BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1301

12 FEBRUARY 2020

Cybersecurity

COMPUTER SECURITY (COMPUSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/CNZ

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

Supersedes: AFMAN17-1301, 10 February 2017

Pages: 63

This Air Force Manual implements computer security in support of Air Force Policy Directive 17-1, *Information Dominance Governance and Management*, implements Department of Defense Instruction 8551.01, *Ports, Protocols, and Services Management (PPSM),* and Secretary of the Air Force Chief Information Officer memorandum, *Compliance with Air Force (AF) Cyberspace Publications (17-Series) for the AF Special Access Program (SAP) Enterprise.* This manual applies to all civilian employees and uniformed members of the Regular Air Force, Air Force Reserve, Air National Guard (ANG), and to contractor personnel when required by the terms of their contract. Failure to observe the prohibitions and mandatory provisions of this instruction as stated in **Chapter 7**, **Attachment 2**, **Attachment 3** by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92, Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective state military code. (T-0). Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Direct questions, recommended changes, or conflicts to this publication through command channels using the Air Force Form 847, Recommendation for Change of Publication, to SAF/CN. Send any supplements to this publication to SAF/CN for review, coordination, and approval prior to 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 Air Force Instruction 33-360, Publications and Forms Management, 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 requestors commander for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document is substantially revised. Management Internal Control Toolset/Self-Assessment Checklist requirements, redundant access control, public key infrastructure policies and assessments were removed. Ports, Protocols, Services Management guidance, Bring Your Own Approved Device and Air Force Information Technology User Responsibilities and User agreement were added. All remaining chapters as a result of Department of Defense and Air Force policy directive updates were revised. Review this manual in its entirety.

Chapter 1—INTRODUCTION **5**

1.1. Overview. 5

1.2. Applicability. 5

1.3. Exceptions. 5

Chapter 2—ROLES AND RESPONSIBILITIES **7**

2.1. Deputy Chief, Information Officer (SAF/CN). 7

2.2. Commander, Headquarters Air Combat Command. 7

2.3. Air Force-Appointed Authorizing Officials. 7

2.4. The 16th Air Force. 8

2.5. Air Combat Command Cyberspace Capabilities Center. 8

2.6. Wing Cybersecurity Office (or Designated Equivalent). 9

2.7. Commanding Officers (or Equivalent). 10

2.8. Program Manager. 10

2.9. Information System Security Manager. 10

2.10. Information System Security Officer. 12

2.11. Commanders Support Staff or Similar Administrative Support Function. 12

2.12. Change Sponsor. 12

2.13. Authorized User. 13

Chapter 3—TRAINING AND RESOURCES **14**

3.1. General. 14

3.2. Wing Cybersecurity Office Training Resource. 14
3.3. Air Force Information Assurance Collaborative Environment. 14
3.4. Methods and Procedures Technical Order. 15
3.5. Information Technology Asset Procurement. 15
3.6. Configuration Management. 17
3.7. Ports, Protocol, and Services Identification, Declaration, and Registration. 17
3.8. Defense Information Systems Agency Resources. 18
Chapter 4—END-POINT SECURITY **19**
4.1. Introduction. 19
4.2. General Protection. 19
4.3. Software Security. 20
4.4. Malicious Logic Protection. 21
4.5. Data Spillage/Negligent Discharge of Classified Information. 21
4.6. Telework. 22
4.7. Data Encryption. 22
4.8. Personally-Owned hardware and software. 23
4.9. Wireless Services. 23
4.10. Mobile Computing Devices. 24
4.11. Peripheral Devices. 26
4.12. Removable Media. 28
4.13. Collaborative Computing. 30
4.14. Contractor-Owned Information Systems. 31
4.15. Foreign-Owned Information Systems. 31
4.16. Other Service or Agency Owned Information Systems. 31
Chapter 5—REMANENCE SECURITY **32**
5.1. Introduction. 32
5.2. Sanitization. 33
5.3. Media Reuse. 35
5.4. Disposal. 35

5.5. Mixed Media Devices. 36

Chapter 6—PORTS, PROTOCOLS, AND SERVICES MANAGEMENT **37**

6.1. Introduction. 37

6.2. Ports, Protocol, and Services Management. 38

6.3. Ports, Protocols, and Services Management Registry. 41

6.4. Ports, Protocol, and Services Declaration. 42

6.5. Ports, Protocol, and Services Registration. 43

6.6. Ports, Protocol, and Services Review. 43

6.7. Ports, Protocol, and Services Updates/Change Management. 43

6.8. Decommissioning Strategy. 44

Chapter 7—BRING YOUR OWN APPROVED DEVICE (BYOAD) **45**

7.1. General Guidance. 45

7.2. A SAF/CN approved BYOAD program will: 45

7.3. The BYOAD program is: 45

7.4. All military: 46

7.5. All users must: 46

7.6. Failure by military members to obey the mandatory provisions in this paragraph: 46

7.7. Users must not: 46

7.8. All participants must: 46

7.9. All supervisors: 46

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION **47**

Attachment 2—BRING YOUR OWN APPROVED DEVICE USER AGREEMENT **57**

Attachment 3—Air Force Information Technology User Responsibilities **60**

Chapter 1

INTRODUCTION

1.1. Overview. Computer Security (COMPUSEC) compliance ensures appropriate implementation of measures to protect all Air Force information system resources and information. The focus of this publication is on end-point security and ports, protocols, and services management within the Air Force (AF). The term major command, when used in this publication, includes field operating agencies and direct reporting units. The COMPUSEC objective is to employ countermeasures designed for the protection of confidentiality, integrity, and availability of United States government information processed by Air Force information systems.

1.2. Applicability. This publication applies to all AF information technology used to process, store, display, transmit, or protect AF information, regardless of classification or sensitivity, unless exempted through the risk management framework process. Information System Security Managers, Information System Security Officers, and cybersecurity workforce personnel entrusted with privileged roles are responsible for compliance with this chapter.

1.2.1. More restrictive federal, Department of Defense (DoD), AF guidance take precedence over this publication.

1.2.2. This publication and implementation guidance identified within is not applicable to Intelligence Community information systems to include Sensitive Compartmented Information information systems. Refer to the Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.*

1.3. Exceptions. Document exceptions and deviations to guidance in this publication affecting information systems as part of the applicable authorization package, according to Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT).* Submit modifications, exceptions, and deviations through the system/enclave configuration management process.

1.3.1. Process acquisition waiver requests for network infrastructure and end-point equipment according to Air Force Manual 17-1203, *Information Technology (IT) Asset Management (ITAM).*

1.3.2. Process exceptions to the use of the Department of Defense Information Network according to Department of Defense Instruction 8010.01, *Department of Defense Information Network (DoDIN) Transport*, and Air Force Manual 17-2101, *Long-Haul Communications Management,* for commercial Internet service provider.

1.3.3. Process information system exceptions (non-compliance) to ports, protocols, and services standards according to AFI 17-101 and the DoD ports, Protocols, and Services Management Exception Management Process as implemented by the Air Force.

1.3.3.1. The AF Information Assurance Collaborative Environment (**https://cs2.eis.af.mil/sites/10060/default.aspx**) provides the latest DoD ports, Protocols, And Services Management Exception and Non-Compliant ports, protocols, and services guidance.

1.3.3.2. Find additional guidance in Methods and Procedures Technical Order 00-33A-1100, *AFNet Operational Change Management Process*, and on the MilSuite collaborative environment at **www.milsuite.mil/wiki/Air_Force_Change_Process**.

1.3.4. Process Department of Defense 8570.01-M, *IA Workforce Improvement Program*, certification waivers according to Air Force Manual 17-1303, *Cybersecurity Workforce Improvement Program.*

1.3.5. Unless explicitly restricted in this publication, commanders may waive non-tiered requirements according to AFI 33-360.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Deputy Chief, Information Officer (SAF/CN). Serves as the Air Force voting representative on the DoD Ports, Protocols, and Services Management Configuration Control Board in accordance with Department of Defense Instruction (DoDI) 8551.01 and the DoD Ports, Protocols, and Services Management Configuration Control Board Charter (available at **https://cyber.mil/ppsm/**).

2.2. Commander, Headquarters Air Combat Command. Provides guidance and oversight on the implementation of ports, protocols, and services policy according to this manual and DoDI 8551.01.

2.2.1. Designates one primary and at least two alternate subject matter experts to serve as Air Force representatives to the DoD Ports, Protocols, and Services Management Technical Advisory Group according to DoDI 8551.01 and the DoD Ports, Protocols, and Services Management Configuration Control Board Charter.

2.2.2. Provides ports, protocols, and services registrars responsible for managing access and entering applicable Air Force information systems and associated ports, protocols, and services information into the DoD Ports, Protocols, and Services Management Registry according to DoDI 8551.01.

2.3. Air Force-Appointed Authorizing Officials. Authorizing Officials (as defined by Air Force Instruction 17-101) are responsible for the secure implementation of Ports, Protocols, and Services Management standards for the information system. **(T-0)**. As a minimum:

2.3.1. Restrict ports, protocols, and services used by the information system to only the ports, protocols, and services required for the information system to meet mission needs. **(T-0)**.

2.3.2. Ensure the documentation and approval of ports, protocols, and services as part of the risk management framework process. **(T-0)**.

2.3.2.1. Ensure declared ports, protocols, and services comply with DoD Ports, Protocols, and Services Management standards for implementation. **(T-2)**.

2.3.2.1.1. Review requests for the temporary use of ports, protocols, and services not listed on the DoD Ports, Protocols, and Services Management Category Assurance List according to DoDI 8551.01 and the DoD Ports, Protocols, and Services Management Exception Management Process. **(T-2)**.

2.3.2.1.2. Review exception requests for ports, protocols, and services according to the DoD Ports, Protocols, and Services Management Exception Management Process. **(T-0)**.

2.3.2.1.3. Ensure compliance with DoDI 8551.01 and the hosting environment connection rules for the use of ports, protocols, and services within research, test, and evaluation information networks. **(T-0)**.

2.3.2.2. Include documentation and assessment of vulnerabilities for the declared ports, protocols, and services. **(T-0)**.

2.3.2.3. Verify ports, protocols, and services registration supporting cybersecurity reciprocity of information systems from other DoD components. **(T-0)**.

2.3.2.4. Review exception requests for ports, protocols, and services according to the DoD Ports, Protocols, and Services Management Exception Management Process. **(T-0)**.

2.4. The 16th Air Force. Regulates the use of ports, protocols, and services within the Air Force ensuring routers, firewalls, and intrusion detection devices are configured to only allow approved ports, protocols, and services according to DoDI 8551.01.

2.4.1. Ensure boundary protection devices allow only approved ports, protocols, and services through configuration control processes. **(T-0)**.

2.4.2. Ensure an annual review, at a minimum, of boundary protection device rules for compliance with Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT).* **(T-0)**.

2.4.3. Verify ports, protocols, and services registration prior to connection of information systems to the Air Force Information Network.

2.4.4. Block ports, protocols, and services not implemented according to this policy and DoDI 8551.01 using boundary protection devices and application whitelisting. **(T-2)**. Whitelisting refers to allowing or excepting ports, protocols, and services when required for mission accomplishment.

2.4.5. Assure the interoperability of ports, protocols, and services across the AF Information Network when implemented according to this policy and DoDI 8551.01. **(T-2)**.

2.5. Air Combat Command Cyberspace Capabilities Center. Provides cybersecurity expertise to Headquarters Air Combat Command (ACC) for COMPUSEC and Air Force Ports, Protocols, and Services Management activities and functions.

2.5.1. Provides COMPUSEC and ports, protocols, and services policy and technical subject matter expertise for the Air Force.

2.5.2. Provides field support and program management for COMPUSEC and ports, protocols, and services to SAF/CN, ACC, and all major commands/Field Operating Agencies/Direct Reporting Units. Supports SAF/CN and ACC cybersecurity initiatives. Reviews, evaluates, and interprets Air Force COMPUSEC and ports, protocols, and services doctrine, policy, and procedures. Develops/coordinates recommendations on implementation of the doctrine, policy, and procedures to Headquarters ACC A3/2/6.

2.5.3. Coordinates with the ACC Cybersecurity Division as required and accomplishes other roles and responsibilities as directed by Headquarters ACC.

2.5.4. Maintain AF Cybersecurity Program content on Information Assurance/Cybersecurity collaborative environments for providing immediate access to and awareness of current AF, DoD, and federal policy and guidance, including recent and pending changes to DoD and AF policy.

2.5.5. Provides ports, protocols, and services policy and implementation guidance to information system program managers, Information System Security Managers/Information System Security Officers, Change Sponsors, Change Managers, network/cyberspace operations squadrons, and 16th Air Force.

2.5.5.1. Register and update ports, protocols, and services for information systems authorized by AF authorizing officials.

2.5.5.2. Manages access to the DoD Ports, Protocols, and Services Management Registry database; processes account requests on behalf of the DoD Ports, Protocols, and Services Management for authorized AF users.

2.5.5.3. Ensure the integrity of ports, protocols, and services records for Air Force information systems in the DoD Ports, Protocols, and Services Management Registry consistent with information system authorization conditions according to AFI 17-101.

2.5.5.3.1. Processes exceptions and risk assessments for non-compliant ports, protocols, and services and provides recommendations for change requests affecting Air Force information system communications interfaces to include DoD Demilitarized Zone whitelist requests. The Demilitarized Zone is the perimeter network segment that is logically between internal and external networks.

2.5.5.3.2. Process change requests for network devices, boundary protection devices, and other configuration control assets under the applicability of DoDI 8551.01.

2.5.5.4. Serves as Air Force Representative for DoD Ports, Protocols, and Services Technical Advisory Group; analyzes DoD Ports, Protocols, and Services Management Technical Advisory Group votes and provides recommendations to the AF Ports, Protocols, and Services Management Configuration Control Board voting member.

2.6. Wing Cybersecurity Office (or Designated Equivalent). The Wing Cybersecurity Office addresses all COMPUSEC requirements on the base, including those of tenant units (i.e., Field Operating Agencies, Direct Reporting Units, and other major command units), unless formal agreements exist. Personnel assigned to the Wing Cybersecurity Office will:

2.6.1. Evaluate modifications, exceptions, and deviations to information systems made through the RMF process for accuracy and completeness before forwarding to the appropriate agency. **(T-1)**.

2.6.2. Train designated organization representatives (Commander's Support Staff, Communications Focal Point, Computer Support Technicians, or other assigned cybersecurity workforce personnel) on COMPUSEC administrative processes and procedures and conduct annual or "as needed" refresher training as outlined in **Chapter 3**. **(T-1)**.

2.6.2.1. The "Reducing Additional Duties" Memorandum by the Secretary of the AF empowers commanders at all levels to consolidate Commander's Support Staff-assigned duties as appropriate, and/or discontinue non-critical duties beyond their ability to resource, while adhering to by-law requirements. Administrative tasks normally accomplished by the Commander's Support Staff may be assumed by Communications Focal Point, Computer Support Technicians, or the Wing Cybersecurity Office.

2.6.2.2. For squadrons too small to warrant a Commander's Support Staff, those duties should be accomplished by a group or wing-level Commander's Support Staff or not at all if the Commander deems them non-critical.

2.6.3. Coordinate with the system/enclave Information System Security Officer/Information System Security Manager before deciding whether to sanitize media for reuse or disposal. *see* **Chapter 5**. **(T-0)**.

2.7. Commanding Officers (or Equivalent). Maintains the COMPUSEC program according to this publication, ensuring Air Force information systems operate effectively by protecting and maintaining the confidentiality, integrity, and availability of information system resources and information processed throughout the system's life cycle. Commanders will:

2.7.1. Ensure proper procedures are followed in response to Unauthorized Disclosureof Classified Information (classified information spillage or formerly called classified message incident) affecting AF information systems. *see* **Chapter 4**. **(T-0)**.

2.7.2. Review all approved removable media/ data loss prevention exemptions semi-annually to ensure continuous validation of mission requirements. *see* **Chapter 4**. **(T-0)**.

2.8. Program Manager. Ensures proper implementation of security controls and processes related to ports, protocols, and services to include plan of actions and milestones actions and annual reviews according to AFI 17-101.

2.9. Information System Security Manager. An Information System Security Manager (formerly an Information Assurance Manager) is responsible for the cybersecurity of a program, organization, system, or enclave and provides direction to the Information System Security Officer (formerly a system Information Assurance Officer). Duties of the Information System Security Manager are outlined in DoDI 8500.01, *Cybersecurity,* AFI 17-101, DoDI 8510.01, and Air Force Manual 17-1303.

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

2.9.1.1. Ensure any changes affecting the system's ports, protocols, and services registration (ports, demilitarized zone whitelisting, Internet Protocol addresses, domain name service) comply with the Department of Defense ports, protocols, and services Category Assurance List and the Department of Defense ports, protocols, and services Vulnerability Assessment reports (**https://cyber.mil/ppsm/**). **(T-0)**

2.9.1.2. Assist stakeholders (system administrators, network infrastructure personnel, programmers, etc.) with the identification, declaration, and documentation of ports, protocols, and services requirements. *see* **Chapter 6**. **(T-0)**.

2.9.1.3. Ensure ports, protocols, and services registration is updated prior to submitting change requests through the Enterprise Information Technology Service Management systems (**https://eitsm2.us.af.mil/** or **https://eitsm2.us.af.smil.mil/** on the Secret Internet Protocol Router Network). **(T-2)**.

2.9.1.4. Assist change sponsors with identifying and declaring ports, protocols, and services required for supporting change requests. Provide guidance completing firewall exception requests, Domain Name Service changes, and DoD demilitarized zone whitelist requests, ensuring requested Internet Protocol addresses, fully qualified domain names, and ports, protocols, and services are registered in the DoD Ports, Protocols, and Services Management Registry database. **(T-0)**.

2.9.2. Maintain approval and inventory documentation for authorizing official-authorized personally-owned hardware and software. *see* **Chapter 4**. **(T-2)**.

2.9.3. Process data loss prevention exemptions and removable media whitelist requests. *see* **Chapter 4**. **(T-2)**.

2.9.4. Protect collaborative computing devices used in classified environments. *see* **Chapter 4**. **(T-0)**.

2.9.5. Participate in remanence security risk management processe. *see* **Chapter 5**. **(T-2)**.

2.9.6. Manage the implementation of ports, protocols, and services for appointed information systems. *see* **Chapter 6**. **(T-0)**.

2.9.6.1. Document and assess the vulnerabilities for the use of ports, protocols, and services not listed on the DoD Ports, Protocols, and Services Management Category Assurance List using the DoD Ports, Protocols, and Services Management Exception Management Process (*see* **Chapter 6**) and ports, protocols, and services guidance on the Air Force Information Assurance Collaborative Environment. **(T-0)**.

2.9.6.2. Obtain approval for the use of ports, protocols, and services through the risk management framework process. **(T-0)**.

2.9.6.3. Submit requests for initial ports, protocols, and services registration based upon initial risk management framework authorization. **(T-0)**.

2.9.6.4. Submit updates to ports, protocols, and services registration based upon configuration management plans, security impact processes, and continuous monitoring under risk management framework. **(T-0)**.

2.9.6.5. Maintain ports, protocols, and services registration records for the information system as an artifact within risk management framework. **(T-0)**.

2.9.6.6. Verify the ports, protocols, and services registration and required interfaces for interconnected information systems. **(T-0)**.

2.9.6.7. Submit exception requests for ports, protocols, and services according to the DoD Ports, Protocols, and Services Management Exception Management Process, ports, protocols, and services guidance on the AF Information Assurance Collaborative Environment, and orders from US Cyber Command, as applicable. **(T-0)**.

2.9.6.8. Annually review the system(s) of record in the DoD Ports, Protocols, and Services Management Registry. **(T-0)**.

2.9.6.9. Ensure the removal of records from the DoD Ports, Protocols, and Services Management Registry upon an information system decommission. **(T-0)**.

2.9.6.10. Submit change requests to network devices, boundary protection devices, and other configuration control assets under the applicability of DoDI 8551.01 using the DoD Ports, Protocols, and Services Management Registration Confirmation Details artifact for the associated information system. **(T-0)**.

2.9.7. Ensure users of the information system are briefed on user responsibilities in accordance with Department of Defense 5500.7-R, *Joint Ethics Regulation.* The CyberAwareness Challenge computer-based training course satisfies this requirement for Air Force Network unprivileged users. Follow guidance from the information owner and information system owner if additional topics from DoD 5500.7-R is required.

2.9.8. User agreements described in this AFI (see **attachment 3**, *Air Force Information Technology User Responsibilities*) is used to document agreement. AF Form 4433, *US Air Force Mobile Device User Agreement* may also be used to document user acknowledgement and consent.

2.10. Information System Security Officer. An Information System Security Officer is responsible for the technical implementation of a cybersecurity program. When circumstances warrant, a single individual may fulfill both the Information System Security Manager and the Information System Security Officer roles. DoDI 8500.01, AFI 17-101, and AFMAN17-1303 outline the duties of the Information System Security Officer. Information System Security Officers will:

2.10.1. Provide protection from threats through implementation of technical and physical security mechanisms. *see* **Chapter 4**. **(T-1)**.

2.10.2. Participate in change management activities as assigned by the Information System Security Manager, assisting stakeholders (system administrators, network infrastructure personnel, programmers, etc.) with the declaration and documentation of ports, protocols, and services required for the information system. **(T-3)**

2.10.3. Participate in remanence security risk management processes. *see* **Chapter 5**. **(T-2)**.

2.10.4. Execute procedures that identify and mitigate the residual risk and risk tolerance; see **Chapter 5**. **(T-0)**.

2.11. Commanders Support Staff or Similar Administrative Support Function. Organizations implement and enforce COMPUSEC administrative processes and procedures using the guidance within this instruction.

2.11.1. If the organization did not establish a Commander's Support Staff, tasks may be performed by the organization's Communications Focal Point/Client Support Technician or the Wing Cybersecurity Office.

2.11.2. Personnel performing administrative cybersecurity functions assist the Wing Cybersecurity Office with downward-directed administrative cybersecurity functions (administrative tasking orders, in/out-processing checklists, distribute user training materials, etc.). *see* **Chapter 4**. **(T-2)**.

2.12. Change Sponsor. Changes to an information system require coordination with the system Information System Security Manager, ensuring requested modifications follow the established change management process and do not introduce vulnerability to AF Information Network. The appointed change sponsor is a trained member of the cybersecurity workforce who has the responsibility of documenting the requested change and interfacing with the Information System Security Manager and any change management request tools. See Methods and Procedures Technical Order 00-33A-1100 for guidance.

2.12.1. Reviewing requests, ensuring the proposed change does not violate policies and have been assessed and approved by the system Information System Security Manager.

2.12.2. Ensuring the system being modified has a current authorization decision. **(T-0)**. For guest systems, assist the change initiator with obtaining a copy of the authorization to operate and the authorization to connect documentation.

2.12.2.1. If modification requests affect interfaces (Internet Protocol addresses, ports/protocols/services, etc.) for the system, provide the DoD Ports, Protocols, and Services Management Tracking Identifier.

2.12.2.2. If the system does not have a valid DoD Ports, Protocols, and Services Management Tracking Identifier, then the system and the proposed changes must be registered in the DoD Ports, Protocols, and Services Management Registry database before any change requests are submitted. **(T-0)**. See **Chapter 6**.

2.13. Authorized User. All users of DoD information systems will sign and abide by a standardized User Rules of Behavior Agreement. **(T-2).** Local organizational commanders must restrict access to AF Information Technology for those personnel who fail to sign the agreement. **(T-3).** Report to the Enterprise Service Desk any failures to sign the agreement for revocation of access to enterprise capabilities. **(T-1).** User’s behaviors are monitored to detect potentially unauthorized activity.

Chapter 3

TRAINING AND RESOURCES

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

3.2. Wing Cybersecurity Office Training Resource. The Wing Cybersecurity Office provides direction, oversight, and annual training for designated representatives of the Commander's Support Staff/Communications Focal Point. **(T-2)**. The Wing Cybersecurity Office locally develops the organization cybersecurity training programs and includes the following COMPUSEC-specific items:

3.2.1. Data loss prevention exemptions and accountability according to the latest Maintenance Tasking Order found on the AFNet Compliance Tracker site. **(T-2)**.

3.2.2. Remanence security sanitization and disposition of media/devices according to **Chapter 5**. **(T-2)**.

3.2.3. Current Negligent Dischargeof Classified Information policy and procedures according to the latest Tasking Order found on the AFNet Compliance Tracker site. **(T-1)**.

3.3. Air Force Information Assurance Collaborative Environment. ACC Cyberspace Capabilities Center maintains AF Cybersecurity Program content on Information Assurance/Cybersecurity collaborative environments for providing immediate access to and awareness of current related AF, DoD, and federal policy and guidance, including recent and pending changes to DoD and Air Force policy. The AF Information Assurance Collaborative Environment serves as a cybersecurity support resource for Air Force Wing Cybersecurity Offices and cybersecurity workforce personnel, providing a collaborative one-stop-shop for COMPUSEC, Ports, Protocols, and Services, and TEMPEST related information, frequently asked questions, discussions, templates, and hosts dynamic content for information sharing (**https://cs2.eis.af.mil/sites/10060**). For classified content, the AF Information Assurance Collaborative Environment - Secret Internet Protocol Router Network is available at **http://intelshare.intelink.sgov.gov/sites/af_cybersecurity/SitePages/Home.aspx**.

3.3.1. Access to the unclassified AF Information Assurance Collaborative Environment is limited to users with AF-issued common access card and an AF Network shell account.

3.3.1.1. If the user has an AF-issued common access card but is not an AF Network user, he or she will already have a shell account in the network; an Air Force Network Commander's Support Staff/Communications Focal Point representative uses the "IAO Express" web application to request/enable access. Authorized users open the SharePoint® Access menu in "IAO Express," enables the new shell account, and strips the Personnel Category Code from the user's login identifier. **Note:** IAO Express is the client interface for the Enterprise Service Desk, normally limited to Commander's Support Staff, Communications Focal Point, Computer Support Technicians, and/or Wing Cybersecurity Office personnel (if supporting an organization in an administrative capacity).

3.3.1.2. An AF sponsor with an "IAO Express" account can create an AF Network shell account for non-AF issued common access card holder, enable SharePoint® access, and strip the Personnel Category Code from the user's login identifier.

3.3.2. Access to the AF Information Assurance Collaborative Environment- Secret Internet Protocol Router Network requires Secret Internet Protocol Router Network token and an Intelink Passport account with the user's classified email account associated with the account. **Note:** Intelink is a group of secure intranets that use the Passport authentication service. Instructions for obtaining an account is on the Air Force Information Assurance Collaborative Environment at **https://cs2.eis.af.mil/sites/10060**.

3.4. Methods and Procedures Technical Order. Methods and Procedures Technical Order 00-33B-5006, *Computer Security (COMPUSEC),* provides procedural guidance to the cybersecurity workforce to implement and manage methods and processes pertaining to COMPUSEC policy. Methods and Procedures Technical Order 00-33A-1100 provides change submission and implementation guidance for the AF Network. Obtain Methods and Procedures Technical Orders via the organizational Technical Order Distribution Account on Enhanced Technical Information Management System (**https://www.my.af.mil/etims/ETIMS/index.jsp**).

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

3.5.1. Follow the guidance in AFMAN 17-1203 and the AF Information Technology Commodity Council guidance available on the AF Portal or AFWay (**https://www.afway.af.mil/**) for procurement activities of all information technology hardware, cellular, and peripheral devices (e.g., desktops, laptops, tablets, servers, enterprise activated/non-enterprise activated commercial mobile devices, multifunction devices printers, plotters, scanners, external wired peripheral devices, and wireless peripheral devices).

3.5.2. Comply with the evaluation and validation requirements of Committee on National Security Systems Policy No. 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,* for all information assurance and information assurance-enabled products.

3.5.3. Life Cycle Management. Procure products and adopt risk-based program management according to Air Force Instruction 63-101_20-101, *Integrated Life Cycle Management.*

3.5.4. Unified Capabilities. Modernizing information technology capabilities while aligning with joint solutions remain two of the Air Force's key goals. Department of Defense Instruction 8100.04, *DoD Unified Capabilities (UC),* and Defense Information Systems Agency *Voice and Video Teleconferencing* Security Technical Implementation Guides/Security Requirements Guides provide guidance related to Voice and Video over Internet Protocol, Video Teleconferencing, and Department of Defense interoperability requirements. Find Security Technical Implementation Guides/Security Requirements Guides at **https://cyber.mil/stigs/**.

3.5.4.1. In accordance with DoDI 8100.04, use/obtain Unified Capabilities products certified by the Defense Information Systems Agency Joint Interoperability Test Command. The Joint Interoperability Test Command certifies interoperability and the Unified Capabilities-implementing DoD component authorizing official or the Defense Information Systems Agency Certifying Authority certifies for cybersecurity under risk management framework. Approved products are listed on the Defense Information Systems Agency Unified Capabilities Approved Products List (**https://aplits.disa.mil/processAPList.action**) and should be added to the enclave security authorization package and assessed for cybersecurity through the risk management process.

3.5.4.2. As a general rule, Section 508-compatible Voice over Internet Protocol devices are not listed on the Defense Information Systems Agency Unified Capabilities Approved Products List unless the vendor has included the assistive technology end device as part of the Voice over Internet Protocol system's evaluation package. Organizations may request that the vendor add the product to the current Unified Capabilities Approved Products List certification package and request a determination from the Defense Information Systems Agency Unified Capabilities Certification Office for inclusion in the certification. The Defense Information Systems Agency Unified Capabilities Certification Office (Email: **disa.meade.ns.list.unified-capabilities-certification-office@mail.mil**) has a listing of all product representatives. This review ensures the product operates with the current fielded Voice over Internet Protocol system.

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

3.5.5.1. Use an approved importer or through a World Trade Organization Government Procurement Agreement country. AFWay, Information Technology Commodity Council, and General Services Administration offer foreign-made products secured from an approved importer or World Trade Organization Government Procurement Agreement. **(T-1)**.

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

3.6. Configuration Management. Cybersecurity/Information Assurance reference documents, such as National Institute of Standards and Technology Special Publications, Defense Information Systems Agency Security Technical Implementation Guides, and Security Requirements Guides, National Security Agency Security Configuration Guides, Air Force Technical Orders/Methods and Procedures Technical Orders, Maintenance Tasking Orders, and other specialized publications are used for the security configuration and implementation guidance. Apply these reference documents according to Department of Defense Instruction 85xx.xx series and Air Force Instruction 17-xxx series publications to establish and maintain a minimum baseline security configuration and posture. Document all configuration changes with the enclave/system Information System Security Manager in the information system security authorization package according to Air Force Instruction 17-101 and secure approval for implementation via the system's configuration management process.

3.6.1. The MilSuite collaborative environment (**www.milsuite.mil/wiki/Air_Force_Change_Process**) provides templates and guidance about the responsibilities of the Enterprise Information Technology Service Management Remedy change initiator and change sponsor, as well as the change process procedures.

3.6.2. Ports, Protocols, and Services Category Assurance List, Vulnerability Assessments, Component Local Service Assessment, and exception management guidance is available on the Department of Defense Cyber Exchange at **https://cyber.mil/ppsm/** and **https://cyber.smil/ppsm/** .

3.7. Ports, Protocol, and Services Identification, Declaration, and Registration. Identify the use of internal and external ports, protocols, and services through the assessment and authorization process as prescribed by Department of Defense Instruction 8510.01. The *Air Force Ports, Protocol, and Services Worksheet* template serves as a supporting assessment and authorization artifact for ports, protocols, and services documentation, along with service level agreements for connections/interfaces, functional dataflow diagrams, and topology diagrams. The *Air Force Ports, Protocol, and Services Worksheet* template and guidance are available on the AF Information Assurance Collaborative Environment (**https://cs2.eis.af.mil/sites/10060/Wiki/AF%20PPS.aspx**).

3.7.1. The Information System Security Manager has the primary responsibility for populating the ports, protocols, and services worksheet and securing registration of the system/enclave for initial authorization, reauthorization, and updates/changes through the change management process. System administrators, programmers, and other members of the cybersecurity workforce may be employed as stakeholders for assistance declaring the ports, protocols, and services properly. Use the Category Assurance List, Vulnerability Assessment reports, and Component Local Service Assessments provided by the DoD Cyber Exchange to determine DoD-authorized ports, protocols, and services.

3.7.2. Defense Information Systems Agency Storefront provides online Ports, Protocols, and Services Management training for Ports, Protocols, and Services Management overview, registry, network boundaries, and using the Category Assurance List at **https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/enterprise-connections-ppsm**.

3.7.3. Federal Virtual Training Environment hosts various courses for understanding firewalls, network security devices, protocols, and other information technology-related content at **https://fedvte.usalearning.gov/**

3.8. Defense Information Systems Agency Resources. The Defense Information Systems Agency operates websites providing Security Requirements Guides, Security Technical Implementation Guides, Ports, Protocols, and Services Management, the Department of Defense Unified Capabilities Approved Products List, Cloud Computing Security, online cybersecurity training, links to Fed Virtual Training Environment, and other related guidance. Access the DoD Cyber Exchange site at **https://cyber.mil/on** the Non-classified Internet Protocol Router Network and **https://cyber.smil.mil** on the Secret Internet Protocol Router Network.

Chapter 4

END-POINT SECURITY

4.1. Introduction. End-point security provides the basis for overall protection of AF-controlled information technology assets. Except where specifically called out, Information System Security Managers, Information System Security Officers, and cybersecurity workforce personnel entrusted with privileged roles are responsible for compliance with this chapter. Follow Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* on the use of DoD-provided, enterprise-wide automated tools/solutions to ensure interoperability with Department of Defense and Air Force provided enterprise-wide solutions for remediation of vulnerabilities for endpoint devices.

4.2. General Protection. All authorized users should protect networked and/or standalone information systems against tampering, theft, and loss. Protect information systems from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, AF publications, and organizationally created procedures. See Air Force Instruction 31-101, *Integrated Defense (ID),* for physical access security guidance. End-point security procedures are located in Methods and Procedures Technical Order 00-33B-5006.

4.2.1. Information System Security Manager/Information System Security Officer provides 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 information systems (e.g., Common Access Card removal lock feature, keyboard locks, secure screen savers, and security software). **(T-0)**. This is done according to the Defense Information Systems Agency *Operating Systems* Security Technical Implementation Guides and the system authorization package. **(T-0)**. See National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

4.2.2. Treat devices released to or potentially accessed by unauthorized personnel (outside DoD control) as an untrusted device until information system security policy requirements are re-established and validated by the system Information System Security Manager/Information System Security Officer.

4.2.3. Protect devices at the applicable security classification of the information stored in the device according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F and this publication.

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

4.2.5. Control viewing of United States-Only information systems and equipment by foreign nationals/local nationals according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F; see the Defense Information Systems Agency *Traditional Security Checklist* (available at **https://cyber.mil/stigs/**).

4.2.6. Ensure transmission of sensitive information is encrypted using National Institute of Standards and Technology-certified cryptography at a minimum according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F.

4.2.7. Ensure the transmission of classified information is encrypted using National Security Agency-approved cryptography according to Air Force Manual 17-1302-O, *Communications Security (COMSEC) Operations,* and Chairman of the Joint Chiefs of Staff Instruction 6510.01F. **(T-0)**.

4.2.8. In areas where classified information is processed, ensure information systems meet TEMPEST requirements according to Air Force Systems Security Instruction 7700, *Emission Security*).

4.2.9. Appropriately mark and label information technology devices according to the highest level of classification processed or displayed on the device according to Department of Defense Manual 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*, and Department of Defense 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* if appropriate.

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

4.2.9.1.1. Display devices located within the same classification environment or mixed environments attached to approved keyboard, video, monitor device are not required to be physically labeled if the desktop backgrounds are configured through the information system to identify the classification level.

4.2.9.1.2. Mark and label all keyboard, video, monitor switches (regardless of classification environment) to identify the switch position and the associated classification of the connected systems according to the Defense Information Systems Agency *Keyboard Video and Mouse Switch* Security Technical Implementation Guide.

4.2.9.2. Mark and label all mobile computing devices with the potential to be located/used in mixed environments with the highest classification level of the information approved to be processed by the device. If necessary due to mission or operating environment requirements, coordinate with wing Cybersecurity Office and wing Information Protection Office in developing alternate marking and labeling methods.

4.2.10. Contact the organizational security assistant or Wing security manager in the Wing Information Protection office for devices involved in data spillage or security incidents according to Air Force Instruction 16-1404, *Air Force Information Security Program.* For remanence security guidance, see **Chapter 5**.

4.2.11. Follow the guidance in current 624 Operations Center Tasking Order for universal serial bus violations, unauthorized software installation, improper use of elevated privileged/administrative accounts, and other similar activities that increase the risk to the Air Force Information Network.

4.3. Software Security. The Information System Security Manager ensures all software is included in the information system security authorization package according to AFI 17-101 and Chairman of the Joint Chiefs of Staff Instruction 6510.01F. Comply with AFMAN 17-1203 for software accountability guidance.

4.3.1. Freeware, public domain software, shareware originating from questionable or unknown sources (e.g., world wide websites), trial or demonstration software, and Peer-to-Peer file sharing software are highly susceptible to malicious logic and can only be used after a risk assessment (see AFI 17-101) has been conducted. **(T-2)**.

4.3.2. Follow DoD and AF procedures for application whitelisting to include the processes for submitting exceptions to allow the execution of authorized software.

4.4. Malicious Logic Protection. Protect information systems from malicious logic (e.g., virus, worm, Trojan horse) attacks by applying a mix of human and technological preventative measures according to the Defense Information Systems Agency Security Technical Implementation Guides and Security Requirements Guides, and Chairman of the Joint Chiefs of Staff Instruction 6510.01F.

4.4.1. Implement antivirus software with current signature files according to DoD Antivirus Security Guidance (**https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/anti-virusanti-spyware-solutions**). The Information System Security Manager documents a process for updating devices that are not able to receive automatic updates (i.e., standalone systems, laptops issued for temporary duty, etc.) in the system authorization package according to National Institute of Standards and Technology Special Publication 800-53.

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

4.4.3. Configure virus scanning frequency and real-time protection according to the applicable Defense Information Systems Agency Security Technical Implementation Guide; document scanning frequency in the system authorization package according to National Institute of Standards and Technology Special Publication 800-53. **(T-0)**.

4.4.4. Using additional antivirus software may be approved through the security authorization process; any additional antivirus software should be used in conjunction with DoD-approved antivirus software (**https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/anti-virusanti-spyware-solutions**).

4.4.5. Implement malicious logic protection for Mobile Code Technologies according to the Defense Information Systems Agency *Application Security and Development* Security Technical Implementation Guide. Mobile code categories are listed in the *Application Security and Development Overview* document.

4.5. Data Spillage/Negligent Discharge of Classified Information. Data spillage/Negligent Discharge of Classified Information incidents occur when a higher classification level of data is placed on a lower classification level system/device (including commercial mobile devices). When classified information is processed or maintained on an unclassified information system, the individual discovering the incident initiates security incident procedures according to Department of Defense Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, Air Force Instruction 16-1404, and the current 624 Operations Center Tasking Order. If an individual in the organization discovers the event, initial notification should be to the organization's security assistant or Wing Information Protection office. Organizations may use locally developed emergency response aids to inform users of the correct procedures. Contact the AF Network Mission Assurance Center for guidance.

4.6. Telework. Criteria for determining eligibility for civilian/military telework are identified in DoDI1035.01_AFI 36-816, *Civilian Telework Program.* For detailed information on telework methods reference National Institute of Standards and Technology Special Publication 800-46, *Guide to Enterprise Telework and Remote Access Security*. (**http://csrc.nist.gov/publications/PubsSPs.html**).

4.7. Data Encryption. Encrypt sensitive information (e.g., Controlled Unclassified Information, For Official Use Only, Personally Identifiable Information, Health Insurance Portability and Accountability Act, Privacy Act, and Proprietary).**(T-1)**.

4.7.1. Validate information assurance/information assurance-enabled products providing encryption according to DoDI 8500.01. **(T-1).**

4.7.2. Verify that information assurance/information assurance-enabled products have been certified and listed on the Common Criteria Evaluation and Validation Scheme website or the Common Criteria Portal website. **(T-1)**.

4.7.2.1. The National Institute of Standards and Technology and the National Security Agency developed the Common Criteria program as part of the National Information Assurance Partnership, establishing an organizational and technical framework to evaluate the trustworthiness of information technology products and protection profiles. Cryptographic modules and algorithms are evaluated according to the National Institute of Standards and Technology Cryptographic Algorithm Validation Program and of Cryptographic Module Validation Program. The Cryptographic Algorithm Validation Program provides validation testing of Federal Information Processing Standards-approved and National Institute of Standards and Technology-recommended cryptographic algorithms and their individual components, such as compliance with Federal Information Processing Standards 180-4, *Secure Hash Standard (SHS)*, for implementing Secure Hash Algorithm 256, Federal Information Processing Standards 197, *Advanced Encryption Standard (AES)*, and other Federal Information Processing Standards. Cryptographic algorithm validation is a prerequisite of the Cryptographic Module Validation Program. The Cryptographic Module Validation Program validates cryptographic modules to Federal Information Processing Standards.

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

4.7.4. Data at rest and data in transit protection requires Federal Information Processing Standards validated cryptographic modules for securing Controlled Unclassified Information and Personally Identifiable Information and National Security Agency-approved cryptographic systems for classified data according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F.

4.7.4.1. Use Common Criteria-validated products or National Institute of Standards and Technology-evaluated cryptographic modules that provide the minimum Federal Information Processing Standards validated cryptographic module implementing Secure Hash Algorithm-256 for data at rest for non-Windows platform operating systems. **(T-0)**.

4.7.5. Classified Data At Rest. Protect classified national security information at rest according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F using National Security Agency-approved cryptographic and key management systems offering appropriate protection levels and approved for protecting classified data at rest. Air Combat Command Cyberspace Capabilities Center Cryptographic Modernization Office (**CYSS.CYS.AFCOMSEC-CryptoMod@us.af.mil**) is the designated lead for all Air Force classified data at rest encryption use cases.

4.8. Personally-Owned hardware and software. Personally-owned hardware and software used to process DoD information requires mission justification and authorizing official approval. **(T-0)**. The Information System Security Officer/Information System Security Manager maintains approval and inventory documentation between the user and government organization in information system security authorization package.

4.8.1. The introduction of personally-owned hardware and/or software to an information system may be a violation of the information system user agreement and subject to repercussions outlined in the information system authorization package, resulting in the loss of user access.

4.8.2. Do not introduce personally-owned/developed software or connect personally-owned media or peripheral devices with volatile or non-volatile memory (including, but not limited to, music/video compact disc/digital versatile disc, commercial portable media players, and universal serial bus drives) to Air Force information systems and/or government furnished equipment. **(T-2)**.

4.8.3. Prior to their introduction into classified processing areas, consult Air Force Instruction 16-1404 and the latest Certified TEMPEST Technical Authority guidance for approving personally-owned devices. This applies to fitness monitors, wearable smart technology devices, tablets, e-readers, recording devices (audio, video, etc.), Bluetooth®, and other wireless devices.

4.9. Wireless Services. Comply with DoDI 8500.01 and Department of Defense Directive 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),* for wireless services (radio frequency and infrared) integrated with or connected to AF information systems.

4.9.1. Implement wireless peripheral devices, to include keyboard, mouse, Common Access Card reader, pointer devices, according to requirements outlined in the Defense Information Systems Agency Security Technical Implementation Guides and the National Information Assurance Partnership Mobile Device Fundamentals Protection Profile, DoD Annex (**https://www.niap-ccevs.org/pp/**). Acquire wireless peripheral devices according to AFMAN 17-1203.

4.9.2. Follow applicable TEMPEST guidance for all wireless capabilities. Wireless capabilities in areas where classified information is discussed or processed require written approval from the AF Enterprise Authorizing Official (or applicable authorizing official if classified wireless capabilities fall entirely within their boundary and do not touch the AF Information Network) and the Air Force Certified TEMPEST Technical Authority according to Department of Defense Directive 8100.02.

4.9.3. Configure wireless network solutions according to the Defense Information Systems Agency Security Technical Implementation Guides and Chairman of the Joint Chiefs of Staff Instruction 6510.01F; document wireless configurations in the information system security authorization package for AF Enterprise Authorizing Official (or applicable authorizing official if the wireless capabilities fall entirely within their boundary and do not touch the Air Force Information Network) approval according to Department of Defense Directive 8100.02. **(T-1)**.

4.9.4. Configure all unclassified wireless peripheral devices (e.g., keyboards, mice, pointers/forwarders, hand-held terminals, etc.) with Federal Information Processing Standards validated encryption modules according to Chairman of the Joint Chiefs of Staff Instruction 6510F. **(T-0)**. Products that advertise compliance with Federal Information Processing Standards must provide the certification number.

4.9.5. Implement end-to-end data encryption for unclassified information over an assured channel, and certify under the National Institute of Standards and Technology Cryptographic Module Validation Program to meet requirements of Federal Information Processing Standards according to DoDD 8100.02. **(T-0)**. Secure classified information within National Security Agency-approved encryption solutions according to Chairman of the Joint Chiefs of Staff Instruction 6510F. **(T-0)**.

4.9.5.1. Individual exceptions to unclassified wireless encryption may be granted on a case-by-case basis according to DoDD 8100.02 and this publication after a risk assessment and approval by the AF Enterprise Authorizing Official (or applicable authorizing official if the wireless capabilities fall entirely within their boundary and do not touch the AF Information Network) **(T-2)**; see boundary specific appointment letters on the DoD Risk Management Framework Knowledge Service at **https://rmfks.osd.mil/rmf**. Navigate to the Collaboration tab and select Air Force from the Component Workspaces option.

4.9.5.2. Infrared wireless mice/pointers and keyboards require authorizing official approval and inclusion in the system authorization package; for use in classified processing areas, implement applicable TEMPEST countermeasures. **(T-2)**.

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

4.10.1. Configure and handle all devices according to applicable Defense Information Systems Agency Mobility Security Technical Implementation Guides, Mobile Policy Security Requirements Guide, any updated/newly released mobile operating system Security Technical Implementation Guide (e.g., Apple, Android, Windows Phone, etc.), and Chairman of the Joint Chiefs of Staff Instruction 6510.01F. **(T-0)**. Obtain authorizing official approval for all non-compliant Security Technical Implementation Guide configuration standards.

4.10.2. Prior to issuance of each commercial mobile devices, the Commander's Support Staff/communications Focal Point/Client Support Technician verifies user compliance with the Defense Information Systems Agency DoD Mobile Devices (or its replacement) training (**https://cyber.mil** under Training Catalog, Cybersecurity Awareness) or similar training module in the Advanced Distributed Learning Service, when available. Commercial mobile devices users complete annual training according to Defense Information Systems Agency Mobility Security Technical Implementation Guides/Security Requirements Guides.

4.10.3. Government-owned mobile devices connecting to Department of Defense systems require proper approval and documentation in the information system security authorization package. **(T-0)**.

4.10.4. Authorizing official authorization is required prior to the introduction of government or personal cellular/personal communications system and/or radio frequency, infrared wireless devices, and other devices such as cell phones and tablets, and devices that have photographic or audio recording capabilities into areas (e.g., rooms, offices) where classified information is processed and discussed. Exceptions to this policy requires adherence to TEMPEST requirements according to DoDD 8100.02, coordination through the AF Certified TEMPEST Technical Authority according to Air Force Instruction 16-1404 and National Institute of Standards and Technology Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* and written approval by the AF Enterprise Authorizing Official (or applicable authorizing official if the wireless capabilities fall entirely within his/her boundary and do not touch the AF Information Network). **(T-1)**.

4.10.4.1. Approval by the authorizing official is based upon the Information System Security Manager risk assessment and Air Force Certified TEMPEST Technical Authority recommendation. Supplemental devices designed to interconnect wirelessly between telehealth/assistive devices to a Voice over Internet Protocol handset, commercial mobile devices, or similar communications device require a TEMPEST countermeasure review, Air Force Certified TEMPEST Technical Authority recommendation, and authorizing official approval prior to use in a classified area.

4.10.5. Use only approved secure (classified) mobile computing (e.g., DoD Mobility Classified Capability-Secret) wireless devices for storing, processing, and transmitting classified information. **(T-0)**

4.10.5.1. Encrypt classified data stored on secure (classified) mobile computing wireless devices using National Security Agency-approved cryptographic and key management systems according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F. **(T-0)**.

4.10.6. Users should immediately report any lost or stolen device to the issuing organization and system Information System Security Officer/Information System Security Manager, see AFMAN 17-1203. Consult applicable user guide or AF Mobile site for guidance on remotely wiping lost or stolen commercial mobile devices and suspending the corresponding service plan.

4.10.7. Maintain positive control over all hardware peripheral devices (i.e., portable printer devices, removable media [authorized universal serial bus storage devices, optical media, external hard drives], external compact disc/ digital versatile disc drives, power accessories, etc.) that may accompany the mobile computing device. **(T-1)**

4.10.8. Non-Enterprise Activated Commercial Mobile Devices/cellular telephones acquired through the AF Information Technology Commodity Council are approved for use within the Air Force for any non-sensitive unclassified Department of Defense tasks. Non-enterprise activated commercial mobile devices/cellular telephones are only authorized to process/store publicly available information (e.g., conducting training, monitoring meteorological data, viewing flight maps, and recruiting activities). **(T-1)**.

4.10.8.1. Non-enterprise activated commercial mobile devices /cellular telephone devices may not store and/or process classified information, Controlled Unclassified Information, Personally Identifiable Information, Health Insurance Portability and Accountability Act information, and other sensitive information. **(T-1)**

4.10.8.2. Configure government-owned non-enterprise activated commercial mobile devices/cellular telephones according to the current Defense Information Systems Agency Security Technical Implementation Guide/Security Requirements Guide.

4.10.8.3. Track and manage all government-owned non-enterprise activated commercial mobile devices/cellular telephones according to AFI 17-210, *Radio Management,* and AFMAN 17-1203.

4.10.9. Consult the current 624 Operations Center Tasking Order for handling, reporting, and sanitizing commercial mobile devices data spillage events involving classified, Controlled Unclassified Information, Personally Identifiable Information, Privacy Act, and Health Insurance Portability and Accountability Act data on government issued and personally-owned devices. **(T-1)**.

4.11. Peripheral Devices. A peripheral is any external device that provides input and output for a computing device. Input devices are mouse, scanners, smart boards, pointers, touch screens, and keyboards). Output devices receive data from the computing device providing a display or printed product (e.g., monitors/televisions, projectors, printers, plotters, and multifunction devices).

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

4.11.2. Web cam usage on any information system requires documentation in the system authorization package. Use of web cams in classified environments requires physical security and/or TEMPEST countermeasures.

4.11.3. Assistive Technology (Section 508 devices). Assistive technology refers to a service or device that is used to increase, maintain, or improve functional capabilities of individuals with disabilities. Assistive technology can refer to a commercially acquired item, piece of equipment, software, or system. Assistive technology solutions may include compact keyboards, breath-controlled keyboard/mouse devices, alternative pointing devices, assistive listening devices (wired and wireless), video phones, screen reader software, screen magnification software, voice recognition software, etc. Contact the AF Enterprise Authorizing Official's office for authorization guidance. For more information, see Air Force Instruction 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508.*

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

4.11.3.1.1. DoDI 6025.22 requires all Computer/Electronic Accommodations Program activities meet applicable acquisition, confidentiality, privacy, security, and disclosure requirements according to Department of Defense Instruction 5400.11, *DoD Privacy and Civil Liberties Programs*, and Department of Defense 5400.11-R, *Department of Defense Privacy Program.* For more information, see the *Handbook for Providing Assistive Technology to Wounded Service Members* (**http://www.cap.mil**).

4.11.3.1.2. The enclave or system Information System Security Manager may submit any non-information assurance/information assurance-enabled software to Air Force Network Integration Center for certification. Once certified (or if there is no software to certify), the Information System Security Manager conducts a risk assessment to determine the overall impact to the enclave/system security posture and adds it to the information system/enclave security authorization package, providing a risk recommendation to the authorizing official.

4.11.4. Configure multifunction devices and networked printers/scanners/plotters according to the Defense Information Systems Agency *Multifunction Device and Network Printers* Security Technical Implementation Guide. **(T-0)** Only use Common Criteria-certified multifunction devices according to Committee on National Security Systems Policy No. 11 and DoDI 8500.01. **(T-0)** Products available on the AFWay website have been Common Criteria/National Information Assurance Partnership evaluated and certified.

4.11.4.1. Acquire all equipment through AF Information Technology Commodity Council enterprise buying programs such as AFWay. The acquisition of any device outside of the AFWay process requires major command approval. If the device is not listed on AFWay, obtain a waiver through AFWay to purchase the desired device. If the product provides information assurance or is information assurance-enabled (encryption, authentication, etc.), it must be Common Criteria/National Information Assurance Partnership certified. Products obtained through the waiver process require a risk assessment and must receive authorizing official approval prior to connection to the AF Information Network; connection authorization is not automatic. Guidance for obtaining a waiver may be pursued through the "Request for Quote" process at the AFWay website (**https://www.afway.af.mil/**). See AFMAN 17-1203 for more information.

4.11.4.2. Document, configure, and implement devices utilizing information assurance - enabled functions (e.g., scan to email/network drive) in the information system security authorization package for approval by the authorizing official.

4.11.5. At the device end-of-life, sanitize and dispose of peripheral devices containing non-volatile memory according to **Chapter 5**.

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

4.12.1. Scan approved formatted removable media devices for viruses before use.

4.12.2. Configure and manage all approved removable media devices according to all applicable Defense Information Systems Agency Security Technical Implementation Guides and Chairman of the Joint Chiefs of Staff Instruction 6510.01F.

4.12.3. Protect removable media containing Personally Identifiable Information, Health Insurance Portability and Accountability Act, Privacy Act, and Controlled Unclassified Information taken outside organizational networks according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F DoDM 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)* and DoDI 6025.18, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs.* **(T-0)**.

4.12.3.1. The Information System Security Officer/Information System Security Manager informs users about data at rest requirements, ensuring stored information on removable media complies with the requirements outlined in **paragraph 4.7**.

4.12.3.2. Report any lost or stolen removable media containing Controlled Unclassified Information, Health Insurance Portability and Accountability Act, Privacy Act, or Personally Identifiable Information to the privacy monitor immediately, according to Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties Program.* **(T-0)**.

4.12.4. 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 DoDM 5200.01, Volume 2.

4.12.4.1. Ensure proper classification, marking, storing, transportation, and destruction of removable flash media devices according to DoDM 5200.01, Volumes 2 and 3, and remanence security guidelines; see **Chapter 5**.

4.12.4.2. Unless an AF Enterprise Authorizing Official-approved write protection mechanism or write protection process is used, unclassified media introduced into a classified information system becomes classified according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F and the AF Enterprise Authorizing Official Memorandum, *Guidance for Manual Data Transfers Across Security Domains.* **(T-2)**. For data transfers across security domains, contact the AF Cross Domain Solutions Office (**afnic.csni@us.af.mil**) for guidance.

4.12.4.3. Disable "write" mechanisms for all forms of removable media on Secret Internet Protocol Router Network information systems according to United States Cyber Command Communications Tasking Order 10-133, *Protection of Classified Information on Department of Defense (DoD) Secret Internet Protocols Router Network (SIPRNet).* **(T-0)**.

4.12.4.4. Organizations with a mission requirement to write to removable media submits requests for a waiver to the authorizing official 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://cs2.eis.af.mil/sites/13954/**).

4.12.4.5. Wing Cybersecurity Offices verify that organization commanders review all approved data loss prevention exemptions according to the current data loss prevention exemption Maintenance Tasking Order to validate the mission requirement. If no longer required due to a change in mission, role, or assignment, the system Information System Security Manager submits a request to remove the device/user account from the exemption. For exemptions on devices connected to the Secret Internet Protocol Router Network, disable write capabilities on the universal serial bus ports/compact disc drives of the exempted devices.

4.12.4.6. Users are required to notify the approving exemption authority if the exemption requirement is no longer needed.

4.12.4.7. System Information System Security Managers validate the approved exemptions against the whitelist according to the current data loss prevention exemption Maintenance Tasking Order, verifying the removed devices/user accounts. For systems unable to implement automated verification, manually verify the removal of write capabilities on each device. See the latest Maintenance Tasking Order found on the AFNet Compliance Tracker site concerning data loss prevention exemptions for procedures and templates.

4.12.5. Removable media devices disguised to look like common items (e.g., pens, bracelets, erasers) in areas where DoD information systems are present are not authorized. **(T-0)**.

4.12.6. The Information System Security Officer/Information System Security Manager ensures the proper handling of storage devices that contain classified information according to **Chapter 5**.

4.12.7. Whitelist all approved external storage media (to include memory sticks, thumb drives, camera memory cards, digital cameras, smart phones, media players, external storage devices, flash media, and similar technologies) prior to connection via universal serial bus ports to Air Force Information Network systems. Submit the whitelist waiver according to the current Tasking Order and/or Maintenance Tasking Order found on the AFNet Compliance Tracker site.

4.12.8. Removable flash media use is allowed once organizations have identified procedures, put appropriate technologies in place, and have received approval from the authorizing official or alternate approving authority (e.g., O-6 Group Commander or equivalent) according to the *AF DAA Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133 Memorandum.* Only universal serial bus removable flash media (thumb drives) devices that have Federal Information Processing Standards certification under the National Institute of Standards and Technology Cryptographic Module Validation Program for encryption are authorized for purchase and use on the Air Force Information Network. View the vendor information at **http://csrc.nist.gov/groups/STM/cmvp/index.html** under the "Module Validation Lists" hyperlink.

4.12.9. Account for all removable media devices in the Defense Property Accountability System or the most current, mandated Air Force information technology inventory control system according to AFMAN 17-1203.

4.12.9.1. Report the loss of any removable media device that is whitelisted immediately to the Wing Cybersecurity Office for whitelist removal actions according to the current Maintenance Tasking Order. Treat recovered removable media devices as untrusted.

4.12.9.2. Report the loss of any removable media device containing Personally Identifiable Information to the organizational privacy monitor immediately.

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

4.13.1. The system Information System Security Manager ensures the use of cameras/microphones in unclassified and/or classified environments are documented and approved in the information system security authorization package. Protect collaborative computing devices used in classified environments, see **paragraph 4.2**.

4.13.2. Configure webcams, attached microphones, and control the projection of information viewable by webcams according to the Defense Information Systems Agency *Voice and Video over IP (VVoIP)* and *Video Services Policy* Security Technical Implementation Guides. Collaborative computing mechanisms that provide video and/or audio conference capabilities need to provide a clear visible indication that video and/or audio mechanisms are operating to alert personnel when recording or transmitting according to the Defense Information Systems Agency VVoIP Overview Security Technical Implementation Guide.

4.14. Contractor-Owned Information Systems. Contractor-owned hardware and software used to process DoD information on behalf of the DoD requires mission justification and authorizing official approval, as required by DoDI 8510.01. Contractor-owned information systems implement security requirements for connection to the Air Force Information Network according to Chairman of the Joint Chiefs of Staff Instruction 6211.02D, *Defense Information Systems Network (DISN) Responsibilities,* and AFI 16-1404. Interconnection with the AF Information Network is accomplished according to Department of Defense Instruction 8510.01 and configured using the appropriate Defense Information Systems Agency Security Technical Implementation Guides.

4.14.1. Externally-owned information system and platform information technology systems that are dedicated to DoD processing and are effectively under DoD configuration control require authorization according to DoDI 8510.01.

4.14.2. Off-base, non-DoD owned facilities require Defense Security Service approval to process classified DoD information according to Department of Defense 5220.22-M.

4.14.3. On base contractors within Air Force-controlled facilities comply with the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and Department of Defense Instruction 4161.02, *Accountability and Management of Government Contract Property,* as required by contract.

4.14.4. Information System Security Officers/Information System Security Managers/organizations maintain a listing of all contractor-owned or operated information system equipment within Air Force facilities.

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

4.15. Foreign-Owned Information Systems. Do not use foreign-owned or -operated (e.g., joint/coalition) information system hardware or software to process United States sensitive but unclassified, controlled unclassified information, or classified information, unless required by international treaties or security agreements. See Chairman of the Joint Chiefs of Staff Instruction 6211.02D, Chairman of the Joint Chiefs of Staff Instruction 6510.01F, and Department of Defense Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* for more information.

4.16. Other Service or Agency Owned Information Systems. Other service/agency-owned and operated information systems (i.e., Army, Navy, State Department, etc.) should meet all security requirements for connection to the Air Force Information Network as defined in AFI 17-101 and Department of Defense Instruction 8510.01. Follow reciprocity and reuse procedures according to DoDI 8510.01 and AFI 17-101. Ports, protocols, and services registration for other Service or Agency owned information systems will follow component specific ports, protocols, and services guidance. Contact the applicable DoD Component Ports, Protocols, and Services Management Technical Advisory Group representative for assistance registering ports, protocols, and services for other Service or Agency information systems; find the DoD Component Ports, Protocols, and Services Management Configuration Control Board or Technical Advisory Group Representative contact list at **https://cyber.mil/ppsm/**.

Chapter 5

REMANENCE SECURITY

5.1. Introduction. Remanence is the residual information remaining on storage media. Remanence security actions are taken to protect the confidentiality of information on information systems (to include infrastructure devices such as routers and switches). See the information system security authorization package for system specific incident response and remanence security procedures. Exercise risk management procedures according to DoDI 8500.01, Chairman of the Joint Chiefs of Staff Instruction 6510.01F, and National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization.*

5.1.1. AF policy is to safeguard classified and sensitive information, no matter what the media. Safeguarding classified and sensitive information in computer memory and media is particularly important during routine maintenance, product end of life, and reuse. Information System Owners, privileged users, Information System Security Managers, Information System Security Officers, wing Cybersecurity Offices, operations personnel, and other responsible people should know the risk factors before sanitizing information systems media and releasing them from the controlled environment. Except where specifically called out, Information System Security Managers, Information System Security Officers, Information System Owners, Wing Cybersecurity Offices, and cybersecurity workforce personnel entrusted with privileged roles are responsible for compliance with this chapter. To protect against compromise, allow only authorized and properly cleared persons with a need to know access to media containing classified and sensitive information.

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

5.1.2.1. When assessing the risk of releasing information systems media from DoD control, the Information System Security Officer should develop procedures that identify the residual risk and risk tolerance (the acceptable level of risk as determined by the Information System Owner). Follow the guidance in National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Risk Assessments.*

5.1.2.2. The Information System Security Officer, assisted by the Wing Cybersecurity Office, assesses the risks in consultation with the Wing Information Protection office before deciding whether to sanitize for reuse or disposal. See the current 624 Operations Center Tasking Order for guidance about reuse after Negligent Dischargeof Classified Information sanitization actions. The Air Force Network Mission Assurance Center established the risk identification, management, and mitigation measures identified for Negligent Dischargeof Classified Information events.

5.1.2.3. The Information System Owner and the information owners consider the full range of vulnerabilities and security implications to include the actual loss if an unauthorized entity extracts the residual information, the threat directed against this information, the threat of recovery, and the potential for damage.

5.1.3. Risk Management. Utilizing remanence security within an organization is a risk management process that involves the information owner, Information System Owner, Information System Security Manager, Information System Security Officer, Wing Information Protection, and security assistant/manager to make a determination of potential impact prior to sanitizing media or devices for reuse or disposal. The decision is based on a complete risk analysis that involves the identification of organizational mission, mission impacts, threats, and possible compromise to the information system or information. A thorough cost benefit analysis coupled with mission priorities provides the framework for this decision.

5.1.3.1. Once the risk analysis has been completed, the Information System Security Manager/Information System Security Officer documents the mitigations and any residual risk in the information system security authorization package and plan of actions and milestones.

5.1.3.2. As the monetary cost of media decreases, the cost of sanitizing media may become impractical and destruction may become more cost effective. Costs to be considered in the sanitization and destruction decision include purchase price of sanitization software and degaussing/destruction equipment, periodic recertification of equipment, cost of outsourcing, and time required for verification, documentation, and tracking of sanitized media.

5.2. Sanitization. Remanence security actions to sanitize medium (smartphone, Flash, random access memory and read only memory, optical disks, solid state drives, magnetic disks, hard disk drives, etc.) is dependent upon classification of data contained within the device.

5.2.1. Sanitization of unclassified devices follows National Institute of Standards and Technology Special Publication 800-88. The term "sanitization" is defined in SP 800-88 as a process to render access to target data on the media infeasible for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize media. Clearing for reuse within the same classification does not require a witness. The sanitization/degaussing/destruction of Controlled Unclassified Information solid state and/or magnetic media does require a witness/validator.

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

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

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

5.2.2. Sanitization of classified devices follows the National Security Agency/Central Security Service Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, and involves the destruction of the media and/or data via degaussing, incineration, disintegration, shredding, embossing/knurling, chopping/pulverizing/wet pulping (paper), grinding, strip shredding/cutting, or power removal (dynamic random-access memory, static random-access memory, and volatile field programmable gate array). Only products listed on the National Security Agency Evaluated Products List or received approval from the National Security Agency may be used to destroy classified information (to include media and devices) per National Security Agency/Central Security Service Policy Manual 9-12. Contact the National Security Agency/Central Security Service System and Network Analysis Center at (410) 854-6358 or via email at **SNAC@radium.ncsc.mil**, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, information technology equipment, electronic components, and other similar or associated materials. The sanitization/degaussing/destruction of classified solid state and/or magnetic media requires a witness/validator.

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

5.2.2.2. Embossing/Knurling (compact discs/digital versatile discs) – One or two rotating knurled shafts press down on the surface, elongating the focal point and making all information unreadable and inaccessible.

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

5.2.2.4. Disintegration (hard disk drives/diskettes/compact discs/digital versatile discs /solid state drives) – Reduces the storage media into small fragments of a specific size, depending upon the type, using a knife mill.

5.2.2.5. Incinerate (hard disk drives/diskettes/compact discs/digital versatile discs/Blu-Ray Disks/solid state drives) – Destruction using high heat/temperatures to reduce the media into ash.

5.2.2.6. Shredding (diskettes/compact discs/digital versatile discs) – Physical shredding of media into small strips using two interlocking patterned drums that rotate in opposing directions.

5.2.2.7. Power Removal (dynamic random access memory/static random access memory/volatile field programmable gate array) – Clearing of volatile memory by removing power source for a specific duration.

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

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

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

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

5.3.1. Clear unclassified media before reuse; purge media containing sensitive data (does not include Controlled Unclassified Information or Personally Identifiable Information) prior to reuse. Reference National Institute of Standards and Technology Special Publication 800-88. **(T-0)**

5.3.2. Ensure removal of data from information system, its storage devices, and other peripheral devices (e.g., copiers or printers) with storage capacity in such a way that the data may not be reconstructed (e.g., degauss, smelt, incinerate, disintegrate, or pulverize), rendering stored information unrecoverable. **(T-0)**

5.3.3. Clear classified media before reuse and reuse only in a classified environment according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F. Classified storage media may not be sanitized and declassified for reuse in an unclassified environment. **(T-0)** See Enclosure C of Chairman of the Joint Chiefs of Staff Instruction 6510.01F.

5.3.4. For spillage events, see the current 624 Operations Center Tasking Order.

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

5.4.1. Purge or destroy all unclassified information system storage media before leaving the control of the DoD, according to National Institute of Standards and Technology Special Publication 800-88 and **paragraph 5.2.1**. **(T-1)**.

5.4.1.1. Dispose of unclassified electronic media according to National Institute of Standards and Technology Special Publication 800-88. Dispose of unclassified computing systems and hard drives according to DoDM 5200.01, Volume 3, Enclosure 7. When no longer needed, unclassified computer systems and hard drives may be disposed of outside the Department of Defense. In some circumstances, the equipment may be provided to non-government entities for reutilization. For devices involved in spillage events, see current 624 Operations Center Tasking Order. **(T-1)**

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

5.4.1.3. Track and dispose of unclassified information system storage media previously contaminated with classified data as classified media according to Chairman of the Joint Chiefs of Staff Instruction 6510.01F. **(T-0)**. Reference DoDM 5200.01, Volume 3, Enclosure 3 for disposal and destruction of classified hard drives, electronic media, processing equipment components, etc. Destroy and declassify according to National Security Agency/Central Security Service Policy Manual 9-12. Document destruction using guidance according to Methods and Procedures Technical Order 00-33B-5006.

5.4.2. Destroy all classified information system storage media unless being used in an information system environment at the same or higher classification level. Reuse of classified information system storage media in unclassified environments is not authorized. **(T-0)**. At the end of life, destroy according to Chairman of the Joint Chiefs of Staff Instruction 6510.01 and the sanitization/declassification procedures of National Security Agency/Central Security Service Policy Manual 9-12, **paragraph 5.2.2**. **(T-0)**. Follow DoDM 4160.21 Volumes 2 and 4 for demanufacture (precious metals recovery) procedures. For installations without the means to sanitize or verify sanitization, National Security Agency does accept and destroy some classified media. Follow the guidance on the National Security Agency Classified Materiel Conversion for packaging, documenting, and shipping devices at **https://www.nsa.gov/cmc/**. Direct questions to the Classified Materiel Conversion Customer Service Office at 301-688-6672 or via email at **cmc@nsa.gov**.

5.5. Mixed Media Devices. Determine the sanitization requirements of mixed media devices, following National Security Agency/Central Security Service Policy Manual 9-12 and National Institute of Standards and Technology Special Publication 800-88. Sanitization is complete by appropriately sanitizing all the media contained within the device. Hardware such as computers, routers, switches, multifunction devices, etc., may contain multiple types of media and the sanitization methods are based on the type of media and the classification of the operational environment. Most network architecture devices have solid-state storage devices such as random access memory, read only memory, field programmable gate array, smart cards, and flash memory. Dynamic random access memory, static random access memory, ferroelectric random access memory, magnetic random access memory, erasable programmable read only memory, ultra-violet erasable programmable read only memory, and electrically erasable programmable read only memory have specific sanitization requirements.

Chapter 6

PORTS, PROTOCOLS, AND SERVICES MANAGEMENT

6.1. Introduction. Ports, protocols, and services requires association to the applicable hardware or software, discovered during the ports, protocols, and services declaration activity during the risk management framework process. Ports, protocols, and services used throughout Air Force Information Network require compliance with DoDI 8550.01. **(T-0)**. The declaration of ports, protocols, and services is based upon official business or authorizing official-determined requirements. Ports, protocols, and services registration in the Department of Defense Ports, Protocols, and Services Management Registry database only occurs as a result of a new authorization or through a configuration change to the information system with a security impact analysis generated by the Information System Security Manager. Except where specifically called out, Information System Security Managers, Information System Security Officers, and cybersecurity workforce personnel entrusted with privileged roles supporting an information system are responsible for compliance with this chapter.

6.1.1. New system authorization: The authorizing official approves the use of ports, protocols, and services via the assessment and authorization process and once the new system has been authorized, the Information System Security Manager requests registration.

6.1.2. Reauthorization of an existing system: The Information System Security Manager reviews the ports, protocols, and services, documents any changes, and requests an update to the existing ports, protocols, and services registration upon reauthorization.

6.1.2.1. Review boundary protection device rules annually, at a minimum, for compliance with Chairman of the Joint Chiefs of Staff Instruction 6510.01F, Department of Defense Instruction 8551.01, and this manual. **(T-1)**

6.1.2.2. Monitor implementation of ports, protocols, and services based upon continuous monitoring guidance, in accordance with National Institute of Standards and Technology Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems, and Organizations, Step 6, Monitor Security Controls.

6.1.3. Modifications to the ports, protocols, and services registration: The requestor contacts the system Information System Security Manager to initiate a change request to modify the ports, protocols, and services for a registered system. The Information System Security Manager reviews the request, conducts a risk assessment, generates the security impact assessment, and submits a request to update the existing ports, protocols, and services registration, if applicable.

6.1.3.1. If the Information System Security Manager determines the risk exceeds the risk tolerance for the system, the request should be denied until sufficient mitigations are implemented as outlined in AFI 17-101. The Information System Security Manager follows DoDI 8510.01, Enclosure 6, for monitoring security controls if the residual risk adversely affects the security posture of the system.

6.1.3.2. Consult the DoD Ports, Protocols, and Services Category Assurance List and Ports, Protocols, and Services Vulnerability Assessment reports for a list of conditions, mitigations, and approved boundary crossings.

6.1.3.3. Air Force Network modifications: All changes should be coordinated through the base change sponsor and the system/enclave Information System Security Manager; follow Methods and Procedures Technical Order 00-33A-1100.

6.1.4. Regulate the use of ports, protocols, and services through interconnection agreements, access control mechanisms, and boundary protection devices according to DoDI 8551.01 and this manual.

6.1.4.1. Applications and platform information technology systems should document and maintain a list of all existing and potential hosting enclaves, see AFI 17-101.

6.1.4.2. Hosting enclaves should document and maintain a list of all hosted information systems and interconnected information systems covered by a separate assessment and authorization package, see AFI 17-101. The list must include the DoD Ports, Protocols, and Services Management Tracking Identifier for each information system. **(T-1)**

6.2. Ports, Protocol, and Services Management. Ports, protocols, and services for information systems connecting to, operating on, or traversing across the Air Force Information Network follow policies to catalog, regulate, and control their use based upon vulnerabilities and risk. Approval for the use of ports, protocols, and services by an information system only occurs through the risk management framework process according to AFI 17-101. The Information System Security Manager has the responsibility of ensuring ports, protocols, and services used by the information system are compliant with DoD Ports, Protocols, and Services Management policies. **(T-0)**.

6.2.1. Limit the use of ports, protocols, and services to only the communications interfaces required for information systems to meet mission needs, also known as the "least function" security principle. **(T-0)**.

6.2.2. Identify and document the ports, protocols, and services within the authorization boundary of the information system according to the following conditions:

6.2.2.1. Associate the ports, protocols, and services with hardware and software listed in the component inventory for the information system.

6.2.2.2. Attribute the ports, protocols, and services to the "listening" services or servers to comply with the security concept of "least function" for hardware and software.

6.2.2.3. Ensure configuration management and control for the hardware and software, to include the ports, protocols, and services, exists under the applicable Information System Owner.

6.2.2.4. Determine the actual or expected users and their communications interfaces to the hardware and/or software. For example, users located on the Internet, from a different DoD component, or within the same hosting enclave.

6.2.2.5. Verify all ports, protocols, and services within the authorization boundary of the information system do not duplicate the ports, protocols, and services under the control and cognizance of another DoD information system.

6.2.2.6. Use the AF- Ports, Protocol, and Services Worksheet to document these communications interfaces. This document will serve as an artifact for risk management framework and documents compliance with DoD Ports, Protocols, and Services Management standards.

6.2.2.7. Ports, protocols, and services documentation must be consistent with functional dataflow diagrams and network topology diagrams. **(T-1)**

6.2.3. Implement Ports, Protocols, and Services Management standards for software and hardware using the DoD Ports, Protocols, and Services Management Category Assurance List and applicable DoD Ports, Protocols, and Services Vulnerability Assessment reports available from the DoD Cyber Exchange (**https://cyber.mil/ppsm/**). **(T-0)**.

6.2.3.1. The use of ports, protocols, and services not listed on the DoD Ports, Protocols, and Services Management Category Assurance List (e.g., no applicable DoD Ports, Protocols, and Services Vulnerability Assessment Report) is not authorized and does not comply with DoD policy require risk assessment. Follow the applicable DoD process for component local srvice assessment or risk assessment and ports, protocols, and services guidance on the Air Force Information Assurance Collaborative Environment for documenting and assessing the vulnerabilities for the use of these unknown and/or unevaluated ports, protocols, and services.

6.2.3.2. Changes to published DoD Ports, Protocols, and Services Vulnerability Assessment reports require supporting documentation, review, and approval. **(T-0)**. Follow the guidance on the Air Force Information Assurance Collaborative Environment for ports, protocols, and services to submit requests for changes to the Vulnerability Assessment reports issued by DoD.

6.2.4. After approval from an authorizing official, the ports, protocols, and services registration actions formally declare the use of the ports, protocols, and services for the associated information system within DoD-level databases available to all Department of Defense Components.

6.2.4.1. Registration enables the regulation and control of ports, protocols, and services across networks, connection authorizations, hosting enclave coordination, and other activities to achieve interoperability and availability.

6.2.4.2. Members of the assessment and authorization team request registration of the information system's ports, protocols, and services using the online AF Ports, Protocol, and Services Registration Request Tool available at: **https://cs2.eis.af.mil/sites/10060**.

6.2.4.3. Upon successful registration, each information system receives a unique, 9 character alpha-numeric DoD Ports, Protocols, and Services Management Tracking Identifier. Ports, Protocols, and Services Management Tracking Identifiers with a "U" prefix indicate operation on the unclassified network environment while the "C" prefix indicates operation on the classified network environment.

6.2.4.4. Updates to the existing ports, protocols, and services registration for an information system should follow the configuration management plans, security impact assessment processes, and continuous monitoring activities for the information system under risk management framework, see AFI 17-101.

6.2.4.5. Registration confirmation notices and the ports, protocols, and services details generated from the DoD Ports, Protocols, and Services Management Registry become official artifacts for the system of record. File these artifacts with the risk management framework authorization package to support connection authorizations, change requests for network devices/assets, and cybersecurity reciprocity.

6.2.5. Identify and document the ports, protocols, and services associated with interconnected information systems according to the following conditions:

6.2.5.1. Applies to ports, protocols, and services with any Internet Protocol-based communications interface to the "listening" service or service of another application or information system with its own DoD authorization package. These ports, protocols, and services do not exist within the authorization boundary of the subject information system since the hardware and software falls under the configuration control of a different Information System Owner.

6.2.5.2. Verify all ports, protocols, and services within the authorization boundary of the information system do not duplicate the ports, protocols, and services under the control and cognizance of interconnected information system. Only one information system may declare the "listening" service or service of hardware and/or software based upon configuration control policies.

6.2.5.3. Use an interconnection artifact, service level agreement, or other similar document to identify these communications interfaces. The document will serve as an artifact for risk management framework.

6.2.6. Exceptions to DoD Ports, Protocols, and Services Management standards follow the DoD Ports, Protocols, and Services Management Exception Management Process and guidance on the Air Force Information Assurance Collaborative Environment for ports, protocols, and services.

6.2.6.1. Exceptions apply to the use of a ports, protocols, and services already evaluated by DoD Ports, Protocols, and Services Management with deviations to the standards specified in the applicable DoD Ports, Protocols, and Services Vulnerability Assessment report. This process provides the Information System Owner with the ability to use non-standard ports, protocols, and services based upon an operational need. The DoD Ports, Protocols, and Services Management Technical Advisory Group and Configuration Control Board will review the non-standard use to determine whether the deviation and implemented measures mitigate shared risk to the DoD Information Network.

6.2.6.2. After completion of the necessary risk management framework actions for non-compliance and guidance for the documentation requirements from the AF Information Assurance Collaborative Environment, submission of the exception request will use the online "Non-Compliant PPS Submission Request Tool" on the Air Force Information Assurance Collaborative Environment at **https://cs2.eis.af.mil/sites/10060**.

6.2.6.3. Any exceptions under the purview of United States Cyber Command must first follow the DoD Ports, Protocols, and Services Management Exception Management Process (**(https://cyber.mil/ppsm/).(T-0)**

6.2.7. For time-sensitive operational interoperability in support of operations with limited duration, Information System Owners and authorizing officials may request temporary use of ports, protocols, and services not listed on the DoD Ports, Protocols, and Services Management Category Assurance List according to DoDI 8551.01. Follow the Department of Defense Ports, Protocols, and Services Management Exception Management Process and ports, protocols, and services guidance on the Air Force Information Assurance Collaborative Environment.

6.2.8. Records in the DoD Ports, Protocols, and Services Management Registry require review on an annual basis, at a minimum, to validate system information, point of contacts, and all communications interfaces remain accurate and up-to-date. Failure to keep records current will result in removal from the DoD Ports, Protocols, and Services Management Registry, which will impact connection authorizations. **(T-2)**.

6.2.9. Boundary protection devices employ a "deny by default, permit by exception" policy for both ingress and egress rules or policy objects. **(T-0)**.

6.2.9.1. Changes to rules require supporting evidence of authorizing official approval for the information system, connection authorization, and DoD ports, protocols, and services registration. **(T-0)**.

6.2.9.2. Changes to rules under the applicability of DoDI 8551.01 require the DoD Ports, Protocol, and Services Registration Confirmation Details artifact as supporting evidence for the change.

6.2.9.3. Changes to other network devices that enable Internet Protocol-based communications follow the same requirements for boundary protection devices. This includes, but is not limited to, application whitelisting, Domain Name Service records, firewalls, next-generation firewalls, application-layer gateways, web application firewalls, web content filtering, and web proxy services.

6.2.10. For cloud services ports, protocols, and services, follow the guidance in the Defense Information Systems Agency *Cloud Computing* Security Requirements Guide and procedures on the Air Force Information Assurance Collaborative Environment at **https://cs2.eis.af.mil/sites/10060/Wiki/AF%20PPS.aspx**.

6.2.11. Information systems with a public component, a public-facing presence, or Internet-facing applications require review and approval through the DoD demilitarized zone whitelist process. Follow guidance on the AF Information Assurance Collaborative Environment at **https://cs2.eis.af.mil/sites/10060/Wiki/AF%20PPS.aspx**.

6.3. Ports, Protocols, and Services Management Registry. The DoD Ports, Protocols, and Services Management operates two databases, one for unclassified systems (Ports, Protocols, and Services Management-U) and another for classified systems (Ports, Protocols, and Services Management-C). Upon registration, each information system/enclave registered in the DoD Ports, Protocols, and Services Management Registry receives a DoD Ports, Protocols, and Services Management Tracking Identifier as proof of registration, retained throughout the lifecycle of the system. Records in the DoD Ports, Protocols, and Services Management Registry remain valid according to the information system/enclave authorization termination date; system/enclave registration records are removed from the DoD Ports, Protocols, and Services Management Registry upon the authorization termination date expiration.

6.4. Ports, Protocol, and Services Declaration. Implement ports, protocols, and services according to DoD ports, protocols, and services standards using the applicable Defense Information Systems Agency Security Technical Implementation Guides, DoD Ports, Protocols, and Services Category Assurance List, Department of Defense Ports, Protocols, and Services Vulnerability Assessment reports, and AF Component Local Service Assessments. **(T-0)**. Additional requirements may be provided via Joint Forces Headquarters-Department of Defense Information Network, United States Cyber Command, and 16th Air Force tasking orders or other directives as situations arise.

6.4.1. Comply with Chairman of the Joint Chiefs of Staff Instruction 6211.02D for "tunneling" across the Air Force Information Network and ensure declaration of the ports, protocols, and services, to include ports, protocols, and services within the tunnel. **(T-0)**.

6.4.1.1. Comply with the Authorization to Connect process according to AFI 17-101. **(T-2)**.

6.4.1.2. Ports, protocols, and services documentation and associated ports, protocols, and services registration must declare the ports, protocols, and services required to establish the tunnel and also the ports, protocols, and services used within the tunnel pursuant to the purposes and applicability of DoDI8551.01.

6.4.2. Ports, protocols, and services associated with information system connections by mission partners require compliance with Department of Defense Instruction 5530.03, *International Agreements*, and Authority to Connect guidance in Air Force Instruction 17-101.

6.4.2.1. Mission partner information systems require a DoD Ports, Protocols, and Services Management Tracking Identifier for operation on, operation through (e.g., encrypted tunnels), and/or connection to the AF Information Network. For more information about mission partner environments, see Department of Defense Instruction 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD.*

6.4.2.2. Develop, maintain, and adhere to interconnection agreements or similar documents for the use of ports, protocols, and services within an enclave or hosting environment. **(T-2)**.

6.4.3. Declare ports, protocols, and services on the Air Force Ports, Protocol, and Services Worksheet, available on the AF Information Assurance Collaborative Environment (**https://cs2.eis.af.mil/sites/10060/Wiki/AF%20PPS.aspx**) and the Air Force Information Assurance Collaborative Environment-Secret Internet Protocol Router Network (**http://intelshare.intelink.sgov.gov/sites/af_cybersecurity/SitePages/Home.aspx**).

6.4.3.1. Document all Internet Protocol-based communication interfaces utilizing a definable port and data service associated with hardware, software, and applications within the authorization boundary as listed in the applicable authorization documentation for the information system.

6.4.3.2. Do not document any Internet Protocol-based communications interfaces associated with hardware, software, and applications owned and declared by another authorized information system.

6.5. Ports, Protocol, and Services Registration. Registration of ports, protocols, and services occurs after authorization of the system. Once registered, a Ports, Protocols, and Services Management Tracking Identifier is assigned to the information system and will substantiate system interconnections such as network changes, boundary modifications, and other connection authorizations throughout the information system lifecycle.

6.5.1. Ports, protocols, and services registration is required for the following:

6.5.1.1. Any computer/device inside a Non-classified Internet Protocol Router Network/Secret Internet Protocol Router Network enclave with any communication interface external to the enclave or authorization boundary.

6.5.1.2. Any computer/device inside a Non-classified Internet Protocol Router Network/Secret Internet Protocol Router Network enclave with only internal (i.e., Local Only) communications interfaces to another computer/device inside that same enclave with no external communications interfaces outside the enclave or authorization boundary.

6.5.1.3. A computer/device inside an encrypted tunnel to communicate across Non-classified Internet Protocol Router Network to any other network to include the Internet.

6.5.1.4. Any computer/device on the Internet connection to another computer inside a Non-classified Internet Protocol Router Network enclave or demilitarized zone to include computers on the Internet connecting to any computer on the .mil domain.

6.5.2. Ports, protocol, and services registration is not required for the following:

6.5.2.1. A computer/device on the Internet with another communications interface to another computer on the Internet (i.e., not on the DoD Information Network).

6.5.2.2. A computer/device that does not interface with the Non-classified Internet Protocol Router Network/Secret Internet Protocol Router Network.

6.5.2.3. A computer/device that does not reside on an Internet Protocol-based network.

6.6. Ports, Protocol, and Services Review. Review mandated changes to ports, protocols, and services security measures (i.e., United States Cyber Command orders, DoD Ports, Protocols, and Services Management Configuration Control Board results) and determine impact, compliance, and remediation actions for the applicable ports, protocols, and services used by an information system. Document the findings as a security impact assessment, indicating the amount of residual risk any change either adds or removes.

6.7. Ports, Protocol, and Services Updates/Change Management. Ports, protocols, and services updates require a current authorization for the system and a DoD Ports, Protocols, and Services Management Tracking Identifier that indicates the system has been registered. Coordinate all updates, modifications, additions, and deletions through the system Information System Security Manager. See the Air Force Change Process guidance on MilSuite at **www.milsuite.mil/wiki/Air_Force_Change_Process** and the Air Force Ports, Protocol, and Services Wiki at **https://cs2.eis.af.mil/sites/10060/Wiki/AF%20PPS.aspx**.

6.8. Decommissioning Strategy. Include ports, protocols, and services used by information systems within the system decommissioning strategy according to DoDI 8510.01. A decommissioning strategy must also include the removal of the information system from the DoD Ports, Protocols, and Services Management Registry, coordination with the Cybersecurity Service Provider and/or hosting environment to remove associated boundary protection device rules, and the termination of ports, protocols, and services exceptions for the system. **(T-1).**

Chapter 7

BRING YOUR OWN APPROVED DEVICE (BYOAD)

7.1. General Guidance. Individuals shall not place Department of Defense Controlled Unclassified Information, except for an individual's own or minor child's Privacy Act protected information, on a personal device except as part of a SAF/CN approved Bring Your Own Approved Device (BYOAD) program. (T-1).

7.2. A SAF/CN approved BYOAD program will: Have a Mobile Device Management (MDM) technical solution that provides a Managed Mobile Service (MMS), enabling the user access to Unclassified DOD Information while ensuring separation between the personal and Unclassified DOD information and when removed will not impact personal information. (T-1). The MMS mandates personally-owned mobile devices that access DOD information and/or DOD Information System (IS):

7.2.1. Must be managed and configured in accordance with appropriate Security Technical Implementation Guides (STIGs) and Security Recommendation Guides (SRGs), monitored by an MMS, and validated against appropriate National Information Assurance Partnership (NIAP) Protection Profile(s). (T-1).

7.2.2. Must have an Authority to Operate (ATO) by an Authorizing Official (AO). (T-1).

7.2.3. Must ensure automated monitoring, compliance, and validation mechanisms are implemented by the MMS to ensure security/configuration settings of BYOAD do not deviate from the AO approved configuration baseline and security controls (e.g., device configurations, approved OS versions, detection of rooted/jailbroken devices). (T-1).

7.2.4. Must validate and support malware detection, over-the-air (OTA) electronic software distribution of applications, remote data-wipe capabilities, remote device configuration management, plus asset/property management capabilities that protect against key and data compromise. (T-1).

7.2.5. Must monitor for violations of defined rules such as violations of application whitelists and blacklists, Subscriber Identification Module (SIM) changes, and roaming state changes. (T-1).

7.2.6. Must validate the device is running the latest approved Operating System (OS)/patch. (T-1). Operations should send notices of approved patch levels, and the device must be updated to the latest OS/patch level within 30 calendar days of the notification. (T-1).

7.2.7. Must block access from any personal device that has failed to be patched/updated and any devices that are considered end of life and no longer receiving patches. (T-1).

7.2.8. Must have a process for approving devices and individuals to participate in the program. (T-1).

7.2.9. Must have a capability to provide a semi-annual report on the number of users to SAF/CN. (T-1).

7.3. The BYOAD program is: Voluntary and is strictly for the convenience of the employee. It shall not be a cost saving measure nor is it a substitute for providing a government mobile device. (T-0).

7.4. All military: Including Air National Guard and Air Force Reserve and civilian employees who choose to participate in the program must agree to and comply with the BYOAD User Agreement in **Attachment 2**. (T-1).

7.5. All users must: Follow the approved process for obtaining and deleting the MMS as outlined by SAF/CN including completing the user training. (T-1).

7.6. Failure by military members to obey the mandatory provisions in this paragraph: Is a violation of Article 92 of the UCMJ. All users who participate in this program shall only use a device for the BYOAD program that:

7.6.1. Is NIAP validated, managed, and operated. Only NIAP devices may be used to participate in the BYOAD program to ensure separation and protection of DOD information. (T-1). A list of NIAP devices can be found at **https://www.niap-ccevs.org/**.

7.6.2. Was purchased in the United States or through a U.S. Military Exchange. (T-1).

7.6.3. Has device-unlock passcode, Personal Identification Number (PIN), or biometric access control enabled on the device. (T-1).

7.7. Users must not: Use any personal wireless capability in areas where classified information is discussed or processed, including communications security (COMSEC) areas, without prior written approval from the AO. (T-1).

7.8. All participants must: Have the approval of their supervisors to utilize the BYOAD program. (T-1).

7.9. All supervisors: Who have employees who participate in the BYOAD program must comply with:

7.9.1. All time and attendance policies. (T-0).

7.9.2. Fair Labor Standards Act. (T-0).

7.9.3. Equal Employment Opportunity. (T-0).

7.9.4. Title 5 United States Code. (T-0).

7.9.5. All supervisors of a BYOAD user must complete supervisor BYOAD training. (T-1).

WILLIAM E. MARION II, SES, USAF
Deputy Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Air Force Policy Directive 17-1, *Information Dominance Governance and Management,* April 12, 2016

Department of Defense Instruction 8551.01, *Ports, Protocols, and Services Management (PPSM);* Incorporating Change 1, July 27, 2017

SAF/CIO Memorandum, *Compliance with Air Force (AF) Cyberspace Publications (17-Series) for the AF Special Access Program (SAP) Enterprise*, September 20, 2018

Air Force Instruction 33-360, *Publications and Forms Management,* December 1, 2015

Air Force Manual 33-363, *Management of Records,* March 1, 2008

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

Air Force Instruction 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* January 23, 2020

Air Force Information Assurance Collaborative Environment: **https://cs2.eis.af.mil/sites/10060/**

Air Force Change Process collaborative environment: **www.milsuite.mil/wiki/Air_Force_Change_Process**

Computer Security Act of 1987 (*Public Law 100-235*) , January 8, 1988

Department of Defense Ports, Protocols, and Services Management Category Assurance List

Air Force Manual 17-1203, *Information Technology (IT) Asset Management (ITAM),* May 18, 2018

AFNet Compliance Tracker: **https://act.af.smil.mil**

Department of Defense Instruction 8010.01, *Department of Defense Information Network (DoDIN) Transport,* September 10, 2018

Air Force Manual 17-2101, *Long-Haul Communications Management,* May 22, 2018

Methods and Procedures Technical Order 00-33A-1100, *AFNet Operational Change Management Process,* May 21, 2018

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

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

Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* March 12, 2014; Incorporating Change 2, July 28, 2017

SAF Chief of Staff Memorandum, *Reducing Additional Duties,* August 18, 2016

Department of Defense Instruction 8500.01, *Cybersecurity*, March 14, 2014

Department of Defense 5500.7-R, *Joint Ethics Regulation*, August 1993; Incorporating Change 7, November 17, 2011

Methods and Procedures Technical Order 00-33B-5006, *Computer Security (COMPUSEC),* December 15, 2017

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

Air Force Instruction 63-101_20-101, *Integrated Life Cycle Management,* May 9, 2017

Department of Defense Instruction 8100.04, *DoD Unified Capabilities (UC),* December 9, 2010

Title 10, United States Code Section 2533a, *Requirement to Buy Certain Articles from American Sources; Exceptions,* January 2, 2013

Federal Acquisition Regulation Subpart 25.1, *Buy American – Supplies,* 25.103 *Exceptions,* current edition

Defense Federal Acquisition Regulation Supplement Part 225 – *Foreign Acquisition,* Subpart 225.1, *Buy American – Supplies,* 225.103 *Exceptions,* current edition

Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* February 9, 2011

Air Force Instruction 31-101, *Integrated Defense (ID)*, July 5, 2017

National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013; Includes updates as of January 22, 2015

Air Force Manual 17-1302-O, *Communications Security (COMSEC) Operations,* (U//FOUO), February 2, 2017

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

Department of Defense Antivirus Security Guidance: **https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/anti-virusanti-spyware-solutions**

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

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

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

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

DoDI1035.01_AFI 36-816, *Civilian Telework Program,* October 29, 2018

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security,* June 2009

National Institute of Standards and Technology Federal Information Processing Standards 180-4, *Secure Hash Standard (SHS),* August 2015

National Institute of Standards and Technology Federal Information Processing Standards 197, *Advanced Encryption Standard (AES),* November 2001

United States Cyber Command Communications Tasking Order 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD),* January 8, 2008

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

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

National Information Assurance Partnership, *Mobile Device Fundamentals* Protection Profile, June 10, 2016

National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* December 2014; Includes updates as of December 18, 2014

Air Force Instruction 17-210, *Radio Management,* May 26, 2016

Air Force Instruction 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508,* 3 July 2019

Department of Defense Instruction 6025.22, *Assistive Technology (AT) for Wounded, Ill, and Injured Service Members,* January 30, 2015

Department of Defense Instruction 5400.11, *DoD Privacy and Civil Liberties Programs,* January 29, 2019

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

Department of Defense Manual 5200.01, Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI),* February 24, 2012

Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties Program,* January 12, 2015; Incorporating Change 1, November 17, 2016

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

Air Force Space Command/A6 Memorandum, *Guidance for Manual Data Transfers Across Security Domains,* May 23, 2018

United States Cyber Command Communications Tasking Order 10-133, *Protection of Classified Information on Department of Defense (DoD) Secret Internet Protocols Router Network (SIPRNet),* November 27, 2010

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

Chairman of the Joint Chiefs of Staff Instruction 6211.02D, *Defense Information System Network (DISN): Policy and Responsibilities,* January 24, 2012

Department of Defense Instruction 4161.02*, Accountability and Management of Government Contract Property*, April 27, 2012

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

National Institute of Standards and Technology Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization,* December, 2014

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

National Security Agency/Central Security Service Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, December 15, 2014

Department of Defense Manual 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification,* February 24, 2012

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

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

National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems, and Organizations,* September 30, 2011

Department of Defense Instruction 5530.03, *International Agreements*, December 4, 2019

Department of Defense Instruction 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD*

Defense Information Systems Agency *Voice and Video Teleconferencing* Security Technical Implementation Guides/Security Requirements Guides (cyber.mil)

Defense Information Systems Agency *Keyboard Video and Mouse Switch* Security Technical Implementation Guide (cyber.mil)

Defense Information Systems Agency *Application Security and Development* Security Technical Implementation Guide (cyber.mil)

Defense Information Systems Agency *Multifunction Device and Network Printers* Security Technical Implementation Guide (cyber.mil)

Defense Information Systems Agency *Voice and Video over IP (VVoIP)* and *Video Services Policy* Security Technical Implementation Guide (cyber.mil)

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls, and Firewall Policy*, September 28, 2009

Committee on National Security Systems Instruction No. 4009*, Committee on National Security Systems (CNSS) Glossary,* April 6, 2015

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 20, 2007

Department of Defense Directive 8140.01, *Cyberspace Workforce Management*, August 11, 2015

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

DoDI 6025.18, *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs,* March 13, 2019

Prescribed Forms

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

Adopted Forms

Department of Defense Form 2987, *CAP Accommodation Request*

Air Force Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFMAN—Air Force Manual

AFNET—Air Force Network

AFSEN—Air Force Special Enclave Networks

BYOAD—Bring Your Own Approved Device

ANG—Air National Guard

COMPUSEC—Computer Security

COMSEC—Communications Security

CSE—Cyber Security Event

CSS—Central Security Service

CTO—Communications Tasking Order

DAA—Designated Accrediting Authority

GIG—Global Information Grid

IA—Information Assurance

ID—Integrated Defense

IT—Information Technology

MMS—Managed Mobile Service

NISPOM—National Industrial Security Program Operating Manual

NSA—National Security Agency

OPR—Office of Primary Responsibility

OTA—Over-The-Air

RMF—Risk Management Framework

SAF/CN—Secretary of the Air Force, Deputy Chief Information Officer

SAP—Special Access Program

SHS—Secure Hash Standard

SIPRNet—Secret Internet Protocol Router Network

UC—Unified Capabilities

UCMJ—Uniform Code of Military Justice

UDCI—Unauthorized Disclosureof Classified Information

USCYBERCOM—United States Cyber Command

VVoIP—Voice and Video over Internet Protocol

Terms

Air Force Information Network—AF provisioned portion of the Department of Defense Information Network.

Air Force Information Technology—Traditional Information Technology, Operational Technology and Platform Information Technology.

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

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

Classified Information Spillage—Security incident that occurs whenever classified data is spilled either onto an unclassified information system or to an information system with a lower level of classification. (Committee on National Security Systems Instruction No. 4009).

Collaborative Computing—Applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment. (Committee on National Security Systems Instruction No. 4009).

Common Criteria—Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Committee on National Security Systems Instruction No. 4009).

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

Computer Security—Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (Committee on National Security Systems Instruction No. 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. (Committee on National Security Systems Instruction No. 4009).

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

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

Data Spillage—Security incident that results in the transfer of classified or Controlled Unclassified Information onto an information system not accredited (i.e., authorized) for the appropriate security level. (Committee on National Security Systems Instruction No. 4009).

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

Degaussing (or Demagnetizing)—Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. (National Security Agency/Central Security Service Policy Manual 9-12).

Demilitarized Zone—1. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. 2. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. (National Institute of Standards and Technology Special Publication 800-45 Version 2, *Guidelines on Electronic Mail Security*).

An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the demilitarized zone and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (National Institute of Standards and Technology Special Publication 800-41 Revision 1, *Guidelines on Firewalls, and Firewall Policy*).

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

Department of Defense Information Network—The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or standalone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Formerly known as the Global Information Grid. (Joint Publication 1-02).

Flash Media—Devices or products that maintain stored data without any external power source. Data can be electro-magnetically written, erased, and/or reprogrammed. General storage and example devices used for data transfers between information systems and other digital products are items such as memory cards, universal serial bus flash drives, and solid-state drives. (Committee on National Security Systems Instruction No. 4009).

Information Assurance—**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. (Committee on National Security Systems Instruction No. 4009).

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. (Committee on National Security Systems Instruction No. 4009).

Mobile Device—A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. **Note:** If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device. (Committee on National Security Systems Instruction No. 4009).

Non-Enterprise Activated Commercial Mobile Device—A non-enterprise activated device is any Department of Defense mobile handheld device that is not connected at any time to a Department of Defense network or enterprise, and does not process sensitive or classified Department of Defense data or voice communications. Sensitive data or information is defined as any Department of Defense data or information that has not been deemed as publicly releasable by a Department of Defense Public Affairs Officer. (*Mobile Policy* Security Requirements Guide Overview).

Nonrepudiation—Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (Committee on National Security Systems Instruction No. 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. (National Institute of Standards and Technology Special Publication 800-53).

Overwriting—The process of writing data on top of the physical location of data stored on the media. (National Institute of Standards and Technology Special Publication 800-88)

Privileged User—A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Committee on National Security Systems Instruction No. 4009).

Privileged users have the same requirements as an authorized user, but have additional permissions to configure information assurance—enabled software products and systems. These uses must hold baseline commercial certifications according to Department of Defense 8570.01-M and be placed in unit manning documented positions that require privileged access. (Department of Defense Instruction 8500.01).

Remanence Security—Residual information remaining on data media after clearing. (Committee on National Security Systems Instruction No. 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, thumb drives, pen drives, and similar universal serial bus storage devices. (Committee on National Security Systems Instruction No. 4009).

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

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

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 Department of Defense 5400.11-R 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 according to the requirements of the Computer Security Act of 1987 (Public Law 100-235). (Committee on National Security Systems Instruction No. 4009).

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

Tempest—A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. (CNSSI 4009).

Vulnerability—Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (Committee on National Security Systems Instruction No. 4009).

Whitelisting—1). An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition. 2). An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments. (Committee on National Security Systems Instruction No. 4009).

Attachment 2

BRING YOUR OWN APPROVED DEVICE USER AGREEMENT

Figure A2.1. BYOAD User Agreement.

The Air Force Bring Your Own Approved Device (BYOAD) program allows military members and civilian employees to use their approved personal devices (i.e., smartphone or tablet) to access unclassified government information and applications by installing a Managed Mobile Service (MMS) on their personal devices. This program is completely voluntary and is for the convenience of the employee. Your acknowledgement of responsibilities and agreement below is required for a government-furnished MMS to be installed on your personal device. If you agree to participate in this program and you subsequently violate terms in this agreement, access to Air Force (AF) systems can be revoked and/or you could be subject to disciplinary action in accordance with the Uniform Code of Military Justice (UCMJ), or the Civilian Personnel procedures as outlined in Air Force Instruction (AFI) 36-704, Discipline and Adverse Actions of Civilian Employees or other applicable Federal law.

1. Only an approved National Information Assurance Partnership (NIAP) device may be used to participate in the BYOAD program. A list of devices can be found at https://www.niap-ccevs.org/.

2. You must ensure that the latest applicable operating system (OS) and security patches are installed on your device(s); you have 30 days to be in compliance after public release. Failure to comply may result in loss of access to BYOAD provisions/capabilities.

3. You must have a device-unlock passcode, Personal Identification Number (PIN), or biometric enabled on your device.

4. You agree to allow the government to install application(s) and/or other appropriate control mechanisms (i.e., the MMS) on your personal device. These provisions enable the government to maintain secure access control over official government applications, information, and services. The MMS and other applications are considered government-furnished equipment, and you are responsible for any malware from your device that penetrates the MMS and causes harm to any government information system.

5. You are responsible for all costs (e.g., data usage, roaming charges, device, equipment installments) associated with your commercial wireless provider agreement(s).

6. You will only access non-public Department of Defense (DOD) systems and DOD information through MMS. However, you may access/download/store your Privacy Act protected data on your personal device outside of the MMS.

7. You agree not to store any DOD non-public information outside of the MMS.

8. When accessing secured U.S. Government Information Systems through the MMS feature, you freely and voluntarily consent to applicable site conditions and government monitoring and collection by government authorities, consistent with the boundaries of the DOD Banner.

9. You agree that you are the primary user of the device, and you will not allow anyone else including family members to access the MMS or use the device while the MMS is open.

10. When travelling outside of the United States, Operational Security (OPSEC) should be adhered to, including the removal or restricted use of the MMS, depending on a unit security manager risk review.

11. By participating in this program, you consent to surrender your personal device to the appropriate authorities based on a security incident. As such, in resolving the incident, your personal phone may be held for investigative or law enforcement purposes, and the MMS is subject to search. It is always encouraged that you backup all personal data on your device.

12. You agree to report seized, lost, or stolen devices or any security incidents (e.g., malware, viruses, or unexplained software installs) to your security manager and the MMS helpdesk within 60 minutes.

13. All Civilian personnel will comply with the applicable time and accounting policies. Work schedules and hours of duty may be modified as necessary but are subject to local management procedures and approval and/or collective bargaining agreement requirements.

14. Users who actively try to subvert security controls (e.g., bypassing rooting/jailbreak detection) are subject to disciplinary action in accordance with the UCMJ, or the Civilian Personnel procedures as outlined in AFI 36-704, or other applicable Federal law.

15. The government will make all reasonable attempts to maintain secure and usable BYOAD products and services; however, they are provided on an "as is" and "as available" basis. The government makes no representations or warranties of any kind; express or implied, as to the operation or the information, content, or materials included on or otherwise made available to you through the BYOAD program. You expressly agree that your use of these products and services is at your own risk. To the full extent permissible by applicable Federal law, the government disclaims all warranties, express or implied, including but not limited to implied warranties of merchantability and fitness of these services and products.

16. While the Air Force attempts to remove and/or mitigate all threats, the government does not warrant that the MMS, information, content, or materials included on or otherwise made available to you through the MMS are free of viruses or other harmful components. The government will not be liable for damages of any kind arising from the use of the MMS from any information, content, or materials, included on or otherwise made available to you through the MMS, including but not limited to direct, indirect, incidental, punitive, and consequential damages.

By signing below you acknowledge your rights and responsibilities and agree to participate in the BYOAD program. This acknowledgement is required for your access and use of official non-public government data on your personally-owned device.

______________________________ ________________________
User's Signature Date

Attachment 3

AIR FORCE INFORMATION TECHNOLOGY USER RESPONSIBILITIES

A3.1. Overview.

A3.1.1. Protecting the confidentiality, integrity, and availability of information that is processed, stored or transmitted through the system may require a great number of discrete controls, and while privileged users may be required to maintain a finer-grained understanding of their control obligations, Air Force Information Technology users are not expected to be familiar with the details of every control.

A3.1.2. All Air Force Information Technology users will be required to be familiar with and comply with a short list of dos and don'ts that more closely pertain to their everyday experience with Air Force Information Technology.

A3.2. Implementation:

A3.2.1. All AF Information Technology Users must observe the requirements in DoD Regulation 5500.7-R, Joint Ethics Regulation (JER) **(T-0)**, and comply with the guidance contained in Air Force Instruction 10-701, Operations Security, Air Force Instruction 33-322, Records Management, Air Force Instruction 33-364, Records Disposition-Procedures and Responsibilities, Air Force Instruction 33-332, Privacy Act Program, Air Force Manual 33-363, Management of Records, and comply with public affairs Internet-based capabilities guidance and related issuances. **(T-0).**

A3.2.2. To this end, all AF Information Technology users must read and sign Rules of Behavior agreements prior to being granted access to AF Information Technology. **(T-1); see Annex 1** to this Attachment. Rules of Behavior agreements should:

A3.2.2.1. Be instantiated as a list.

A3.2.2.2. Articulate in short declarative sentences what is explicitly allowed and what is explicitly proscribed.

A3.2.2.3. Address rules that every users must read, internalize, and apply in their normal, day-to-day jobs.

A3.2.3. Rules of Behavior should be designed to reinforce the concept that every authorized Air Force Information Technology user accepts responsibility for protecting the system from compromise, commensurate with privileges associated with their role. Rules of Behavior agreements must require that, as a condition of employment and/or access, Air Force Information Technology users:

A3.2.3.1. DO adhere to legal, regulatory (T-0), and command **(T-0)** requirements.

A3.2.3.2. DO use Air Force Information Technology in a manner that protects and preserves information confidentiality, integrity and/or availability. **(T-2)**.

A3.2.3.3. DO use Air Force Information Technology in a manner that protects and preserves the physical integrity of Air Force Information Technology and Air Force cyberspace assets and resources. **(T-3).**

A3.2.3.4. DO NOT attempt to exceed the limits of authorized access and privilege. **(T-2).**

A3.2.3.5. DO NOT use Air Force Information Technology in a manner which may tend to bring discredit on users or the Air Force, or degrade the Air Force's ability to execute on its assigned missions, except for disclosure protected by Whistleblower statues. **(T-1).**

A3.2.3.6. DO NOT waste Air Force Information Technology or Air Force cyberspace assets and resources. **(T-2**).

A3.2.3.7. DO NOT connect Air Force Information Technology through public networks (Internet cafés and kiosks, hotel business centers, home networks, etc.) for processing government-owned information unless mobile computing device encryption and connection policies are followed. **(T-3).**

A3.2.4. Disciplinary Actions.

A3.2.4.1. Failure to observe the prohibitions and mandatory provisions of this Attachment by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92, Failure to Obey Order or Regulation. **(T-0).**

A3.2.4.2. Violations by civilian employees may result in administrative disciplinary action in accordance with AFI 36-703, Civilian Conduct and Responsibility, without regard to otherwise applicable criminal or civil sanctions for violations of related laws. **(T-0).**

A3.2.4.3. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. **(T-0).**

A3.2.4.4. Violations by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. **(T-0).**

Figure A3.1. ANNEX 1. Rules of Behavior and Acceptable Use Standards for Air Force Information Technology.

The following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology. By signing below, you indicate both your understanding of these standards, and your agreement to act in accordance with them as a condition of your service with or access within the Air Force. Air Force Instruction 17-130, *Cybersecurity Program Management*, applies.

1. I WILL adhere to and actively support all legal, regulatory, and command requirements.

a. I understand that Air Force Information Technology is to be used primarily for Official/ Government Business, and that limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the Air Force or the DoD.

b. I will not use my access to government information or resources for private gain.

c. I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains.

d. I will observe all software license agreements and Federal copyright laws.

e. I will encrypt sign and any message containing For Official Use Only or Personally Identifiable Information.

f. I will promptly report all security incidents in accordance with Air Force policy.

2. **I WILL use the system in a manner that protects information confidentiality, integrity and/or availability.**
   a. I will not store or process classified information on any system not approved for classified processing.
   b. I will protect my Common Access Card/hardware token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.
   c. I will protect my passwords/Personal Identification Numbers from disclosure: I will not post or write these down in my work space.
   d. I will lock or log-off my computer or terminal any time I walk away.
   e. I understand that my password/Personal Identification Numbers must adhere to current Air Force standards for length, key-space, and aging requirements.
   f. I will not disclose any non-public Air Force or DoD information to unauthorized individuals.
   g. I understand that everything done using my Common Access Card/hardware token/password/Personal Identification Number will be regarded as having been done by me.
   h. I will employ anti-malware software and update it as required; I will immediately notify my CFP or WCO if I believe Air Force Information Technology assets entrusted to me have been compromised; I will take immediate measures to limit damage.
3. **I WILL protect the physical integrity of computing resources entrusted to my custody or use.**
   a. I will protect Air Force Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.
   b. I will protect Air Force Information Technology from tampering, theft or loss; I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.
   c. I will protect Air Force Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of the information contained, and practice proper labeling procedures.
   d. I will not allow anyone to enter DoD or Air Force facilities without proper authorization.
   e. I will not install, relocate, modify, or remove any Air Force Information Technology without proper approval.
4. **I WILL NOT attempt to exceed my authorized privileges.**
   a. I will not access, research, or change any account, file, record, or application not required to perform my job.
   b. I will not modify the operating system configuration on Air Force Information Technology without proper approval.
   c. I will not move equipment, add or exchange system components without authorization by the appropriate approval of my local systems manager or local hardware custodial personnel.
   d. I will not use, or connect to, non-official hardware, software or networks for official business without proper approval and without the use of authorized mobile device network encryption.
5. **I WILL NOT use systems in a way that brings discredit on Air Force users or the Air Force, or degrade Air Force missions.**
   a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.
   b. I will not receive or send inappropriate material using my official email or Internet accounts.
   c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral or philosophical agenda.
   d. I will not add slogans, quotes, or other personalization to an official signature block.

e. I understand that pornography, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the bases of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militant, extremist, or terrorist activities will not be tolerated.
f. I will not connect or remove any form of removable media without proper approval.

6. I WILL NOT waste system and network resources.

a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook, Twitter, Instagram, Snapchat, etc.)
b. I will not make excessive use of my official computer for shopping, or to view full-motion video from non-official sources (e.g., YouTube, online multiplayer video games, etc.)
c. I will not auto forward e-mail from my official account to a personal e-mail account.

______________________________	____________________
Signature	Date
______________________________	____________________
Printed name (Last, First, MI)	Rank/Position