute reusable IS user accounts on systems with frequent user-turnover (e.g., students, temporary employees, exercise accounts). For specific procedures, see MPTO 00-33B-5004, Chapter 3.

4.4.1.5. Develop local procedures in coordination with privileged users to log off users manually if automatic log off functions are not technically feasible (e.g., SIPRNET clients, non-Windows based).

4.4.1.6. Develop notification procedures for de-provisioning IS user accounts when an employee (e.g., military, civilian, or contractor) transfers, retires, separates, or is terminated, or for any other loss of IS access.

4.4.1.7. Perform annual audit of user accounts to verify permissions/least privilege and ensure that de-provisioning of accounts has taken place according to DoDI 8500.2.

4.4.2. Privileged User Account Actions. Specific procedural information is located in TO 00-33A-1202, *Air Force Network Account Management.* Privileged users will:

4.4.2.1. Configure all individual IS accounts with a unique identifier. For group or shared accounts see paragraph **5.7** for group accounts with PKI.

4.4.2.2. Permit group accounts only for reasons of operational necessity on unclassified and classified systems and networks as determined by the organizational commander,

reviewed by the system IAM, approved by the ISO, and fully documented in the C&A package.

4.4.2.3. Associate each IS user identity with all auditable actions supporting nonrepudiation and accountability according to DoDI 8500.2.

4.4.2.4. Incorporate electronic or paper tracking and reviewing methods to match individual users to generic usernames (e.g., user log sheet) every 30 days.

4.4.2.4.1. Per direction of the IAO/IAM, disable user accounts once the users no longer require access (e.g., permanent change of station, separation, class graduation).

4.4.2.5. Configure account lockout parameters according to the USCYBERCOM Public Key Infrastructure (PKI) Implementation CTO 07-015 and CJCSI 6510.01.

4.4.2.6. Configure automatic log off functions due to user inactivity according to the minimum standards identified in according to DoDI 8500.2 and the applicable DISA OS/Database STIGs.

4.4.2.7. Configure and implement automated IS controls to check and disable IS user accounts that have been dormant more than 30 days according to CJCSI 6510.01. *AF CIO Exception:* Disable National Guard and Reserve member IS user accounts only after 90 days of inactivity.

4.4.2.7.1. If an approved hardware token is used as the only IS's account authentication method, user account access expires when the approved hardware token expires according to CJCSI 6510.01.

4.4.2.7.2. For PK-enabled ISs using Personal Identification Numbers (PINs), disable or limit pin caching features according to the applicable DISA OS (e.g., Windows) and DISA *Access Control* STIGs.

4.4.2.8. 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) according to the configuration information in the IS C&A package before allowing any user access to the system.

4.4.2.8.1. Rename default accounts that cannot be deleted, according to applicable DISA STIGs.

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

4.4.2.9. Disable user accounts (do not delete) 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 4.3.

4.4.2.10. Before unlocking the user account, a validated mechanism must be in place to validate the user's identity with the IAO (e.g., in-person identification, digitally signed email).

**4.5. Password/PIN Management.** ISs must follow PKI requirements in USCYBERCOM *Public Key Infrastructure (PKI) Implementation* CTO 07-015 and **Chapter 5**, Public Key Infrastructure as an authentication means to the NIPRNET.

4.5.1. Specific procedural information for password management is located in MPTO 00-33B-5004, Chapter 4.

4.5.2. According to DoDI 8520.02,, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, and the DISA STIG, *Access Control in Support of Information Systems*, all DoD networks required by DoDD 8500.1 to authenticate users will perform this authentication using certificates issued by DoD-approved PKI on hardware tokens. The CAC is the primary hardware token, but there are special instances where the CAC cannot be used to perform various missions. To accommodate these various missions, the DoD CIO has approved the use of the Alternate Login Token (ALT). See Chapter 5, Public Key Infrastructure.

4.5.3. In addition to the AF-specific password guidance contained within this publication, configure IS password authentication according to the DISA *Access Control* STIG. DISA STIG and/or USCYBERCOM Tasking Order (TO) password requirements take precedence only if more restrictive than guidance in this publication.

4.5.4. The ISO and system IAM will ensure where passwords are used for access to AF-GIG restricted assets (i.e., networks, workstations, or applications), at a minimum, passwords are created and changed in accordance with current USCYBERCOM CTOs and CJCSI 6510.01.

4.5.4.1. Meet the minimum complexity requirements as specified in the applicable DISA STIGs and MPTO 00-33B-5004. See CTO 07-015 for additional guidance.

4.5.4.2. One-time password generators or hardware token implementation must follow the guidance provided in the DISA *STIG*, *Access Control in Support of Information Systems*,.

4.5.4.3. ISO and system IAM will establish a frequency based on mission, operational needs or IS technical feasibility if not able to meet this requirement (e.g., AF Reserve Components).

4.5.5. Protect all passwords and PINs based on the sensitivity of the information or critical operations they protect (e.g., a password used to gain access to a SECRET network is itself classified SECRET).

4.5.5.1. Classify passwords and PINs at the highest level of information processed on that system. As a minimum, safeguard passwords as “For Official Use Only” (FOUO). See Appendix 3 of DoD Regulation 5200.1-R, *Information Security Program*, for an explanation of FOUO.

4.5.5.2. If necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a properly marked, sealed envelope or Standard Form 700, *Security Container Information Form*, and store in a General Services Administration (GSA)-approved container as specified in the DISA *Access Control* STIG.

4.5.6. The ISO and system IAM ensure compliance with DoDI 8500.2 for shared/group passwords and PINs and obtain approval by the DAA according to CJCSI 6510.01. Implement system and physical auditing procedures in conjunction with these methods to support non-repudiation and accountability.

4.5.6.1. Consider unauthorized sharing of passwords a security incident according to CJCSI 6510.01. See Chapter 7, Data Spillage and COMPUSEC Incident Reporting.

4.5.7. In the event of a compromised password or PIN, the ISO and system IAM ensures procedures are in place to implement immediate password and PIN change activities. The IAO follows established reporting and investigation procedures according to AFI 33-138, *Enterprise Network Operations Notification and Tracking* (to become AFI 33-115, *AF GIG Services*). If the PIN is the access code to an approved PKI token, the compromise of the PIN warrants probable compromise of the certificates. See paragraph **5.8**

4.5.8. Protect all passwords and PINs during transmission using Federal Information Processing Standards (FIPS)-approved encryption according to DoDI 8500.2. If not technically feasible, require the use of a one-time password to access the IS.

4.5.9. Privileged users will incorporate electronic or paper tracking methods to account for user activity when using shared passwords. Shared passwords will meet all requirements as specified in this publication.

4.5.10. Institute automated procedures to reject rapid retries when entering a password incorrectly.

4.5.11. The ISO will ensure the establishment of procedures for manual or automatic password changes by users. The IS will require users to change the one time password at initial logon according to DoDI 8500.2.

4.5.11.1. Configure IS user accounts to enforce password history in accordance with applicable DISA STIG. If ISs cannot support STIG requirements, configure to maximum and document in C&A package.

4.5.11.2. IS privileged users implement policies enforcing a minimum seven-day wait before a user may optionally change the password.

4.5.12. Upon a suspected or confirmed compromised or "cracked" password and/or PIN, the IAO must immediately take measures to lock down the account in question.

4.5.13. Configure password cracking tools and procedures according to DoDI 8500.2. See MPTO 00-33B-5004 for password cracking specific guidance.

**4.6. Biometric Management.** The definition of biometrics is a measurable biological (anatomical and physiological) and behavioral characteristic used for automated recognition. As a process, biometrics is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

4.6.1. Biometrics is an important AF operational enabler that will be fully integrated to conduct the AF mission in support of joint military operations according to DoDD 8521.01E, *Department of Defense Biometrics.*

4.6.1.1. Design biometrics programs to improve the effectiveness and efficiency of biometrics activities throughout the AF by eliminating duplication and overlap of technology development and information management efforts.

4.6.1.2. Configure biometric programs according to the DISA *Biometrics Security Checklist* (**http://iase.disa.mil/stigs/checklist/**).

4.6.2. 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.

4.6.3. All biometrics activities shall be coordinated via the sponsoring AF functional organization through the Biometrics Identity Management Agency (BIMA) at **http://www.biometrics.dod.mil**/ and approved by DoD Biometrics Executive Committee (EXCOM) before acquisition.

4.6.4. When used, biometrics will be collected, matched, transmitted, stored, shared, archived, and received according to AF procedures for each group as defined by the *National Science and Technology Council Subcommittee on Biometrics Glossary*; AFI 63-101, *Acquisition and Sustainment Life Cycle Management;* and AFI 33-332.

4.6.5. In accordance with Office of the DoD CIO disposition definitions, biometrics fall into two groups governing storage and retention.

4.6.5.1. Group 1 consists of military, government civilians, and military dependents; indefinite storage and retention apply.

4.6.5.2. Group 2 consists of contractors, visitors, and temporary workers; disposition of biometric data occurs at the end of the access period.

4.6.6. All biometrics data and associated information collected as a result of DoD operations or activities will be maintained or controlled by the Department of Defense, unless otherwise specified by BIMA for DoD Biometrics at a later date.

**4.7. Account Auditing.**

4.7.1. IS auditing events will be configured according to CJCSI 6510.01 and the applicable DISA STIGs (application, operating system, database, etc).

4.7.1.1. Privileged users must ensure the IS audit trail function is enabled for accounts. Only privileged users have access to the audit trail file.

4.7.2. The audit trail must not contain unencrypted (clear text) passwords, incorrectly entered passwords, or character strings, as this could expose the password of a legitimate user.

4.7.3. All audit records must be maintained according to AFRIMS, *Records Distribution System (RDS)*, Table 33-25, Rule 8 (**https://www.my.af.mil/afrims/afrims/afrims/rds/rds_series.cfm**).

## Chapter 5

## PUBLIC KEY INFRASTRUCTURE

**5.1. Introduction.** The DoD and the Committee on National Security Systems (CNSS) PKIs use asymmetric cryptography to identify and authenticate users to systems and networks for the NIPPRNET and SIPRNET. PKI hardware tokens provides two-factor authentication for access to DoD and AF ISs and networks for both NIPRNET and SIPRNET. Two-factor authentication is a combination of something the user has and something the user knows.

**5.2. NIPRNET PKI.** The most commonly used unclassified PKI hardware token or smart card is the CAC. On AF installations, the Air Force Military Personnel Flight (MPF) issues the CAC. On non-AF locations, any Real-time Automated Personnel Identification System (RAPIDS) issues CACs.

5.2.1. The CAC is the primary hardware token for identifying individuals for logical access to NIPRNET assets and physical access to DoD facilities according to Directive-Type Memorandum (DTM) 08-003, *Next Generation Common Access Card (CAC) Implementation Guidance* (to be incorporated into DoD Manual 1000.13-M Volume 1).

5.2.2. Air Force Personnel Center (AFPC) manages the issuance of CACs through Defense Enrollment Eligibility Reporting System/Real-Time Automated Personal Identification System (DEERS/RAPIDS).

5.2.2.1. According to AFI 36-3026 IP. Volume 1, *Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, authorized users are issued PKI certificates on the CAC.

5.2.3. The CAC provides a cryptographic certificate-based logon identity that is valid until expiration of the CAC (not to exceed three years).

5.2.4. Personal Identity Verification (PIV) Authentication certificates can be utilized on CAC's to logon to additional accounts in the domain/AF GIG. See TO 31S5-4-7255-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon/Next Generation Using Personnal Identity Verification (PIV) Certificate* for further information on implementing this capability.

5.2.5. DoD PIV Authentication certificates can be utilized on CAC's for smart card logon to multiple accounts in the domain/AF GIG. See TO 31S5-4-7256-8-1, *Configuration and Operations Guide for Air Force Certificate-Based Smart Card Logon / Next Generation Using Alternate Security Identification (ALTSECID)* for further information on implementing this capability.

5.2.6. The ALT is an unclassified PKI hardware token or smart card containing a computer chip with a certificate issued by the AF PKI Registration Authority (RA). Use of an ALT with DoD PKI certificates is authorized for specific cases when certificates issued on the CAC cannot be used by various groups of network users.

5.2.6.1. The ALT standard operating procedure defines use categories. Standard operating procedures are available on the AF PKI System Program Office (SPO) site **https://afpki.lackland.af.mil**.

5.2.7. The VoLAC is an unclassified PKI hardware token or smart card used for volunteers and issued by MPF for network access only. Request a VoLAC through the organization CVS TA.

5.2.8. All NIPRNet Systems are required to be SHA-256 compliant NLT 31March 2015. **(T-1)** Program managers should follow FIPS 180-4, Secure Hash Standard, FIPS 140-2, and the validation lists available through the NIST Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) sites at **http://csrc.nist.gov/groups/STM/cmvp/index.html**. Guidance for determining SHA-256 compliance is available on the Information Assurance Collaborative Environment .

**5.3. SIPRNET PKI.** SIPRNET currently uses two forms of access, username/password or PKI hardware token/smart card and PIN. The SIPRNET PKI token is currently being implemented with an estimated completion date of December 2012. During the deployment, the username/password will remain as an option to authenticate to the SIPRNET as an alternative to using the SIPRNET hardware token or smart card.

5.3.1. The Local Registration Authority (LRA), normally residing at the supporting base, issues the SIPRNET hardware token or smart card with a computer chip. The SIPRNET hardware token or smart card 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.

5.3.1.1. The SIPRNET hardware token or smart card is a high-value unclassified item. Maintain the SIPRNET hardware token according to CNSSI Instruction for *National Security Systems Public Key Infrastructure X.509 Certificate Policy,* Registration Practice Statement (RPS).

5.3.1.2. The token is classified SECRET when inserted into SIPRNET hardware token reader and PIN is entered (unlocked) and in use, and is considered unclassified when removed from its SIPRNET hardware token reader and not in use.

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

5.3.2. Maintain the SIPRNET hardware token in the positive control of the authorized user, who is represented by the embedded certificates according to the applicable CNSS policy or RPS.

5.3.2.1. Immediately report any suspected loss of control to the LRA. Positive control includes maintaining visual contact when in use. When not in use, the assigned user must maintain physical possession of the SIPRNET hardware tokenor it must be locked in a container that only the assigned user can unlock.

5.3.2.2. 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 will return the token to NSA for investigation and/or destruction. See paragraph **5.8** for key compromise guidance.

5.3.2.3. If the SIPRNet hardware token is lost or stolen and not recovered, immediately report this information to the LRA to initiate the revocation process according to the applicable Certificate Practice Statement (CPS). See paragraph **5.8** for key compromise guidance.

5.3.3. Permit only the latest version of domain-aware middleware on SIPRNET ISs where the SIPRNet hardware token is to be utilized. Configure the domain-aware middleware to activate only SIPRNet hardware tokens initialized for use on the SIPRNET. Remove all other middleware products from the IS. ActivClient is not authorized for use on SIPRNet.

5.3.4. 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 according to the applicable CPS.

5.3.5. Prohibit the introduction of (operational) SIPRNET tokens on unclassified ISs. **NOTE:** This does not apply to testing cards on unclassified test beds.

5.3.5.1. SIPRNET hardware tokens inserted into unclassified IS may result in a security violation and must be reported to the local network ISO through the IAO to determine if the incident is a security violation.

5.3.5.2. If a SIPRNET hardware token incident occurs, report the incident to the local information system security officers, confiscate the SIPRNet hardware token and ensure the certificates are revoked. Follow the guidance in **Chapter 7**, Data Spillage and COMPUSEC Incident Reporting.

5.3.6. Introduction of unclassified tokens (e.g., CAC, ALT, PIV, VoLAC, and or PIV-I) on SIPRNET ISs is NOT authorized.

5.3.6.1. The SIPRNET domain aware middleware configuration must detect the NIPRNet token, block PIN entry, and block any service applets that do not require PIN entry.

5.3.6.2. An unclassified hardware token inserted into a SIPRNET IS does not constitute a security violation unless the PIN prompt appears. Report the incident to the local network Information Security Officer through the IAO to determine if the incident is a security violation. Follow the guidance in **Chapter 7**, Data Spillage and COMPUSEC Incident Reporting.

5.3.7. The connection of keyboards with built-in CAC readers and external USB CAC readers to classified ISs are not permitted. Connect only approved SIPRNET token readers (i.e. Omikey 3121) to SIPRNET ISs.

5.3.8. All SIPRNet Systems are required to be SHA-256 compliant NLT 31 December 2015. **(T-1)** Program managers should follow FIPS 180-4, Secure Hash Standard, FIPS 140-2, and the validation lists available through the NIST Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) sites at **http://csrc.nist.gov/groups/STM/cmvp/index.html**. Guidance for determining SHA-256 compliance is available on the Information Assurance Collaborative Environment **https://cs3.eis.af.mil/sites/OO-SC-IA-01/default.aspx**.

**5.4. External PKI.** Only rely on certificates that are issued by a DoD PKI or by an external PKI that has been approved for use. DoDI 8520.02 outlines the policies for External PKI approved for use with DoD relying parties.

5.4.1. Before an organization can add any PKI Certificate Authorities (CA) into its website's Certificate Trust List (CTL), the organization must coordinate with AF PKI Requirements Lead (AFNIC/EVAI, **afnic.evai@us.af.mil**).

5.4.1.1. The IAO and/or IAM ensure access approval and validation by the external PKI, coordinating with AFNIC/EVAI prior to any configuration activities.

5.4.1.2. The IAO implements access control measures to enable enforcement of need-to-know requirements according to the DoD CIO Memorandum, *Compliance and Review of Logical Access Control in Department of Defense (DoD) Processes.*

**5.5. Escrowed Certificates.** The CA provides automatic escrow of the e-mail encryption key according to *X.509 Certificate Policy for United States Department of Defense*. Perform recovery of escrowed encryption keys according to the CA associated practice statements.

5.5.1. 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.

**5.6. Software Certificate Issuance and Control.**

5.6.1. AF PKI RA's, LRA's, Certification Authority Managers, CA Operators, System Administrators, and CA Security Managers will comply with the detailed policy and procedures in the following documents, where applicable. **(T-1)** These documents are available on the AF PKI SPO website, **https://afpki.lackland.af.mil/html/policy.cfm**.

5.6.1.1. The United States Air Force Internal Medium Assurance Public Key Infrastructure Root Certification Authority Certification Practice Statement.

5.6.1.2. The X.509 Certificate Policy for the United States Air Force Internal Medium Assurance PKI.

5.6.1.3. Certification Practices Statement for the United States Air Force Internal Medium Assurance Subordinate Certification Authorities.

5.6.1.4. The Air Force Internal Basic Assurance X.509 PKI Certificate Policy.

5.6.1.5. The Air Force Internal Basic Assurance Certification Authority Certification Practices Statement.

5.6.1.6. The Air Force Internal Less Than Medium Assurance (LTMA) X.509 PKI Certificate Policy (CP) (v1.0).

5.6.1.7. The Air Force Internal Less Than Medium Assurance (LTMA) PKI Root Certification Authority (CA) Certification Practices Statement (CPS) (V1.0).

5.6.2. Software certificates are available for use on both unclassified and SIPRNET ISs after inclusion in the C&A package and DAA approval. If DAA approved, software certificates remain in use only for the minimum time according to the applicable DISA STIGs.

5.6.3. Encryption software certificates for organizational e-mail mailboxes, to include portable electronic devices (PEDs), must have a designated sponsor appointed in writing to receive and manage the certificates using a standard memorandum. The AF RA or LRA, as appropriate, will maintain a file of requirement validation documentation. For organizational e-mail mailboxes on PEDs, follow the appropriate DISA STIG. For additional guidance, see the AF PKI SPO website.

5.6.4. DoD PKI certificates and associated private keys are stored in a *Public-Key Cryptography Standards (PKCS)* #12 file on a removal storage medium. PKCS#12 files will NOT be left in on-line file systems, and must be properly installed into the cryptographic module on an IS for use. See paragraph **5.6.6.1** for more information.

5.6.5. Authorized users will not share personal software certificate passwords and must protect the media containing their private keys from unauthorized access at all times according to paragraph 4.5.

5.6.6. Integrated Network Operations and Security Centers (I-NOSCs) will verify removal of software certificate installation files (.p12 or .pfx) from hard drvies and other online storage devices weekly.

5.6.6.1. 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.

**5.7. Group Accounts Utilizing PKI.** Group accounts (not to be confused with organizational accounts) are special case accounts where more than one person may hold an ALT (private key) to access the same account. Procedural material is available on the AF PKI SPO web site.

5.7.1. Authorized users must request individual ALTs to access the group account; each token will contain an individual identification certificate. See paragraphs **5.2.6** and **5.2.6.1**

5.7.2. The IAM and/or the TA maintains an inventory of token serial numbers and their assignment at all times.

**5.8. Key Compromise.**

5.8.1. The IAO immediately notifies the supporting TA, LRA, or the AF RA (**afpki.ra@lackland.af.mil**) directly by encrypted e-mail if an AF PKI certificate holder (software certificate or token) suspects a compromise of the holder's private key. See Chapter 7, Data Spillage and COMPUSEC Incident Reporting.

5.8.1.1. The AF RA must revoke certificates suspected of key compromise within 24 hours or the next duty day (whichever is first) after notification.

5.8.2. 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.

5.8.2.1. Revoke all other certificates (e.g., encryption and digital signature) on the token if there is a revocation of a user's ID certificate. Enter the revoked certificates into a DoD Certificate Revocation List. All applications (i.e. web sites, 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.

**5.9. Server Certificates.**

5.9.1. The AF RA will approve issuance of Medium-Assurance DoD PKI or NSS (SIPRNET) server certificates based on validation by a properly appointed LRA, or TA. Specific instructions to obtain and load DoD server certificates are available on the AF PKI web site.

5.9.2. A server certificate must be reissued when the fully qualified domain name (FQDN) for the server changes or after three years.

5.9.3. All private Air Force Web servers must be issued a DOD X.509 PKI Server certificate and have 128-bit encryption Secure Sockets Layer (SSL); this certificate must be enabled at all times according to DoDI 8520.02.

**5.10. Code Signing Certificates.** Code signing certificates are specially formatted certificates used for digitally signing executable program code in any number of languages or formats.

5.10.1. Submit these software certificates requests to AF PKI Requirements Leads office for issuance on a hardware token by the AF RA/AF PKI SPO. For additional guidance, see the AF PKI SPO web site.

**5.11. Certificate Reissuance Prior to Expiration.** Certificate owners needing continued PKI services must ensure reissue of their certificates at least 30 days prior to the certificate expiration date in order to prevent disruption in service.

**5.12. Network Authentication.** Enable all unclassified networks to use hardware tokens, DoD PKI certificate-based authentication, and set authorized user accounts to require smart card logon by selecting, "Smart card is required for interactive logon," in Windows Active Directory environments. Obtain exceptions to this policy from the AF DAA through the respective MAJCOM PKI or IA representative. See paragraph **4.5**

**5.13. PKI Waivers.** Coordinate all PKI waivers with AFNIC/EVAI. See DoDI 8520.02 for PKI waiver requirements.

## Chapter 6

## END POINT SECURITY

**6.1. Introduction.** End Point security provides the basis for overall protection of AF-controlled IT assets. Follow CJCSI 6510.01 and AFI 33-138 (to become AFI 33-115) on 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.

**6.2. General Protection.** All authorized users will protect networked and/or stand-alone 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. Basic end point security procedures are located in MPTO 00-33B-5006, *End Point Security for Information Systems.*

6.2.1. Identify and authenticate users before gaining access to any government IS, according to guidance in **Chapter 4**, Information System Access Control.

6.2.2. ISOs 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., CAC removal lock feature, keyboard locks, secure screen savers, add-on security software).

6.2.3. Setup desktops, laptops, PEDs, and other display devices preventing the inadvertent viewing of controlled or sensitive information by unauthorized users (e.g., away from windows, doorways, public areas).

6.2.4. Control viewing of US-Only ISs and equipment by FN/LNs according to CJCSI 6510.01.

6.2.5. Ensure transmission of sensitive information is encrypted using NIST-certified cryptography at a minimum according to DoDI 8500.2 and CJCSI 6510.01.

6.2.6. Ensure the transmission of classified information is encrypted using NSA-approved cryptography according to AFMAN 33-283, Communications *Security (COMSEC) Operations, 3 September 2014.*

6.2.6.1. In areas where classified information is processed, the IS must meet TEMPEST requirements (formerly called EMSEC) found at https://cs3.eis.af.mil/sites/OO-SC-IA-01/default.aspx. **(T-1)**

6.2.7. ISOs will ensure procedures are in place to provide physical security for network connections to the appropriate information classification level according to the applicable DISA STIGs and DODM 5200.01, Volume 1, DoD Information Security Program: Overview, Classification, and Declassification; Volume 2, DoD Information Security Program: Marking of Classified Information; and Volume 3, DoD Information Security Program: Protection of Classified Information.

6.2.7.1. Install, operate, and store IS devices used for processing classified information that contain non-volatile, non-removable storage media (e.g., switches, routers,

multifunction devices, other interconnection devices) in areas approved for open storage of classified information.

6.2.7.1.1. Storage of IS devices using non-volatile or non-removable storage media in areas not approved for open storage requires a risk-based decision according to the technology, mission, and physical/operating environment. The responsible IAM documents the risk decision within the C&A package for DAA approval.

6.2.7.1.2. Temporary storage of IS devices used to conduct classified processing requires protection at or above the highest classification level of the information processed.

6.2.7.2. Any deviations to physical procedures in place due to operational need (e.g. no screen-saver, network management products) must be configured according to the applicable DISA OS STIGs, approved by the DAA, and meet the following requirements:

6.2.7.2.1. Implement "least privilege" policies preventing logon as a privileged user.

6.2.7.2.2. Justify and document the deviation as a mission requirement in the IS C&A package. See paragraph **4.4**

6.2.7.2.3. Locate the devices in controlled access areas.

6.2.8. Ensure all personnel authorized to use the IS are cleared to the highest level and most restricted category of information contained in the IS (unless multi-level security is implemented).

6.2.8.1. Ensure the use of a separate copy of the OS and other necessary software for each level of classification on ISs employing periods processing; see paragraph **6.3**

6.2.8.2. When changing modes of operation from or to higher classification levels, clear equipment and media according to **Chapter 8**, Remanence Security**.**

6.2.9. The classification of the IS determines the classification of the removable media; mark and label removable media with the highest classification of the IS, according to CJCSI 6510.01.

6.2.9.1. Unless a write protection mechanism is used or a write protection process has been approved by the DAA, unclassified media introduced into a classified IS becomes classified according to CJCSI 6510.01.

6.2.10. The IAO ensures the proper handling of storage devices that contain classified information according to **Chapter 8**, Remanence Security.

**6.3. Periods Processing.** Periods processing is the act of accessing various levels of classified and unclassified information at distinctly different times from the same IS. Processing classified and unclassified levels on the same IS will be configured according to DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

6.3.1. Ensure the use of a separate copy of the OS and other necessary software for each level of classification on the IS.

6.3.2. Ensure procedures are developed and employed to identify and switch out the different hard drives within the IS. For specific procedures reference MPTO 00-33B-5006, Chapter 11.

6.3.2.1. The system and organizational IAM must validate these procedures before implementation and operation.

6.3.3. Ensure that each swappable hard drive is labeled according to DoD 5200.1-R.

6.3.4. Ensure the area processing classified information meet EMSEC requirements according to DoDI 8500.2 and AFSSI 7700.

6.3.5. Sanitization or destruction procedures of hardware and any removable media must follow the guidance in **Chapter 8,** Remanence Security.

**6.4. Software Security.** Ensure all software is included in the IS C&A package.

6.4.1. Comply with AFMAN 33-153 for software guidance.

6.4.2. Freeware, public domain software, shareware originating from questionable or unknown sources (e.g., World Wide Web sites), and Peer-to-Peer (P2P) file sharing software are highly susceptible to malicious logic will only be used after a risk assessment (see AFI 33-210) has been conducted. The software must receive DAA approval through the C&A process according to AFI 33-210 and CSCSI 6510.01.

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

6.4.4. Do not allow use of software (e.g., foreign) on an IS that does not meet restrictions laid out by the Buy American Act (41 U.S.C), the Excluded Parties List, and the Trade Agreements Act of 1979. Coordinate with the ISO and/or system IAM, and contracting office for approval prior to any purchase.

**6.5. 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 according to DoD 8500.2.

6.5.1. The IS must employ antivirus software with current signature files according to DoD Antivirus Security Guidance (**http://www.disa.mil/antivirus/index.html**) or approved whitelisting methodology to prevent malware from running on mobile computing devices not configured with antivirus software (refer to applicable mobile device STIGs).

6.5.2. Use only antivirus tools and signature files/data files obtained from the AFCERT site operated by the 33rd Network Warfare Squadron (**https://33ios.lackland.af.mil/virus/sym_sigs.htm**) and/or from the DoD Patch Repository (**https://patches.csd.disa.mil/Default.aspx**).

6.5.3. When technically feasible, configure virus scanning frequency and real-time protection according to the applicable DISA STIG.

6.5.4. Using additional antivirus software (in conjunction with DoD-approved antivirus software; **http://www.disa.mil/antivirus/index.html**) may be approved through the C&A process.

6.5.5. Authorized users must report malicious logic intrusions or any other deviation and misconfiguration according to the reporting guidance in **Chapter 7,** Data Spillage and COMPUSEC Incident Reporting.

6.5.6. Scan approved removable media devices for viruses before and after use.

6.5.7. Preserve malicious logic reports as evidence for ongoing investigations until the conclusion of the investigation and supporting organizational Judge Advocate (JA) procedures. Include virus prevention, detection, eradication, and reporting procedures in user IA training.

6.5.8. Confirm implementation of malicious logic protection requirements according to DoDI 8552.01, *Use of Mobile Code Technologies in DoD Information Systems* and the DoD Policy Memorandum, *Mobile Code Technologies Risk Category List Update* (**https://powhatan.iiie.disa.mil/mcp/mcpdocs.html**).

**6.6. Telework.** A voluntary arrangement where an employee or service member performs assigned official duties at home or alternate worksites geographically convenient to the employee or Service member on a regular, recurring, or a situational basis (not including while on official travel).

6.6.1. Configure all teleworking government furnished equipment (GFE) for remote access with an approved encryption solution (e.g. VPN, SSL).

6.6.2. Use of a publicly accessed (wired or wireless) Internet Service Provider for remote access telecommuting is authorized provided the general guidelines in the DISA *Secure Remote Computing* STIG are followed for securing remote devices.

6.6.3. Do not process, store, or transmit DoD information on public ISs (e.g. public kiosks, hotel business computers).

6.6.4. Prior to implementing a telecommuting program, system IAOs will ensure compliance according to DoDI 1035.01, *Telework Policy* and the DISA *Secure Remote Computing, Remote Access Policy, and Wireless LAN Client* (if applicable) STIGs.

6.6.4.1. Users that telework complete and sign the DD Form 2946, *DoD Telework Agreement,* according to DoDI 1035.01.

6.6.4.2. Users must complete applicable training as outlined in the DISA *Remote Access Policy* STIG.

6.6.4.3. For specific organizational teleworking procedures see MTPO 00-33B-5006, Chapter 4.

6.6.5. Remote Telework Methods. Contact the organizational IAO and/or host Communications Squadron helpdesk for available remote telework method solutions (e.g., Virtual Private Networks (VPNs), application portal access [e.g., AF Portal, webmail], or virtual desktop applications).

6.6.5.1. For more detailed information on telework methods reference Special Publication (SP) 800-46, *Guide to Enterprise Telework and Remote Access Security*: **http://csrc.nist.gov/publications/PubsSPs.html**.

6.6.5.2. For approved virtual desktop solutions refer to: **http://iase.disa.mil/stigs/app_security/remote_desktop/remote_desk.html**

**6.7. Data Encryption.** Protect sensitive information (e.g., CUI, FOUO, Personally Identifiable Information [PII], Health Insurance Portability and Accountability Act [HIPAA], Privacy Act [PA], Proprietary) with strong encryption when transmitting data according to DODI 8500.2, DOD CIO Memorandum, "*Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile*

*Computing Devices and Removable Storage Media*," and 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).*

6.7.1. Implement approved DAR products (e.g., AF EPL, DoD Enterprise Software Initiative [for laptops]: **http://www.esi.mil/taglist.aspx**). If not explicitly listed on the Air Force or DoD approved products lists, but included as an integral component of OS (e.g., BitLocker), then refer to applicable DISA OS STIGs (Windows 7, SmartPhones, or Tablets for configuration requirements (**http://iase.disa.mil/stigs/os/index.html**).

**6.8. Privately-Owned hardware and software.** Privately owned hardware and software used to process unclassified and/or unclassified sensitive information requires operation mission justification and DAA approval according to DoDI 8500.2. Document the approval between the user and government organization. The organizational IAO maintains the documentation and provides it to the system IAM as required.

6.8.1. Violations of the IS user agreement and/or DoD IA training may result in the confiscation of personal hardware and software. Follow Security Forces and AF Office of Special Investigations (AF OSI) procedures along with supporting JA advice and guidance on confiscation of personal equipment.

6.8.2. Privately owned ISs contaminated with classified information will be confiscated and sanitized as specified in **Chapter 8**, Remanence Security.

6.8.3. Document in the enclave IS C&A package the approval for using privately owned systems to access government web sites (e.g., AF Portal, Outlook Web Access).

6.8.4. Do not connect privately-owned media or peripheral devices (including, but not limited to, music/video CD/DVDs, i-devices, commercial MP3 players, and Universal Serial Bus [USB] drives) to AF ISs and GFE.

6.8.5. Do not process or store Controlled Unclassified Information (CUI) or PII on privately owned systems to include mobile devices unless encrypted with approved DAR solution or PKI.

**6.9. Contractor-Owned Information Systems.** Contractor-owned or operated ISs must meet all security requirements for connection to the AF-GIG as defined in DoDI 8500.2, Enclosure 2, and AFI 31-601, *Industrial Security Program Management.*

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

6.9.2. On base contractors within AF-controlled facilities must comply with the *Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS)* and DoD 4161.2-M, *DoD Manual for the Performance of Contract Property Administration*.

6.9.3. Identification of all contractor-owned or operated IS equipment within AF facilities must be maintained by the organizational IAO.

6.9.4. Contractor ISs connected to the AF-GIG must comply with CJCSI 6211.02, *Defense Information Systems Network (DISN): Policy and Responsibilities.*

6.9.5. Any system configuration outside the normal baseline client image requires documentation in the IS C&A package and program contract.

**6.10. 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. This requirement applies to IS governed by international treaties and/or security agreements.

**6.11. Other Service or Agency Owned Information Systems.** Other service (i.e. Army, Navy, State Department, etc.) owned and operated ISs must meet all security requirements for connection to the AF-GIG as defined in AFI 33-210. Follow reciprocity and reuse procedures according to AFI 33-210.

**6.12. Mobile Computing Devices.** Mobile computing devices are IS devices such as Portable Electronic Devices (PEDs), laptops, and other handheld devices that can store data locally and access AF-managed networks through mobile access capabilities.

6.12.1. Configure and handle all devices according to applicable DISA STIGs (e.g. *Wireless, Sharing Peripherals Across the Network [SPAN], General Wireless Policy, Secure Remote Computing* and any updated/newly released STIGs [e.g., Android, Windows Mobile STIGs] **http://iase.disa.mil/stigs/index.html**) and CJCSI 6510.01. Obtain DAA approval for all non-compliant STIG configuration standards.

6.12.2. Prohibit connecting of privately-owned devices to the AF-GIG and introduction of privately owned devices into areas (e.g. rooms, offices) where classified information is processed and discussed, unless approved by the DAA. See paragraph 6.8.

6.12.3. IAOs ensure all users issued a mobile device sign an AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement,* according to AFI 10-712, paragraph 4.7.

6.12.4. IAOs ensure devices comply with the DAR requirements of paragraph 6.7.

6.12.5. The connection of government owned devices to the AF-GIG requires proper approval and documentation in the IS C&A package.

6.12.6. Identify software used on devices approved for use by the DAA in the IS C&A package.

6.12.7. IAO's ensure all devices are configured with an approved CAC readers and/or a DAA approved process for installation of PKI software according to the DISA *Wireless* STIG. See Chapter 4, Information System Access Control, for password requirements for devices not capable of supporting PKI.

6.12.7.1. Approved CAC readers for PEDs can be found on Infostructure Technology Reference Model (I-TRM) on the AF Portal.

6.12.7.2. Organizations working to comply with the mandate to use CAC readers and require the use of software certificates, must submit a Plan of Actions and Milestones (POA&M) to AF PKI Requirements Lead office. The AF PKI Requirements Lead office reviews the request and make recommendations to the AF DAA (AFSPC/A6). Once approved by AF DAA, use PKI software certificates for the minimum time necessary to comply with the CAC reader mandate.

6.12.7.3. Submit CAC reader waiver exceptions to the AF PKI Requirements Lead office. The Requirements Lead office reviews the request and makes recommendations to the AF DAA (AFSPC/A6).

6.12.7.4. See MPTO 00-33B-5006, Chapter 5, for the process to setup a CAC reader, and established standards, processes and procedures for using software certificates on BlackBerry devices. POA&M and waivers samples can also be found in this MPTO.

6.12.7.5. The DAA must approve CAC readers or PKI software certificates on personally owned PEDs that are used to transmit, receive, store, or process DoD information according to the DISA *General Wireless* STIG.

6.12.8. Users immediately report any lost or stolen device to the IAO using the reporting requirements outlined in AFI 31-401 and AFI 33-138 (to become AFI 33-115).

6.12.9. Do not use wireless-enabled devices in areas where classified information is discussed or processed without written approval from the DAA, the Certified TEMPEST Technical Authority (CTTA), and adherence to EMSEC requirements.

6.12.10. Use only approved secure (classified) mobile computing (e.g., Secure Mobile Environment [SME] PED) wireless devices for storing, processing, and transmitting classified information.

6.12.10.1. Encrypt classified data stored on secure (classified) mobile computing wireless devices using NSA-approved Type 1 cryptographic and key management systems according to CJCSI 6510.01.

6.12.10.2. Configure secure (classified) mobile computing wireless devices according to the appropriate the DISA STIG (e.g., *SME PED*).

6.12.11. Unclassified devices contaminated with classified information will be confiscated and sanitized according to **Chapter 8**, Remanence Security.

6.12.12. The organizational IAO educates device users on specific computer and physical security requirements as specified within this publication when traveling and at TDY locations (e.g., airports, hotels).

6.12.13. 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.

6.12.14. Protect devices at the applicable security classification of the information stored in the device according to AFI 31-401.

6.12.15. Maintain positive control over all hardware peripheral devices (e.g., portable printer devices, removable media (Universal Serial Bus [USB] storage devices, optical media, external hard drives, power accessories, etc.) that may accompany the mobile computing device.

6.12.16. Air Force Space Command (AFSPC) is the approval authority for all optional security settings for all wireless devices as defined in the appropriate DISA STIGs Configuration Tables located at http://iase.disa.mil/stigs/net_perimeter/wireless/Pages/index.aspx. Requests for optional settings must be submitted through the enclave/system ISSM for entry into the configuration management process. Optional settings that degrade the

system/enclave security posture must be submitted via the AF Form 4169 and routed through AFSPC/CYSS and AFSPC/A6. **(T-1)**

6.12.16.1. Approved DoD Mobile Device (i.e.Blackberry® or other smartphones) users will complete AF Form 4433 and annotate the optional settings authorized and the date the specialized OPSEC training was completed. This OPSEC training needs be accomplished annually is accessed via ADLS and is available at https://golearn.csd.disa.mil/kc/login/login.asp.

**6.13. 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). Output devices receive data from the desktop or laptop providing a display or printed product (e.g. monitors, printers, and multifunction devices).

6.13.1. Regardless of the classification, configure and handle peripheral devices (e.g., multifunction devices, printers, digital senders, scanners) according to the DISA *Removable Storage and External Connection Technologies* STIG and identify in the IS C&A package.

6.13.2. Any deviation to the configuration specified in the DISA *Removable Storage and External Connection Technologies* STIG requires approval by the DAA, to include classified networks and systems.

6.13.3. MFDs connected to unclassified and/or classified ISs must be documented in the IS C&A package and approved by the DAA.

6.13.3.1. Use the Voice Protection System (VPS) to secure unclassified Multifunction Device (MFD) connections. See AFI 33-111, *Voice Systems Management* (to become AFI 33-145) for VPS connection requirements and guidance.

6.13.3.2. On classified MFD's, disable facsimile capabilities at the hardware level to prevent classified information spillage. Prohibit physical connections to the fax portion of the MFD and disable this capability by human and technological means according to the DISA *Multi-Function Device (MFD)* STIG.

6.13.4. Appropriately mark and label peripheral devices according to the highest level of classification processed or displayed on the device according to DoD 5200.1-R and DoD 5220.22-M. Authorized users must be clearly notified of the presence of the information needing protection and all applicable protection methods.

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

6.13.4.1.1. 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.

6.13.4.1.2. Mark and label all KVM switches (regardless of classification environment) to identify the switch position and the associated classification of the connected systems according to the DISA *Sharing Peripherals Across the Network (SPAN), Keyboard, Video, Mouse Switch Security* STIG.

6.13.4.2. Physically mark and label all mobile computing devices with the potential to be located/used in a mixed environments or publically accessible areas with the highest classification level of the information approved to be processed by the device. WIAO's may develop appropriate physical marking and labeling methods based on the local operating environment requirements.

6.13.5. Password and authentication methods (e.g., PKI enabled MFDs) must follow the guidance in paragraph **4.4**.

6.13.6. Dispose of peripheral devices containing non-volatile memory according **Chapter 8**, Remanence Security.

6.13.7. All Bluetooth peripheral devices, to include keyboard/mouse/pointer devices, must comply with Bluetooth requirements outlined in the Wireless STIG and specific requirements published by the NSA at **https://www.nsa.gov/ia/_files/wireless/BlueToothDoc.pdf**, DoD Bluetooth Peripheral Device Security. The only exception is to the FIPS 140-2 requirement for Bluetooth keyboards, mice and pointing devices used on the unclassified Air Force Network (AFNET). The risk for use of these non-FIPS 140-2 certified devices has been accepted by the AF due to the lack of device availability in the commercial marketplace. Acquisition of these devices needs to be done through approved sources (i.e. AFWAY).

6.13.7.1. The use of headsets with Bluetooth technology for unclassified voice communication for Government-authorized mobile devices is approved for use within the Air Force while driving a motor vehicle and for on-base, mission-required communications, to include Voice over Internet Protocol (VoIP) headsets in unclassified work environments. This approval enhances the safety of AF personnel using mobile devices and complies with Federal, State and local policies while driving on public roads and AFI 91-207, *The US Air Force Traffic Safety Program*, when driving on military installations. This approval is limited to hands-free unclassified voice, not data. The organizational commander should determine what is mission-required use.

6.13.7.2. All Health Insurance Portability and Accountability Act (HIPAA) compliant medical Bluetooth devices determined to be medically necessary or beneficial to patient care are authorized for use with AFNET and CMD devices with or without FIPS 140-2 certification.

6.13.7.3. Organizations must ensure Bluetooth® peripheral devices are procured and managed IAW AFMAN33-153. **(T-1)**

**6.14. Removable Media.** Removable media is any type of storage media designed to be removed from a computer. See the AF DAA *Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133 (Removable Flash Media device implementation within and between Department of Defense (DoD networks))* memorandum for removable media and flash media definitions (https://cs.eis.af.mil/afdaa/cto10133/AF%20DAA%20Docs/Forms/AllItems.aspx).

6.14.1. Configure and handle all approved removable media devices according to all applicable DISA STIGs and CJCSI 6510.01.

6.14.1.1. Classified and unclassified information stored on removable flash media must be physically controlled and safeguarded according to the USCYBERCOM *Removable*

*Flash Media device implementation within and between Department of Defense (DoD) networks* CTO 10-084 (**https://www.cybercom.mil/J3/orders/default.aspx**).

6.14.2. Report immediately the loss of any removable media device to the organizational IAO or wing IA according to requirements outlined in AFI 31-401, AFI 33-138 (to become AFI 33-115), and any locally developed procedures.

6.14.3. Protect removable media containing PII and CUI taken outside organizational networks according to CJCSI 6510.01 and DODM 5200.01, Vol. 4.

6.14.3.1. The IAO ensures information stored on removable media complies with the DAR requirements of paragraph **6.7** and configured according to the DISA *End Point STIG*.

6.14.3.2. USB approved external or optical media devices must be approved by the ISO in accordance with AFI 33-332 prior to storing PII electronic records assigned as High or Moderate Impact categories require DAA approval through the C&A process or as defined in CTO 10-084.

6.14.3.3. Users immediately report any lost or stolen removable media device containing CUI or PII according to paragraph 6.14.2.

6.14.4. Ensure the safeguarding, marking, and labeling of all media according to the requirements for the highest level of information ever contained on the media according to DoD 5200.1-R and AFI 33-332.

6.14.4.1. Ensure proper classification, marking, storing, transportation, and destruction of removable flash media devices according to AFI 31-401 and remanence security guidelines.

6.14.5. Configure removable media and related peripherals using physical or software configuration settings to disable "write" mechanisms for all forms of removable media on SIPRNet ISs. See a full description in the USCYBERCOM *Protection of Classified Information on Department of Defense (DoD) Secret Internet Protocols Router Network (SIPRNet)* CTO 10-133 (https://www.cybercom.mil/default.aspx).

6.14.5.1. Organizations with a mission requirement to write to removable media must first submit requests for a waiver to the AO (formerly DAA) or alternate approving authority (e.g., Group Commander) according to the *AF DAA Combined Implementation Guidance for USCYBERCOM CTO 10-084 and CTO 10-133 Memorandum* located at https://cs.eis.af.mil/afdaa/cto10133/AF%20DAA%20Docs/Forms/AllItems.aspx. **(T-0)**

6.14.5.2. Organization commanders must 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 (formerly system IAO) will submit a request to remove the device/user account from the waiver and the USB ports/CD Drives must be disabled. **(T-1)**

6.14.5.3. Users are required to notify the approving waiver authority if the waiver requirement is no longer needed. **(T-2)**

6.14.6. Non-Volatile “flash” media refers to 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.

6.14.6.1. Removable flash media use is prohibited until organizations have identified procedures, put appropriate technologies in place, and have received approval from the DAA or alternate approving authority (e.g., Group Commander) according to the AF DAA *Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133* memorandum (**https://cs.eis.af.mil/afdaa/cto10133/AF%20DAA%20Docs/Forms/AllItems.aspx**).

6.14.6.2. Removable flash media use is only authorized pursuant to CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media,* policy in conjunction with the procedures and technologies described in the USCYBERCOM *Removable Flash Media device implementation within and between Department of Defense (DoD networks),* CTO 10-084.

6.14.6.3. Permit only DAA or the alternate approving authority (e.g., Group Commander) approved and government procured "flash" media devices according to the AF DAA *Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133* memorandum.

6.14.6.4. Only USB removable flash media (USB thumb drives) devices that meet the standards outlined in the FIPS140-2 for encryption are authorized for purchase and use on the AF-GIG. For a current listing go to the USCYBERCOM website: **https://www.cybercom.mil**/.

6.14.6.5. Approved and authorized removable flash media use is subject to requirements appropriate for the classification level of the data contained within the device according to the applicable DISA STIG and applicable local procedures.

6.14.6.5.1. The organizational IAO maintains a list of authorized users accountable for the use of these devices.

6.14.6.5.2. The organizational IAO maintains a list of authorized removable flash media devices under their control.

6.14.6.5.3. The organizational IAO submits a complete list of all removable flash media devices to the wing IA office in September of every year. Maintain records according to AFRIMS, RDS, Table and Rule: T33 - 45 R 09.00.

6.14.6.6. Removable flash media devices will be marked externally indicating classification of data stored on the device and the device serial number.

6.14.6.7. Devices that use removable flash media (non-volatile memory) used to store PII/CUI must comply with requirement outlined for data-at-rest.

6.14.6.8. 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.

6.14.7. Assign all devices covered by this section to an automated digital processing equipment account and will be 100% accountable in the Asset Inventory Management system or the most current, mandated IT inventory control system.

**6.15. Wireless Services.** Wireless services integrated or connected to AF ISs will comply with DoDD 8500.01and DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG).*

6.15.1. All AF wireless IS services will be configured according to the applicable DISA *Wireless* STIGs.

6.15.1.1. Data encryption for unclassified information must be implemented end-to-end over an assured channel and certified under the NIST Cryptographic Module Validation Program (CMVP) as meeting requirements per FIPS 140-2 according to DoDD 8100.02. Secure classified information within NSA-approved Type-1 encryption solutions according to the DISA *Wireless* STIG.

6.15.1.2. Configure all unclassified wireless peripheral devices (e.g., keyboards, mice, pointers/forwarders, etc.) with FIPS 140-2 encryption according to the DISA *Wireless* STIG.

6.15.1.3. Individual exceptions to unclassified wireless encryption may be granted on a case-by-case basis after an operational risk assessment and approval by the DAA according to DoDD 8100.02.

6.15.2. The IAO ensures proper procedures, in coordination with the Unit Security Manager (USM), are in place to prevent the introduction of unauthorized wireless devices into unclassified and classified areas.

6.15.3. All wireless capabilities will follow applicable EMSEC guidance.

6.15.3.1. In areas where classified information is discussed or processed, do not use wireless capabilities without written approval from the DAA, the Certified TEMPEST CTTA, and adherence to EMSEC requirements. See paragraph **6.12.10** for use of mobile computing wireless devices within classified environments.

6.15.4. Configure wireless network solutions according to the DISA Wireless STIGs and CJCSI 6510.01. Document wireless configurations in the IS C&A package and obtain DAA approval according to DoDD 8100.2. **(T-0)**

6.15.4.1. For commercial Internet Service Provider (ISP) connections (e.g., fixed, mobile), follow configuration and waiver requirements outlined in AFI 33-200.

6.15.4.2. Configure mobile device wireless network solutions according to the applicable DISA *Wireless* STIGs. See paragraph 6.12.

6.15.5. Configure wireless network interface cards according to the applicable DISA STIG.

6.15.6. Voice over Internet Protocol (VoIP) wireless services are not authorized until properly tested, certified, and approved to connect according to TCNO 2008-353-001 (**https://33nws.lackland.af.mil/advisories/advisory_list.asp**).

6.15.6.1. All phones must meet the VoIP requirements according to AFI 33-111, *Voice Systems Management* (to become AFI 33-145) and will be configured and handled according to the DISA *Video and Voice over IP (VVoIP)* STIG.

**6.16. 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 to prevent unauthorized users from seeing and/or hearing national security information and material at another user's workstation area. This policy establishes the minimum technical and procedural controls required to reduce these risks.

6.16.1. The system IAM ensures the use of cameras/microphones in unclassified and/or classified environments is documented and approved in the IS C&A package. Protect collaborative computing devices used in classified environments according to paragraph **6.2**.

6.16.2. Configure webcams and attached microphones according to the DISA *Video and Voice over IP (VVoIP)* STIG: http://iase.disa.mil/stigs/net_perimeter/telecommunications/Pages/voip.aspx.

6.16.2.1. The user controls the projection of information viewable by the webcam according to DoD 5200.1-R.

6.16.2.2. Collaborative computing mechanisms that provide video and/or audio conference capabilities must provide a clear visible indication that video and/or audio mechanisms are operating to alert personnel when recording or transmitting according to the DISA *VVoIP* STIG.

6.16.3. Training on video teleconferencing must include requirements identified in the DISA *Video Tele-Conference (VTC*) STIG: http://iase.disa.mil/stigs/net_perimeter/telecommunications/Pages/vtc.aspx.

**6.17. Non-enterprise activated (NEA) Commercial Mobile Devices (CMD).** A NEA CMD is any mobile handheld device that does not store credentials used to login to a DoD network or information system (wired or wireless) or to a PC that is/will be connected to a DoD network, is not configured to process, store or display sensitive information from a DoD electronic messaging system, and is not centrally controlled or monitored from a DoD network.

6.17.1. NEA CMDs acquired through the AF IT Commodity Council (ITCC) are approved for use within the Air Force. The devices can be used for any non-sensitive unclassified DoD tasks and to process/store publically available information. Personal CMDs are not authorized for any non-sensitive unclassified DoD tasks.

6.17.1.1. NEA CMD devices are prohibited from storing and/or processing classified information, Controlled Unclassified Information (CUI), HIPAA information, and other sensitive information. Examples of valid use cases include conducting training, monitoring meteorological data, viewing flight maps, and non-sensitive recruiting activities. The following policies apply to non-enterprise activated commercial mobile devices.

6.17.1.1.1. Government-owned NEA CMDs need to be configured according to General Mobile Device (Non-Enterprise Activated) STIG and applicable MPTO, to include passwords and passcodes.

6.17.1.1.2. Government-owned NEA CMDs need to be listed on DoD Unified Capabilities (UC) Approved Products Lists and procured using normal acquisition channels and/or AF ITCC Blanket Purchase Agreement.

6.17.1.1.3. Organizations must ensure government-owned NEA CMDs are tracked and managed IAW AFI 33-590, *Radio Management* and AFMAN 33-153. **(T-2)**

6.17.1.1.4. Do not use DoD-issued software certificates on NEA CMDs.

6.17.1.1.5. All NEA CMDs are authorized to use hardware tokens via CAC readers and access any public facing DoD PKI-enabled websites.

6.17.1.1.6. Organizations must ensure NEA CMDs involved in classified spillages incidents are reported to the local security manager and sanitized per Chapter 7, this manual. **(T-2)**

6.17.1.1.7. If sensitive unclassified information is accessed from a NEA CMD, users shall consult with their IAO to delete files from storage, clear browser history and cache, and if necessary, sanitize the CMD.

6.17.1.1.8. NEA CMD users shall complete approved CMD OPSEC Training provided by AFSPC or, when published from DISA http://iase.disa.mil. **(T-2)** OPSEC training can be accessed via ADLS and is available at https://golearn.csd.disa.mil/kc/login/login.asp.

6.17.1.1.9. Organizational IAOs (to be Cybersecurity Liaisons) need to ensure all NEA CMD users sign the AF Form 4433, IAW para. 6.12.3 this manual and will ensure completion of CMD OPSEC training by annotating completion in Block 12 of the form.

6.17.1.1.10. The Program Manager, in the case of NEA CMDs being fielded as a part of a PMO system, or the organizational commander, in all other cases, will validate all software applications installed on non-enterprise activated CMDs. **(T-2)**

6.17.1.1.10.1. For each application that requires purchasing, licenses shall be acquired per the company's software licensing agreement. Licenses will be tracked to ensure fiscal responsibility and prevent duplicate purchases IAW AFMAN 33-153.

6.17.1.1.10.2. Typically, administrators are the only individuals authorized to download and install approved applications. Users of government-owned NEA CMDs are not authorized to download and install software, unless from an approved government/DoD App Store, when available or other AFSPC approved process.

6.17.1.1.10.3. In accordance with DoD CIO Memorandum, *DoD Commercial Mobile Device (CMD) Interim Policy*, para 3.2., installed applications must be validated against DISA's security evaluation criteria and appear on the DoD Approved CMD Application List, once available. **(T-0)** Air Force approved mobile applications are listed on the Air Force Evaluated Products List (AF EPL) at https://cs3.eis.af.mil/sites/afao/Lists/COTSGOTS%20Software/EPL.aspx?View={0D6A1DD1-7065-4702-9FEE-AE9F7A2432CF}&FilterField1=COTS%5Fx0020%5FType&FilterValue1=Mobile%20Application under the "Mobile App" COTS/GOTS Type. If not already validated and approved, the PMO or organization shall sponsor the application under the "Mobile App" COTS/GOTS Type. If not already validated and approved, the PMO or organization shall sponsor the application for testing and evaluation, instructions for submission are found on the Air Force DAA's AF Mobile SharePoint Site https://cs3.eis.af.mil/sites/afao/mobile/CMT%20MemosPolicys/Forms/AllItems.aspx.

6.17.1.1.11. Organizations/administrators must ensure Notice to Consent banners are displayed on all government-owned CMDs, when possible. Additionally, the use of Standard Form 710, *Unclassified Label,* and "If found, Return to" labels are recommended as a best practice. **(T-2)**

6.17.1.1.12. The NEA CMD user must report the loss of their device to his/her security manager. **(T-2)** The lost device is remotely wiped (through previously installed wiping application or by cellular carrier) and the corresponding service plan suspended, if applicable.

6.17.1.1.13. Functional organizations or PMOs need to develop a process for auditing NEA CMDs on a recurring basis to ensure no unauthorized changes or misuse.

6.17.1.1.14. Use of all NEA CMDs needs to be in accordance with all existing OPSEC and EMSEC guidance.

**6.18. Enterprise activated CMD.** Enterprise activated CMDs are government-issued devices and must be part of an approved/accredited system (e.g., Blackberry or other DoD approved smartphones) and follow configuration and operation guidance according to the DISA Commercial Mobile Device (CMD) Policy STIG, CMD Management Server Policy STIG, Mobile Policy Security Requirements Guide (SRG), and the applicable Smartphone/Tablet STIG. The devices can be used for any sensitive unclassified DoD tasks and process, store, or display sensitive information using FIPS 140-2 validated encryption.

## Chapter 7

## DATA SPILLAGE AND COMPUSEC INCIDENT REPORTING

**7.1. Introduction.** An incident is defined as an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS; or when the information on the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security polices, security, procedures, or acceptable use policies (See Committee on National Security Systems Instruction [CNSSI] 4009).

7.1.1. The ISO ensures the IS is monitored to detect and react to incidents, intrusions, disruption of services, or other unauthorized activities that threaten the security of DoD operations or IT resources, in accordance with CSCSI 6510.01, DoDI 8500.2, and the applicable DISA STIGs.

7.1.2. The Incident Response Plan (IRP) for the IS defines reportable incidents, outline standard operating procedures, establish an incident response team, and is exercised at least every six months, according to DoDI O-8530.2, *Support to Computer Network Defense, (CND).*

7.1.2.1. The IAO ensures reporting procedures identify user actions for reporting CAC removal screen lock malfunctions and violations of IA policy. See MPTO 00-33B-5007, *Security Incident Management for Information Systems,* Chapter 3, Section 3.4.4., and Table 2-1, for specific guidance.

7.1.2.2. The IAO reviews and/or updates reporting procedures every six months or sooner, as mission dictates.

7.1.2.3. The IAO/IAM documents the results of the exercise.

7.1.3. When classified information is processed or maintained on an unclassified IS, the individual discovering the incident follows the procedures in paragraph **7.4** and initiates security incident procedures according to DoD 5200.1-R, AFI 31-401, *Information Security Program Management*, and reporting requirements from AFI 33-138 (to become AFI 33-115).

7.1.4. The system/device in question must be confiscated if directed by the IRP chief and/or physically guarded and stored appropriately according to the suspected level of classification on the device until the original classification authority is contacted and/or appropriate Security Classification Guide is reviewed to determine if an incident has occurred.

7.1.5. If the determination indicates contamination, the system/device is contaminated it must be sanitized or destroyed according to **Chapter 8**, Remanence Security.

7.1.5.1. See paragraph **6.8.2** for confiscation guidance on privately owned ISs involved in a data spillage or CMI.

7.1.6. The Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, *Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program)* provides Computer Network Defense (CND) processes to rapidly identify and respond to incidents that adversely affect AF ISs.

7.1.7. Specific procedural information for incident response is located in MPTO 00-33B-5007.

**7.2. Data Spillage.** Data spillage occurs when a higher classification level of data is placed on a lower classification level system/device according to CNSSI 4009. For example, when a user takes a file such as a word document and copies it to removable media (e.g. DVD or CD) from SIPRNET and then the user takes that media and loads the data onto a NIPRNET computer.

7.2.1. Data spillage should not be confused with a CMI. A CMI is a data spillage but a data spillage is not necessarily a CMI.

**7.3. Classified Message Incidents.** A classified message incident occurs when higher classification level of data is transferred to a lower classification level system/device via messaging systems according to AFI 33-138 (to become AFI 33-115, *AF GIG Services*).

**7.4. Incident Response Flow.** Incident response planning must include appropriate tasks to secure the computing environment from further malicious activity and preserve computer forensic evidence for analysis.

7.4.1. User disconnects affected IS or media from the network (i.e. removal of network cable, turn off wireless capability, etc.). Do not turn off the IS. Protect the IS or media accordingly to its highest classification level of data involved.

7.4.2. User notifies organizational or system IAO or other designated representative as outlined in local operating instructions such as the Unit Security Manager (USM), supervisor, security manager, servicing network control center, etc. The USM notifies the wing Information Protection (IP) office as soon as possible (preferably within 24 hours).

7.4.3. IAO or other designated representative initiates containment, which may include notification of all affected parties.

7.4.4. IAO or other designated representative begins reporting process such as the Wing IA office, unit leadership, affected server operations, all users affected to include owners of any affected mail accounts or network user accounts.

7.4.5. IAO or other designated representative identifies key information for sanitization.

7.4.6. IAO or other designated representative hands over sanitization process to Client Support Technicians (CSTs) who then follow local procedures (see MPTO 00-33B-5007) to eliminate the affected file(s).

7.4.7. IAOs or other designated representatives at every level must understand this flow. IAO must educate users to this process. Basic incident response procedures are located in MPTO 00-33B-5007.

**7.5. CMD Spillage.** Commanders and users will follow NSA Guidance, NSA MIT-005FS-2014, *Mitigations for Spillage of Classified Information onto Unclassified Mobile Devices*, and the Air Force Authorizing Official memorandum, *Commercial Mobile Device Spillage Policy* **https://cs3.eis.af.mil/sites/afao/mobile/CMT%20MemosPolicys/Forms/AllItems.aspx**, for handling CMD spillage . Contact HQ AFSPC/A2/3/6 A6S, DSN 692-5880, **afspc.a6s@us.af.mil** for questions on CMD spillage. **(T-0)**

## Chapter 8

## REMANENCE SECURITY

**8.1. Introduction.** Remanence security is actions taken to protect the confidentiality of information on ISs. Methods to protect confidentiality include sanitization, overwriting, and destruction. Each method provides specific levels of information protection.

8.1.1. Unless determined by mission or operational need and documented in the IS C&A package or directed by the IP chief, the destruction of any media is the preferred method for all rather than clearing or sanitizing. See USCYBERCOM CTO 10-084 and the DISA *Removable Storage and External Connection Technologies* STIG for higher risk data transfer requirements.

8.1.1.1. In situations where a media sanitization plan of action is not clearly defined and governed by this guide, MPTO 00-33B-5008, *Remanence Security for Information Systems*, or the IS C&A package, exercise risk management procedures according to guidelines in DoDD 8500.01, CJCSI 6510.01, and NIST Special publication 800-88, *Guidelines for Media Sanitization*. Balance risk management decisions on information sensitivity, threats and vulnerabilities, and the effectiveness and potential impact of the decided action.

8.1.1.2. Consider mitigation options (e.g., clearing, sanitization, destruction) based on operational risk management as approved within the IS C&A package before sanitizing IS media due to classified information spillages. Notify the wing IAO of the selected sanitization method.

8.1.2. All unclassified IS storage media will be sanitized before leaving the control of the DoD, according to the Deputy Secretary of Defense Memorandum, *Disposition of Unclassified Hard Drives*, dated 4 June 2001.

8.1.2.1. Track and dispose of unclassified IS storage media previously contaminated with classified data as classified media. Destroy according to the declassification procedures of NSA/CSA Policy Manual 9-12, *NSA/CSS Storage Device Declassification Manual.*

8.1.3. Prohibit reuse of classified IS storage media in unclassified environments; destroy according to CJSCI 6510.01 and the declassification procedures of NSA/CSA Policy Manual 9-12. Classified IS storage media can be reused in an IS environment at the same or higher classification level.

8.1.4. Specific procedural information for remanence security is located in MPTO 00-33B-5008.

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

*Air Force (AF) Internal Basic Assurance (IBA) X.509 PKI Certificate Policy (CP), (v1.0),* January 2014

*Certification Practices Statement for the United States Air Force Internal Medium Assurance Subordinate Certification Authorities, (v3.0),* February 19, 2010

Committee on National Security Systems Policy (CNSSP) No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 10, 2013

Defense Information Systems Agency (DISA) *Wireless Security Technical Implementation Guide Overview*, Version 6, Release 9, October 24, 2014

Deputy DoD CIO Memorandum, *Use of Commercial Mobile Devices Not Connected to Department of Defense Networks*, July 31, 2012

DoD CIO Memorandum, *Department of Defense Commercial Mobile Device Implementation Plan*, February 15, 2013

DoD CIO Memorandum, *DoD Commercial Mobile Device (CMD) Interim Policy*, January 17, 2012

DoD CIO Memorandum, *Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD),* April 6, 2011

DoDI 8500.1, *Cybersecurity*, March 14, 2014, March 12, 2014

National Information Assurance Partnership (NIAP), *Mobile Device Fundamentals Protection* Profile (**https://www.niap-ccevs.org/pp/PP_MD_v2.0/**

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

*Title 5 United States Code, Section 552a (Privacy Act),* update January 7, 2011

*Title 8 Code of Federal Regulations (CFR), Aliens and Nationality*, electronic CFR (e-CFR) March 23, 2011

*National Science and Technology Council Subcommittee on Biometrics Glossary*, September 14, 2006

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46, *Guide to Enterprise Telework and Remote Access Security,* April 2010

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, September 2006

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

National Security Agency (NSA)/ Central Security Service (CSS) Policy Manual 9-12, *NSA/CSS Storage Device Declassification Manual*, March 13, 2006

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

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

CJCSM 6510.01, *Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program),* June 24, 2009

CNSS-14-2011, *(U/FOUO) Approval of Continued Use of SC560 Token –DECISION MEMORANDUM,* February 17, 2011

CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media*, November 2010

CNSSI 4009, *National Information Assurance (IA) Glossary*, April 26, 2010

CJCSI 6211.02, *Defense Information System Network (DISN): Policy and Responsibilities,* July 9, 2008

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, May 15, 2011

*United States Air Force Internal Medium Assurance Public Key Infrastructure Root Certification Authority Certification Practice Statement (v2.3)*, March 29, 2013

*X.509 Certificate Policy for the United States Air Force Internal Medium Assurance PKI, (v2.2),* February 19, 2010

*X.509 Certificate Policy for United States Department of Defense*, February 9, 2005

Federal Information Processing Standard (FIPS)140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001

DoD 4161.2-M, *DoD Manual for the Performance of Contract Property Administration,* December 31, 1991

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 1*, March 21, 2012

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012; *Incorporating Change 1*, March 21, 2012

DoDM 5200.01, Volume 4, *Controlled Unclassified Information (CUI)*, February 24, 2012

DoD 5200.2-R, *Personnel Security System,* 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

DoD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, October 21, 2010

DoD 8570.01-M, *IA Workforce Improvement Program*, December 19, 2005; Incorporating Change 2, April 20, 2010

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; Incorporating Change 1, July 28, 2011

DoDD 8100.02 *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),* April 14, 2004; Certified Current as of April 23, 2007

DoDD 8521.01, *Department of Defense Biometrics,* February 21, 2008

DoDI 1035.01, *Telework Policy,* October 21, 2010

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

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

DoDI O-8530.2, *Support to Computer Network Defense, (CND),* March 9, 2001

DoDI 8552.01, *Use of Mobile Code Technologies in DoD Information Systems*, October 23, 2006

DoD Antivirus Solutions, **http://www.disa.mil/antivirus/index.html**

DoD CIO Memorandum, *Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement,* May 9, 2008

DoD Policy Memorandum, *Mobile Code Technologies Risk Category List Update,* March 14, 2011, **https://powhatan.iiie.disa.mil/mcp/mcpdocs.html**

Directive-Type Memorandum (DTM) 08-003, *Next Generation Common Access Card (CAC) Implementation Guidance,* December 1, 2008; Incorporating Change 3, September 27, 2011

DISA Security Technical Implemenation Guides (STIGs), **http://iase.disa.mil/stigs/**

SAF/XC Memorandum, *Air Force Guidance Memorandum to amend SAF/XC Memo, PKI Capability for Mobile Devices, dated 24 September 2009,* March 23, 2010

SAF/XC Memorandum, *PKI Capability for Mobile Devices,* September 2009

USCYBERCOM Communications Tasking Orders (CTOs), **https://www.cybercom.mil/default.aspx**

AFSPC/A6 *Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133* Memorandum, July 6, 2011

AFMAN 33-152, *User Responsibilities and Guidance for Information Systems,* June 1, 2012

AFMAN 33-153, *Information Technology (IT) Asset Management (ITAM),* March 19, 2014

AFI 10-701, *Operations Security (OPSEC),* June 8, 2011

AFI 10-712, *Telecommunications Monitoring and Assessment Program,* June 8, 2011

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

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* December 1, 2004

AFI 31-401, *Information Security Program Management Information Security Program Management,* November 1, 2005

AFI 31-501, *Personnel Security Program Management,* January 27, 2005

AFI 31-601, *Industrial Security Program Management,* June 29, 2005

AFI 33-111, *Voice Systems Management,* March 24, 2005

AFI 33-115, *Air Force Information Technology (IT) Service Management,* September 16, 2014

AFI 33-200, *Information Assurance (IA) Management,* December 23, 2008

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP),* December 23, 2008

AFI 33-332, *Air Force Privacy Program,* May 16, 2011

AFI 33-360, *Publications and Forms Management,* Sep 25, 2013

AFI 33-590, *Radio Management,* April 8, 2013

AFI 36-2201, *Air Force Training Program,* March 8, 2011

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

AFI 63-101, *Acquisition and Sustainment Life Cycle Management,* April 17, 2009

AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program,* June 17, 2011

AFMAN 33-363, *Management of Records,* March 1, 2008

AFI 90-201, *The Air Force Inspection System,* 2 August 2013, Incorporating Change 1 10 March 2014

AFI 91-207, *The US Air Force Traffic Safety Program,* September 12, 2013

AFPD 10-7, *Information Operations,* September 6, 2006

AFPD 33-2, *Information Assurance (IA) Program,* August 3, 2011

AFPD 63-1/20-1, *Acquisition and Sustainment Life Cycle Management,* April 3, 2009

Air Force Records Information Management System (AFRIMS), Records Distribution System (RDS), **https://www.my.af.mil/afrims/afrims/rims.cfm**

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

Information Assurance, *Platform Information Technology Guidebook*

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

MPTO 00-33B-5006, *End point Security for Information Systems*

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

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

MTO 2009-070-101, *Reduce Smart Card Logon (SCL) Exemptions*

T.O. 00-5-1-WA-1, *Air Force Technical Order System*, October 1, 2007

T.O. 00-5-3-WA-1, *Air Force Technical Order Life Cycle Management,* March 1, 2007

T.O. 00-33A-1202-WA-1, *Air Force Network Account Management,* May 12, 2011

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

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

***Prescribed Forms***

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

***Adopted Forms***

Standard Form (SF) 312, *Nondisclosure Agreement*

Standard Form (SF) 700, *Security Container Information Form*

DD Form 2056, *Telephone Monitoring Notification Decal*

DD Form 2842, *Department of Defense (DoD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities*

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

DD Form 2946, *DoD Telework Agreement*

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

AF Form 847, *Recommendation for Change of Publication*

***Abbreviations and Acronyms***

**2GWLAN**—2nd Generation Wireless Local Area Network

**ADLS**—Advanced Distributed Learning System

**ADX**—Active Directory Exchange

**AETC**—Air Education and Training Command

**AF**—Air Force (as used in forms)

**AFCAP**—Air Force Certification and Accreditation Program

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFNet**—Air Force Network

**AFNIC**—Air Force Network Integration Center

**AFPC**—Air Force Personnel Center

**AFPD**—Air Force Policy Directive

**AFRIMS**—Air Force Records Information Management System

**AFSPC**—Air Force Space Command

**AFSSI**—Air Force System Security Instruction

**AFSUP**—Air Force Supplement

**ALT**—Alternate Logon Token

**BIMA**—Biometrics Identity Management Agency

**CA**—Certificate Authority

**C&A**—Certification and Accreditation

**CAC**—Common Access Card

**CCO**—Cyber Control Order

**CD**—Compact Disk

**CE**—Computing Environment

**CIO**—Chief Information Officer

**CJCSI**—Chairman of the Joint Chiefs of Staff Instruction

**CJCSM**—Chairman of the Joint Chiefs of Staff Manual

**CMI**—Classified Message Incident

**CND**—Computer Network Defense

**CNSSI**—Committee on National Security Systems Issuances

**CNSSP**—Committee on National Security Systems

**COMPUSEC**—Computer Security

**COMSEC**—Communications Security

**CoP**—Community of Practice

**CPS**—Certificate Practice Statement

**CST**—Client Support Technician

**CTTA**—Certified TEMPEST Technical Authority

**CTL**—Certificate Trust List

**CTO**—Communications Tasking Order

**CUI**—Controlled Unclassified Information

**CVS**—Contractor Verification System

**DAA**—Designated Accrediting Authority

**DaR**—Data at Rest

**DEERS/RAPIDS**—Defense Enrollment Eligibility Reporting System/Real-Time Automated Personal Identification System

**DFARS**—Defense Federal Acquisition Regulation Supplement

**DIACAP**—DoD Information Assurance Certification and Accreditation Process

**DISA**—Defense Information Systems Agency

**DISN**—Defense Information Systems Network

**DoDD**—Department of Defense Directive

**DoD**—Department of Defense

**DoDI**—Department of Defense Instruction

**DoDIIS**—DoD Intelligence Information System

**DPI**—Digital Printing and Imaging

**DRU**—Direct Reporting Unit

**DSS**—Defense Security Service

**DVD**—Digital Versatile Disc

**EPL**—Evaluated Products List

**EMSEC**—Emission Security

**EXCOM**—Executive Committee

**FAR**—Federal Acquisition Regulation

**FDCC**—Federal Desktop Core Configuration

**FDO**—Foreign Disclosure Office

**FIPS**—Federal Information Processing Standards

**FISMA**—Federal Information Security Management Act

**FMAA**—Flash Media Approval Authority

**FN/LN**—Foreign National/Local National

**FOA**—Field Operating Agencies

**FOIA**—Freedom of Information Act

**FOUO**—For Official Use Only

**FQDN**—Fully Qualified Domain Name

**GAL**—Global Address List

**GFE**—Government Furnished Equipment

**GIG**—Global Information Grid

**GSA**—General Services Administration

**HD**—Hard Drive

**HIPAA**—Health Insurance Portability and Accountability Act

**HQ**—Headquarters

**HQ AETC**—Headquarters Air Education and Training Command

**HQ AFSPC**—Headquarters Air Force Space Command

**IA**—Information Assurance

**IAM**—Information Assurance Manager

**IAO**—Information Assurance Officer

**IASE**—Information Assurance Support Environment

**ID**—Identification

**IMT**—Information Management Technology

**I-NOSCs**—Integrated Network Operations and Security Centers

**INFOSEC**—Information Security

**IP**—Information Protection

**IS**—Information Systems

**ISO**—Information System Owners

**ISP**—Internet Service Provider

**IT**—Information Technology

**ITCC**—Information Technology Commodity Council

**I-TRM**—Infostructure Technology Reference Model

**ITS**—Information Transport System

**JA**—Judge Advocate

**JWICS**—Joint Worldwide Intelligence Communications System

**KVM**—Keyboard, Video, Monitor

**LAN**—Local Area Network

**LRA**—Local Registration Authority

**MAJCOM**—Major Command

**MFD**—Multifunction Device

**MPF**—Military Personnel Flight

**MPTO**—Methods and Procedures Technical Orders

**MTO**—Maintenance Tasking Order

**NetD**—Network Defense

**NIPRNET**—Non-classified Internet Protocol Router Network

**NISPOM**—National Industrial Security Program Operating Manual

**NIST**—National Institute of Standards and Technology

**NSA**—National Security Agency

**NSS**—National Security Systems

**NSTISSP**—National Security Telecommunications and Information Systems Security Policy

**OPSEC**—Operations Security

**OSI**—Office of Special Investigations

**OS**—Operating System

**OWA**—Outlook Web Access

**P2P**—Peer-to-Peer

**PA**—Privacy Act

**PDA**—Personal Digital Assistant

**PED**—Portable Electronic Device

**PII**—Personally Identifiable Information

**PIN**—Personal Identification Number

**PIV**—Personal Identity Verification

**PIV**—I—Personal Identity Verification-Interoperable

**PKI**—Public Key Infrastructure

**PMO**—Program Management Office

**POA&M**—Plan of Actions and Milestones

**QEB**—Quarterly Enterprise Buy

**RAPIDS**—Real-time Automated Personnel Identification System

**RDS**—Records Disposition Schedule

**RPS**—Registration Practice Statement

**SAAR**—System Authorization Access Request

**SAF**—Secretary of the Air Force

**SCI**—Sensitive Compartmented Information

**SCL**—Smart Card Logon

**SIAO**—Senior Information Assurance Officer

**SIPRNET**—Secret Internet Protocol Router Network

**SIPR REL**—SIPRNET RELEASABLE

**SME PED**—Secure Mobile Environment PED

**SOFA**—Status of Forces Agreement

**SPAN**—Sharing Peripherals across the Network

**SPO**—System Program Office

**SP**—Special Publications

**SSL**—Secure Sockets Layer

**STIG**—Security Technical Implementation Guides

**TA**—Trusted Agent

**TDY**—Temporary Duty

**TMAP**—Telecommunications Monitoring and Assessment Program

**TO**—Technical Order

**TODA**—Technical Order Distribution Account

**USB**—Universal Serial Bus

**U.S.C.**—United States Code

**USCYBERCOM**—United States Cyber Command

**USM**—Unit Security Manager

**US**—United States

**VoIP**—Voice over Internet Protocol

**VoLAC**—Volunteer Logical Access Credential

**VVoIP**—Voice and Video over Internet Protocol

**VPN**—Virtual Private Network

**VPS**—Voice Protection System

**VTC**—Video Teleconferencing

**WIAO**—Wing Information Assurance Office

***Terms***

**Accountability**—The principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (CNSSI 4009)

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

**Air Force—Global Information Grid (AF-GIG)—**Air Force provisioned portion of the DoD GIG. See GIG.

**Alternate/Hardware Logon Token (Alt Token)**—A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions. (DoDI 8520.2)

**Application**—Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs. (DoDD 8500.01)

**Assurance**—Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

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

**Audit Trail**—A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. (CNSSI 4009)

**Authentication**—The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (CNSSI 4009).

**Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST SP 800**—53)

**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. (DoDD 8500.01).

Require a U.S. security clearance commensurate with the level of system access being granted, have a mission need to know, and completed DoD IA training. (DoDI 8500.2)

**Availability**—The property of being accessible and useable upon demand by an authorized entity. (CNSSI 4009)

**Ensuring timely and reliable access to and use of information. (NIST 800**—53)

**Ensuring timely and reliable access to and use of information. (NIST 800**—53)

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

**Certification Practice (CP) Statement**—A statement of the practices that a Certificate Authority, Registration Authority, or other PKI component employs in issuing, revoking, and renewing certificates and providing access to them, in accordance with specific requirements specified in a CP. (DoDI 8520.2)

**Classified Message Incident**—Inadvertent dissemination of classified information through an unclassified E-mail, either within the body of the E-mail or as an attachment. (AFI 33-138)

**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)

**Clearance**—Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material. (CNSSI 4009)

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

**Commercial Mobile Device (CMD)**—A subset of portable electronic devices (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.

**Common Access Card (CAC)**—Standard identification/smart card issued by the Department of Defense that has an embedded integrated chip storing public key infrastructure (PKI) certificates. (CNSSI 4009)

**A Department**—wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. (DoDI 8520.2)

**Computing Environment**—A computer workstation or server (host) and its operating system, peripherals, and applications. (DoDI 8500.2)

**Computer Network Defense**—Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (CNSSI 4009)

**Confidentiality**—The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (CNSSI 4009)

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST SP 800.53)

**Controlled Unclassified Information**—Information, other than classified information, that has been determined to require some type of protection or control. (DoDM 5200.1, Vol 4)

A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special

handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces the term "sensitive but unclassified" (SBU). (CJCSI 6510.01)

**Confidentiality**—The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (CNSSI 4009)

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST SP 800.53)

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

**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)

**Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (NIST SP 800**—53)

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

**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**—The authorized change in the status of information from classified information to unclassified information. (DoDM 5200.01, Vol 1)

**Designated Accrediting Authority (DAA)**—Official with the authority to assume formal responsibility for operating a system at an acceptable level of risk. This term is synonymous with authorizing official and delegated accrediting authority. (CNSSI 4009)

**Enclave**—Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security requirements from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DoDD 8500.01)

**Encryption**—The process of changing plaintext into ciphertext for the purpose of security or privacy. (CNSSI 4009)

**Flash Memory**—A small printed circuit board that holds large amounts of data in memory. Flash memory is used in PEDs and laptops because it is small and holds its data when the computer is turned off. Flash memory is also used in Thumb Drives and Flash Drives. (USCYBERCOM CTO 10-133, *Protection of Classified Information on Department of Defense Secret Internet Protocol Network (SIPRNET)*)

**Memory sticks, thumb drives, and camera memory cards most commonly connected via USB ports on all DoD unclassified, SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) computers using Windows operating systems pose a severe security risk to the GIG. (USCYBERCOM Removable Flash Media device implementation within and between Department of Defense (DoD) networks CTO 10**—084)

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

**Formal Access Approval**—A formalization of the security determination for authorizing access to a specific type of classified or sensitive information, based on specified access requirements, a determination of the individual's security eligibility and a determination that the individual's official duties require the individual be provided access to the information. (CNSSI 4009)

**GIG—**The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. (CNSSI 4009)

**High Impact 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 Infrastructure**—The underlying security framework that lies beyond an enterprise's defined boundary, but supports its IA and IA-enabled products, its security posture and its risk management plan. (CNSSI 4009)

**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)

**Information Assurance**—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-

repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (CNSSI 4009 and DoDD 8500.01)

**Information**—Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. (CNSSI 4009)

**An instance of an information type. (NIST SP 800—53)**

**Data derived from observing phenomena and the instructions required to convert that data into meaningful information. Note: Includes operating system information such as system parameter settings, password files, audit data, etc. (DoD) Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1—02)**

**Information Assurance Manager (IAM)**—Principal advisor on computer security matters to DAA. **Note:** See DoDI 8500.2 IA Manager (IAM). The individual responsible for the information assurance program of a DoD information system or organization. (DoDI 8500.2)

**Information Assurance Officer (IAO)**—Official who manages the COMPUSEC program for an information system assigned to him or her by the IAM, including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. **Note:** DoDI 8500.2 IA Officer (IAO). An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the DoD, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (DoDI 8500.2)

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

**Integrity**—Quality of an information system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Note: In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (DoDD 8500.01)

**Guarding against improper information modification or destruction, and includes ensuring information non**—repudiation and authenticity. (NIST 800-53)

**Information System Owner (ISO)**—See AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP).*

**Information Technology (IT)**—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a

contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (CNSSI 4009)

**IT Position Category**—Applicable to unclassified DoD information systems, 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. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in DoD 5200.2-R (reference (r)). Investigative requirements for each category vary depending on the role and the status of the incumbent. Requirements differ if the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor, or a foreign national. The term "IT Position" is synonymous with the older term Automated Data Processing Position. (DoDI 8500.2)

**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)

**Malicious Logic**—Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (CNSSI 4009)

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

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

**Mobile Computing Device**—IS devices such as personal electronic devices, laptops, and other handheld devices that can access AF managed networks through mobile access capabilities and can store data locally. (COMPUSEC Publication)

**Multilevel Security**—Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (CNSSI 4009)

**Need—to-Know—**determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (DoDM 5200.01, Vol 1)

**A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (DoD 5200.01**—R)

**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)

**Non-Enterprise Activated (NEA) CMD**—Any mobile handheld device that does not store credentials used to login to a DoD network or information system (wired or wireless) or to a PC that is/will be connected to a DoD network, is not configured to process or store email from a DoD electronic messaging system, and is not centrally controlled or monitored from a DoD network.

**Open Storage**—Any storage of classified national security information outside of approved containers. This includes classified information that is resident on information systems media and outside of an approved storage container, regardless of whether or not that media is in use (i.e., unattended operations). (CNSSI 4009)

**Original Classification Authority (OCA)**—An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance). (DoDM 5200.01, Vol 1)

**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)

**Personally Identifiable Information (PII)**—Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (CNSSI 4009)

Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity. Information such as his/her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual. [DoD Memo (DoD Guidance on PII)]

**Personal Identification Number**—A short numeric code used to confirm identity. (CNSSI 4009)

**Personal Identity Verification**—The process of creating and using a government-wide secure and reliable form of identification for Federal employees and contractors, in support of HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors. (CNSSI 4009)

**Portable Electronic Device (PED)**—Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo

images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers. (CNSSI 4009)

**Any non**—stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/Personal Communications Service phones, two-way pagers, electronic mail (E-mail) devices, audio/video recording devices, and hand-held/laptop computers. (DoDD 8100.02)

**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 according to DoD 8570.01-M and be placed in unit manning documented positions that require privileged access. (DoDI 8500.2)

**Protected Workplace**—Workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level as established in DoDI 8500.2, AFJI 31-102, and AFI 31-401 provide additional guidance for physical and information security, respectively. (AFI 33-200)

**Public Domain Software**—Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator. (CNSSI 4009)

**Public Key Infrastructure**—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)

**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)

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

**Safeguards**—Measures and controls that are prescribed to protect classified information. (DoDM 5200.01, Vol 3)

Protective measures and controls prescribed to meet the security requirements of an information system. **Note:** Safeguards include security features and management constraints from the various security disciplines (i.e., administrative, procedural, physical, personnel, communications,

emanations, and computer security) used in concert to provide the requisite level of protection. (COMPUSEC Publication)

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

**Security Label**—Information that represents or designates the value of one or more security relevant attributes (e.g., classification) of a system resource. (CNSSI 4009)

**Security Mechanism**—A device designed to provide one or more security services usually rated in terms of strength of service and assurance of the design. (CNSSI 4009)

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

**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 in accordance with the requirements of the Computer Security Act of 1987 (Public Law 100-235). (CNSSI 4009)

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

**Stand Alone System**—See AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP).*

**Strong Authentication**—The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. (CNSSI 4009)

**Tampering**—An intentional event resulting in modification of a system, its intended behavior, or data. (CNSSI 4009)

**Telework**—A voluntary arrangement where an employee or Service member performs assigned official duties at home or other alternate worksites geographically convenient to the employee or Service member on a regular and recurring or a situational basis (not including while on official travel). (DoDD 8500.01)

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

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

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

**Virtual Private Network (VPN)**—Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line. (CNSSI 4009)

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

**Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. (JP 1**—02)

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

**Zeroize**—To remove or eliminate the key from cryptographic equipment or fill device. (CNSSI 4009)


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu