BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
MANUAL 17-1301

9 DECEMBER 2024

Cybersecurity

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CNZ

Certified by: SAF/CNZ
(Mr. James Bishop, SES, DAF)

Supersedes: AFMAN17-1301, 12 February 2020

Pages: 67

This Department of the Air Force Manual (DAFMAN) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, Air Force Instruction (AFI) 17-130, *Cybersecurity Program Management*, and Department of Defense (DoD) Instruction (DoDI) 8551.01, *Ports, Protocols, and Services Management*, with a focus on Computer Security (COMPUSEC). This manual applies to all civilian employees and uniformed members of the U.S. Space Force (USSF), the Regular Air Force (RegAF), Air Force Reserve (AFR), Air National Guard (ANG), the Civil Air Patrol (CAP) when conducting missions as the official Air Force (AF) Auxiliary, and those with a contractual obligation to abide by the terms of Department of the Air Force (DAF) issuances, except when noted otherwise. Failure to obey the terms of the User Agreements - DAF Form 4394, *The Department of the Air Force User Agreement Statement - Notice and Consent Provision*, and when applicable, DAF Form 4433, *The Department of the Air Force Mobile Device User Agreement* —per paragraphs **2.17.1, 7.4, and 7.6** (including its subparagraphs), constitutes a violation of "Article 92(1), Uniform Code of Military Justice (UCMJ)" by military personnel—failure to obey lawful order or regulation. "Article 92(1), UCMJ" does not apply to members of the ANG while in Title 32 status (that is, activated for state duty under state command), but ANG members may be subject to an equivalent article under a state military justice code. Violations by civilian employees may result in administrative disciplinary action in accordance with (IAW) the Department of the Air Force Instruction (DAFI) 36-147, *Civilian Conduct and Responsibility*, without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contractor personnel may be handled according to applicable laws and the terms of the contract. This Instruction requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by Department

of Defense Instruction (DoDI) 5400.11, *DoD Privacy and Civil Liberties Programs*. The applicable System of Record Notice (SORN) F017 SAF/CNA, *Bring Your Own Approved Device (BYOAD),* is available at: **https://dpcld.defense.gov/Privacy/SORNs/**. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program,* and are disposed IAW the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of the Chief Information Officer (SAF/CN) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. Send any supplements to this publication to SAF/CN for review, coordination, and approval prior to publication. The authorities to waive wing or delta, 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* DAFMAN 90-161, *Publishing Processes and Procedures, for a description of the authorities associated with the Tier numbers*. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority or alternately, to the publication Office of Primary Responsibility (OPR) for non-tiered compliance items. Further, all T-1 tiered compliance items cannot be waived without the coordination and Approval of the publication OPR. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

SUMMARY OF CHANGES

This manual, formerly issued as AFMAN 17-1301, has been updated and reissued as DAFMAN 17-1301. Significant revisions have been made to clarify COMPUSEC requirements and ensure alignment with DAFMAN 90-161. Key updates include clearer guidance on accountability and responsibilities for military personnel, civilian employees, and contractors, and revised sections on Ports, Protocols, and Services Management, as well as IT hardware procurement. User Agreements (DAF Forms 4433 and 4394) are now referenced as **Prescribed Forms** with their intent clarified, and a Virtual Mobile Infrastructure User Agreement for mobile devices has been attached to DAF Form 4433. Redundancies were eliminated, SAP equities references were removed, chapters were reorganized, and the section on abbreviations, acronyms, and terms was expanded. Additionally, a new table of valid URL references and governance document references has been added, along with guidance on safeguarding classified data at rest. Prohibitions on connecting Internet of Things devices to DAF systems and government-furnished equipment were introduced, and responsibilities for Wing or Delta Cybersecurity Offices were updated.

Further changes include adding a required Privacy Act statement for forms collecting personal information, proper tiering of T-0 based on federal law, and greater specificity regarding roles and exceptions. The Sixteenth Air Force (Air Forces Cyber) must now inform the DAF CISO of configuration changes affecting compliance with DoDI 8551.01, focusing on information sharing rather than prior approval. Foreign IT use must comply with NDAA 2023 Section 5459 and NDAA 2019 Section 889. The manual also addresses policy gaps in DISPATCH, IT procurement, data spillages, and sanitization processes. Clarifications include the treatment of classified information, end-of-life procedures, reclassification, and requirements for cybersecurity-enabled IT software and sanitization software. Updates also address device usage (e.g., laptops connected to hotspots) and processing sensitive data. A conflict with AFI 17-130 on waiver authorities was resolved.

Reflecting broader DoD and DAF policy updates, the manual incorporates changes related to mobile devices, wireless capabilities, and the reuse of media containing Controlled Unclassified Information. A comprehensive review is strongly recommended.

Chapter 1

INTRODUCTION

1.1. Overview. COMPUSEC is a cybersecurity discipline focused on protecting Information Systems and data by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Compliance with this publication ensures the appropriate implementation of measures designed to protect all information system resources and information. This publication focuses on Endpoint Security, Remanence Security, and Ports, Protocols, and Services Management (PPSM) within the DAF; also, refer to the technical standards for IT in the DoDI 8310.01, *Information Technology Standards in the DoD*. For guidance on Zero Trust-related topics, including principles for data security and access, please refer to the *DAF Zero Trust strategy*. When used in this publication, the term major command (MAJCOM) includes AF MAJCOMs, USSF Field Commands, field operating agencies, and direct reporting units.

1.2. Applicability. This publication applies to all DAF IT used to process, store, display, transmit, or protect DAF information, regardless of classification or sensitivity, unless exempted through **paragraph 1.3** exceptions. For specific guidance for Intelligence Community information technology refer to the Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation;* and applicable instructions issued by the Committee on National Security Systems (CNSS).

1.2.1. More restrictive federal, DoD, and/or DAF guidance takes precedence over this publication.

1.2.2. This publication and implementation guidance identified within is not applicable to Special Access Program (SAP) information systems and networks. Refer to the Department of Defense Manual (DoDM) 5205.07 Volumes 1-4, the DoD Joint SAP Implementation Guide (JSIG), and the DAF SAP Cybersecurity Office MilSuite (*see* **Table A.2–URLs**).

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

1.3.1. Process acquisition waiver requests for network infrastructure and endpoint equipment according to DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability.*

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

1.3.3. Process information system exceptions (non-compliance) to PPS (Ports, Protocols, and Services) standards according to AFI 17-101 and the DoD PPSM Exception Management Process as implemented by the DAF.

1.3.3.1. The DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**) provides the latest DoD PPSM exception and Non-Compliant PPS 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 (*see* **Table A.2–URLs**).

1.3.4. Process waivers to the DoD-approved cybersecurity baseline certification requirements for civilian and military personnel IAW DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program,* and DAFMAN 17-1305, *Cyberspace Workforce Management.*

1.3.5. Unless specifically restricted in this publication, commanders have the authority to waive non-tiered requirements IAW DAFI 90-160, *Publications and Forms Management*. However, they must send a copy of the approved waiver to the OPR of the higher headquarters publication being waived within 30 days of approval.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Introduction. Information System Security Managers, Information System Security Officers, and all workforce personnel entrusted with privileged roles are responsible for compliance with this issuance.

2.2. Chief Information Officer (SAF/CN). Appoints all DAF Authorizing Officials (AO) in writing and specifies the authorities delegated to the AO. Serves as the DAF voting representative on the DoD PPSM Configuration Control Board IAW DoDI 8551.01 and the DoD PPSM Configuration Control Board Charter (*see* **Table A.2–URLs**).

2.3. Commander, Headquarters Air Combat Command (ACC). Provides guidance and oversight on the implementation of PPS policy according to this manual and DoDI 8551.01; s*ee* paragraph 2.7 and paragraph 3.3.

2.3.1. Designates one primary and at least two alternate subject matter experts to serve as DAF representatives to the DoD PPSM Technical Advisory Group according to DoDI 8551.01 and the DoD PPSM Configuration Control Board Charter.

2.3.2. Provides PPS registrars responsible for managing access and entering applicable DAF information systems and associated PPS information into the DoD PPSM Registry according to DoDI 8551.01.

2.4. Space Operations Command (SpOC). Manages mission circuits and is responsible for the majority of the RMF process for USSF, including hosting the USSF AO for many Space Systems. It also plans and programs for Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), and DoDIN Operations. SpOC relies on Air Combat Command (ACC) for guidance and oversight on implementing PPS policy and on Cyberspace Capabilities Center (CCC) for cybersecurity expertise, including COMPUSEC and PPSM activities; *see* **paragraph 2.3.**

2.5. DAF CIO-Appointed Authorizing Officials (AO). Per AFI 17-101, AOs are the officials with the authority and responsibility for accepting risk for an IT system. They balance the level of risk for a system with mission requirements and are the only person with the authority to grant authorization decisions within their area of responsibility IAW AFI 17-101. AOs have the flexibility to augment, execute, and implement RMF for systems in their AOR. COMPUSEC and PPSM are smaller and individual components that help address security controls that comprise the RMF program and processes. Non-compliance with COMPUSEC or PPSM requirements must be identified against associated security controls to the AO in the system's RMF package. The AO's responsibility is to ensure compliance with this regulation whenever possible and evaluate and consider accepting risks that are within their authority. At a minimum, AOs will:

2.5.1. Restrict PPS used by the information system to only the PPS required for the information system to meet mission needs.

2.5.2. Ensure the documentation and approval of PPS as part of the risk management framework process.

2.5.2.1. Ensure declared PPS comply with DoD PPSM standards for implementation.

2.5.2.1.1. Review requests for the temporary use of PPS not listed on the DoD PPSM Category Assurance List according to DoDI 8551.01 and the DoD PPSM Exception Management Process.

2.5.2.1.2. Review exception requests for PPS according to the DoD Ports, PPSM Exception Management Process.

2.5.2.1.3. Ensure compliance with DoDI 8551.01 and the hosting environment connection rules for the use of PPS within research, test, and evaluation information networks.

2.5.2.2. Include documentation and assessment of vulnerabilities for the declared PPS.

2.5.2.3. Verify PPS registration supporting cybersecurity reciprocity of information systems from other DoD components.

2.5.2.4. Review exception requests for PPS according to the DoD PPSM Exception Management Process.

2.6. Sixteenth Air Force (Air Forces Cyber). Regulates the use of PPS within the DAF, ensuring routers, firewalls, and intrusion detection devices are configured to allow only approved PPS, according to DoDI 8551.01.

2.6.1. Ensures boundary protection devices allow only approved PPS through configuration control processes.

2.6.2. Ensures an annual review, at a minimum, of boundary protection device rules for compliance with DoDI 8510.01, *Risk Management Framework for DoD Systems.*

2.6.3. Verifies PPS registration prior to connection of information systems to the Air Force Information Networks (AFIN).

2.6.4. Blocks PPS not implemented according to this policy and DoDI 8551.01 using boundary protection devices and application whitelisting.

2.6.5. Assures the interoperability of PPS across the AFIN when implemented according to this policy and DoDI 8551.01.

2.6.6. Informs DAF CISO of configuration changes that take PPS, routers, firewalls, and intrusion detection devices out of compliance with DoDI 8551.01.

2.7. Headquarters Cyberspace Capabilities Center (HQ CCC). Provides cybersecurity expertise to ACC for COMPUSEC and DAF PPSM activities and functions.

2.7.1. Provides COMPUSEC and PPS policy and technical subject matter expertise for the DAF.

2.7.2. Provides field support and program management for COMPUSEC and PPS to SAF/CN, ACC, and all major commands. Supports SAF/CN and ACC cybersecurity initiatives. Reviews, evaluates, and interprets DAF COMPUSEC and PPS doctrine, policy, and procedures. Develops/coordinates recommendations on implementation of the doctrine, policy, and procedures to ACC/A6, Communications Directorate.

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

2.7.4. Maintains DAF Cybersecurity Program content on cybersecurity collaborative environments for providing immediate access to and awareness of current DAF, DoD, and federal policy and guidance, including recent and pending changes to DoD and DAF policy.

2.7.5. Provides PPS policy and implementation guidance to information system program managers, Information System Security Managers/Information System Security Officers, Change Sponsors, network/cyberspace operations squadrons, and Sixteenth Air Force (Air Forces Cyber).

2.7.5.1. Registers and updates PPS for information systems authorized by DAF AOs.

2.7.5.2. Manages access to the DoD PPSM Registry database and processes account requests on behalf of the DoD PPSM for authorized DAF users.

2.7.5.3. Ensures the integrity of PPS records for DAF information systems in the DoD PPSM Registry is consistent with information system authorization conditions according to AFI 17-101.

2.7.5.3.1. Processes exceptions and risk assessments for non-compliant PPS and provides recommendations for change requests affecting DAF information system communications interfaces to include DoD Demilitarized Zone (DMZ) whitelist requests. Ensures DAF DMZ whitelist records are compliant prior to submission to JFHQ-DoDIN for processing in the Defense Information Systems Agency (DISA) DMZ whitelist database (*see* **Table A.2–URLs**). The DMZ is the perimeter network segment that is logically between internal and external networks.

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

2.7.5.4. Serves as DAF Representative for DoD PPS Technical Advisory Group; analyzes DoD PPSM Technical Advisory Group votes and provides recommendations to the DAF PPSM Configuration Control Board voting member.

2.8. Space Delta 6 (Cyberspace Operations). Prepares, presents, and integrates assigned and attached forces to secure and defend the USSF space systems enterprise and provide assured access to space mission systems. As the USSF certified and accredited Cyber Security Service Provider, Space Delta 6 (DEL 6) provisions cybersecurity services to protect USSF Space Enterprise Platform IT and mission systems. It provides mission-area expertise to SpOC on force or capability assessment and development efforts; *see* **paragraph 2.4**.

2.9. Wing or Delta Cybersecurity Office (or Designated Equivalent). The Wing Cybersecurity Office (WCO) addresses all Unclassified (to include CUI), and Secret Collateral 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 to the contrary exist. In certain Wings and Deltas, the WCO operates under the Comm Squadrons, so any references to USAF terminology WCO will also pertain to the <Base> Cybersecurity Office or its USSF counterpart, as applicable. Personnel assigned to the WCO will:

2.9.1. Evaluate modifications, exceptions, and deviations to information systems made through the RMF process for accuracy and completeness before forwarding them to the appropriate agency.

2.9.2. 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**.

2.9.3. Coordinate with the system/enclave Information System Security Manager/Information System Security Officer before deciding whether to sanitize media for reuse or disposal; *see* Chapter 5.

2.9.4. Maintain organizational email account with an SMTP alias of <wing>**.cybersecurity@us.af.mil**.

2.9.5. The WCO will ensure the maintenance and compliance of appropriate cybersecurity posture of tenants and organizations. Bases have discretion on how to maintain compliance. Bases may integrate Management Internal Control Toolset (MICT), Self-Assessment Checklists (SAC), SharePoint, and/or on-site inspections into local Base compliance programs. The WCO is responsible for establishing a local compliance program on its Base. Conduct continual evaluation to maintain program oversight and identify gaps or deficiencies in existing policy, guidance, training, and resources. Participate in the continual evaluation processes by monitoring data. Utilize the MICT SAC to help assess and prioritize higher headquarters' requirements and document self-identified, non-compliant observations with corrective action plans IAW DAFI 90-302, *The Inspection System of the Department of the Air Force*.

2.10. Commanding Officer (or Equivalent). Maintains the COMPUSEC program according to this publication, ensuring DAF 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:

2.10.1. Ensure proper procedures are followed in response to Unauthorized Disclosure of Classified Information (classified information spillage or, formerly called, classified message incident) affecting DAF information systems; *see* Chapter 4.

2.10.2. Review all approved removable media/data loss prevention exemptions semi-annually to ensure continuous validation of mission requirements; *see* Chapter 4.

2.11. Program Manager (PM). Ensures proper implementation of security controls and processes related to PPS, including developing and maintaining a plan of actions and milestones (POA&M) and conducting annual reviews according to AFI 17-101. In the absence of a designated PM, an ISO is appointed to fulfill all PM roles and responsibilities as outlined in AFI 17-101. PMs will:

2.11.1. Ensure system users' privileges are validated, at a minimum, annually. When warranted, system owners are required to reassign or remove privileges to reflect duties in support of mission/business needs correctly.

2.11.2. Manage and facilitates the operation of defensive cyber operations and internal cybersecurity for mission systems.

2.11.3. Ensure all systems in the DoD PPS Management Registry are reviewed and updated if needed, a minimum of annually; *see* AFI 17-101.

2.11.4. Document these validations and reviews.

2.12. Information System Security Manager (ISSM). Formerly an Information Assurance Manager, responsible for the cybersecurity of a program, organization, system, or enclave and providing direction to the Information System Security Officer (formerly a system Information Assurance Officer). The duties of the ISSM are outlined in DoDI 8500.01, *Cybersecurity,* AFI 17-101, DoDI 8510.01, and DAFMAN 17-1305. ISSMs will:

2.12.1. Perform risk identification and assessment activities supporting the change management activities for the system/enclave; *see* Chapter 3.

2.12.1.1. Ensure any changes affecting the system's PPS registration (ports, DMZ whitelisting, Internet Protocol addresses, domain name service) comply with the DoD PPS Category Assurance List and the DoD PPS Vulnerability Assessment reports (*see* **Table A.2–URLs**).

2.12.1.2. Assist stakeholders (system administrators, network infrastructure personnel, programmers, etc.) with the identification, declaration, and documentation of PPS requirements; *see* Chapter 6.

2.12.1.3. Ensure PPS registration is updated prior to submitting change requests through the Enterprise Information Technology Service Management systems on the Secret Internet Protocol Router Network (*see* **Table A.2–URLs**).

2.12.1.4. Assist change sponsors with identifying and declaring the PPS required for supporting change requests. Provide guidance completing firewall exception requests, Domain Name Service changes, and DoD DMZ whitelist requests, ensuring requested Internet Protocol addresses, fully qualified domain names, and PPS are registered in the DoD PPSM Registry database.

2.12.2. Maintain approval and inventory documentation for AO-authorized personally owned hardware and software in eMASS; *see* Chapter 4 and **Table A.2–URLs**.

2.12.3. Process data loss prevention exemptions and removable media whitelist requests; *see* Chapter 4.

2.12.4. Protect collaborative computing devices used in classified environments; *see* Chapter 4.

2.12.5. Participate in remanence security risk management processes; *see* Chapter 5.

2.12.6. Manage the implementation of PPS for appointed information systems; *see* Chapter 6.

2.12.6.1. Document and assess the vulnerabilities for the use of PPS not listed on the DoD PPSM Category Assurance List using the DoD PPSM Exception Management Process (*see* Chapter 6) and PPS guidance on the DAF Cybersecurity Collaborative Environment.

2.12.6.2. Obtain approval for the use of PPS through the risk management framework process.

2.12.6.3. Submit requests for initial PPS registration based upon initial risk management framework authorization.

2.12.6.4. Submit updates to PPS registration based upon configuration management plans, security impact processes, and continuous monitoring under the risk management framework.

2.12.6.5. Maintain PPS registration records for the information system as an artifact within the risk management framework and required repositories, to include eMASS, DoD PPS Registry, and other DAF approved repositories.

2.12.6.6. Verify the PPS registration and required interfaces for interconnected information systems.

2.12.6.7. Submit exception requests for PPS according to the DoD PPSM Exception Management Process, PPS guidance on the DAF Cybersecurity Collaborative Environment, and orders from US Cyber Command, as applicable.

2.12.6.8. Annually reviews the system(s) of record in the DoD PPSM Registry.

2.12.6.9. Ensure the removal of records from the DoD PPSM Registry upon an information system decommission and/or system expiration.

2.12.6.10. Submit change requests to network devices, boundary protection devices, and other configuration control assets under the applicability of DoDI 8551.01 using the DoD PPSM Registration Confirmation Details artifact for the associated information system.

2.12.7. Manage and implements the operation of defensive cyber operations and internal cybersecurity for mission systems.

2.12.8. Ensure users of the information system are briefed on user responsibilities IAW DoD 5500.7-R, *Joint Ethics Regulation.* The Cyber Awareness Challenge computer-based training course satisfies this requirement for the AFNet unprivileged users. Follow guidance from the information owner and information system owner if additional topics from DoD 5500.7-R are required.

2.12.9. All ISSM personnel, including civilians, military, and contractors, shall receive comprehensive training on cybersecurity, COMPUSEC, PPS, and TEMPEST policies, as well as other relevant topics to ensure they possess the necessary skills and knowledge to carry out their duties effectively. The ISSM course at Keesler is a DAF residential requirement for ISSMs IAW DAFMAN 17-1305; if unavailable, attend similar DAF or DoD recommended training. Refer to the DoD Manual 8140.03, "Cyberspace Workforce Qualification and Management Program," qualification matrices at The DoD Cyber Exchange (*see* **Table A.2–URLs**) for further information and guidance on qualification criteria.

2.13. 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 ISSM and the Information System Security Officer roles. DoDI 8500.01, AFI 17-101, and DAFMAN 17-1305 outline the duties of the Information System Security Officer. Information System Security Officers will:

2.13.1. Protect all assets, to include information systems and data, from threats by implementing technical and physical security mechanisms; *see* Chapter 4.

2.13.2. Participate in change management activities as assigned by the ISSM, assisting stakeholders (system administrators, network infrastructure personnel, programmers, etc.) with the declaration and documentation of PPS required for the information system.

2.13.3. Participate in remanence security risk management processes; *see* Chapter 5.

2.13.4. Execute procedures that identify and mitigate the residual risk and risk tolerance; *see* Chapter 5.

2.14. Commanders Support Staff, or Similar Administrative Support Function. Organizations implement and enforce AFIN account management and COMPUSEC administrative processes and procedures using guidance within this manual.

2.14.1. The organization shall appoint a Primary and Alternate designated to perform these administrative functions and will be the focal point for Information System (IS) access control, endpoint security, and COMPUSEC assessments.

2.14.2. Personnel performing administrative cybersecurity functions assist WCO with downward-directed administrative cybersecurity functions (administrative tasking orders, in/out-processing checklists, distributing user training materials, etc.); *see* Chapter 4.

2.15. Change Sponsor. Changes to an information system require coordination with the system ISSM, ensuring that requested modifications follow the established change management process and do not introduce vulnerability to AFIN. 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 ISSM and any change management request tools; *see Methods and Procedures Technical Order 00-33A-1100* for guidance. Organizations in need of a change sponsor can contact their WCO or attached WCO. Change Sponsor will:

2.15.1. Review requests, ensuring the proposed change does not violate policies and has been assessed and approved by the system ISSM.

2.15.2. Ensure the system being modified has a current authorization decision. For guest systems, assist the change initiator with obtaining a copy of the authorization to operate and the authorization to connect documentation.

2.15.2.1. If modification requests affect interfaces (Internet Protocol addresses, ports/protocols/services, etc.) for the system, provides the DoD PPSM Tracking Identifier.

2.15.2.2. If the system does not have a valid DoD PPSM Tracking Identifier, then the system and the proposed changes must be registered in the DoD PPSM Registry database before any change requests are submitted; *see* Chapter 6.

2.16. Privileged User. IAW the regulations outlined in DAFMAN 17-1305, users with administrative or elevated access rights must meet the qualifications and Computing Environment certification requirements. These qualifications are established based on the KSAs (knowledge, skills, and abilities) and tasks of specific cyberspace work roles and include the following minimum requirements: Foundational: (1) Education, training, or personnel certification; (2) Residential: On-the-job qualification and discretionary environment-specific requirements; (3) Continuous Professional Development: Ongoing professional development requirements and sign a Privileged User Agreement. **(T-0)**.

2.17. Authorized User. All users of DoD information systems will sign and abide by DAF Form 4394. Local organizational commanders must restrict access to DAF IT for those personnel who fail to sign the agreement. Report to the Enterprise Service Desk any failures to sign the agreement for revocation of access to enterprise capabilities. User behaviors are monitored to detect potentially unauthorized activity. Also *see* **paragraph 2.17.1**.

2.17.1. User Agreements: DAF Form 4394, which is mandatory for all users of DAF Information Systems, and DAF Form 4433, which applies to users of DAF-issued Mobile Devices, DAF Approved Mobile Devices (AMD), or AMD Virtual Mobile Infrastructure (VMI), are used to document agreements by DAF users.

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

3.2.1. Data loss prevention exemptions and accountability according to the latest Tasking Order (TASKORD) found on the DISPATCH website (*see* **Table A.2–URLs**). **(T-2)**.

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

3.2.3. Current Negligent Discharge of Classified Information policy and procedures according to the latest Tasking Order found on the DISPATCH site. **(T-1)**.

3.3. DAF Cybersecurity Collaborative Environment. ACC Cyberspace Capabilities Center maintains DAF Cybersecurity Program content on cybersecurity collaborative environments for providing immediate access to and awareness of current related DAF, DoD, and federal policy and guidance, including recent and pending changes to DoD and Air Force policy. The DAF Cybersecurity Collaborative Environment serves as a cybersecurity support resource for the USAF and USSF WCO and cybersecurity workforce personnel, providing a collaborative one-stop-shop for COMPUSEC, PPS, and TEMPEST-related information, frequently asked questions, discussions, templates, and hosts dynamic content for information sharing. For classified content, the DAF Cybersecurity Collaborative Environment - Secret Internet Protocol Router Network is available (*see* **Table A.2–URLs**).

3.3.1. Sites with a usaf.dps.mil domain/URL, including the DAF Cybersecurity Collaborative Environment, are accessible by both DAF users and guests from other DoD Microsoft 365 tenants. Non-DAF365 personnel in other DoD tenants should refer to the Guest Access article on milBook for details on obtaining a guest account in the DAF365 tenant (*see* **Table A.2–URLs**).

3.3.1.1. Access to AFNet shell accounts via Information Assurance Officer (IAO) Express or Air Force Directory Services (AFDS) is limited to logging into AF machines. For SharePoint Online (SPO), non-DAF365 DoD personnel can be invited as guests to access SPO sites without needing a network shell account. Detailed documentation on guest access scenarios is available in the Guest Access with the tenant article (*see* **Table A.2–URLs**).

3.3.1.2. If the user has a DAF-issued common access card but is not a DAF Network user, he or she will already have a shell account in the network; a DAF Network Commander's Support Staff/Communications Focal Point representative may use a DAF approved account management tool to request/enable access. For example, in the IAO Express web

application, an authorized user can enable the new shell account and remove the Personnel Category Code from the user's login identifier by opening the SharePoint® Access menu in IAO Express. **Note:** IAO Express is the client interface for the Enterprise Service Desk, normally limited to the Commander's Support Staff, Communications Focal Point, Computer Support Technicians, and/or WCO personnel (if supporting an organization in an administrative capacity).

3.3.1.3. A DAF sponsor with a DAF approved account management tool such as "IAO Express" account can create a DAF Network shell account for non-DAF issued common access card holders, enable SharePoint® access, and strip the Personnel Category Code from the user's login identifier.

3.3.2. Access to the DAF Cybersecurity Collaborative Environment- Secret Internet Protocol Router Network requires a 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 DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**).

3.4. Methods and Procedures Technical Order. Methods and Procedures Technical Order 00-33A-1100, *AFNet Operational Change Management Process*, provides change submission and implementation guidance for the DAF Network. Obtain Methods and Procedures Technical Orders via the organizational Technical Order Distribution Account on Enhanced Technical Information Management System (*see* **Table A.2–URLs**). Contact the DAF COMPUSEC Field Support office via email at **daf.compusec.field.support@us.af.mil** for procedural guidance to the cybersecurity workforce to implement and manage methods and processes pertaining to COMPUSEC policy.

3.5. IT Asset Procurement. Comply with evaluation and validation requirements in DoDI 8500.01 for all IT services, hardware, firmware, software components, or products incorporated into DoD information systems using validated Commercial Off-The-Shelf (COTS) products from the National Information Assurance Partnership (NIAP) Product Compliant List (PCL). COTS cybersecurity IT products and cybersecurity-enabled IT products, formerly known as IA and IA-enabled IT products, must be NIAP certified and meet the requirements of the Committee on National Security Systems Policy (CNSSP) No. 11. Products evaluated in another Common Criteria Recognition Arrangement (CCRA) Scheme can be procured for National Security Systems only if listed on NIAP's PCL. Products on the Common Criteria (CC) Portal must follow the process to be added to the NIAP PCL before being eligible for procurement. Refer to **Table A.2–URLs** for the link to the NIAP certified products website. NIAP requires that the Common Criteria Testing Laboratories (CCTL) reside within the U.S. The System's AO should be consulted about what product(s) can be connected to a system to ensure the necessary level of protection.

3.5.1. Follow the guidance available on the 771st Enterprise Sourcing Squadron (ESS) Client Computing Solutions III (CCS-3) SharePoint site and in DAFMAN 17-1203. The 771st ESS Enterprise Hardware Commodity Acquisition Programs is the primary Air Force procurement office for strategically sourced IT requirements. Guidance for smaller purchases of IT hardware, cellular, and peripheral devices can be found at local contracting offices. If the device is not listed on such buying programs, obtain a waiver to purchase the desired device, which requires major command approval. Products must be National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme (NIAP/CCEVS) certified if

it provides cybersecurity or is cybersecurity-enabled (encryption, authentication, etc.). Products obtained through the waiver process require a risk assessment and must receive AO approval prior to connection to the AFIN; connection authorization is not automatic. Guidance for obtaining a waiver, waiver form, and "Request for Quote" process is posted on the CCS-3 SharePoint site (*see* **Table A.2–URLs**).

3.5.2. Life Cycle Management. Procure products and adopt risk-based program management according to DAFI 63-101/20-101, *Integrated Life Cycle Management.*

3.5.3. Unified Capabilities. Modernizing IT capabilities while aligning with joint solutions remains two of the DAF's key goals. DoDI 8100.04, *DoD Unified Capabilities (UC),* and applicable DISA Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) provide guidance related to Voice and Video over Internet Protocol, Video Teleconferencing, and DoD interoperability requirements (*see* **Table A.2–URLs**).

3.5.3.1. IAW DoDI 8100.04, use/obtain Unified Capabilities products certified by the DISA Joint Interoperability Test Command (JITC). The Joint Interoperability Test Command certifies interoperability, and the Unified Capabilities-implementing DoD component AO or the DISA Certifying Authority certifies cybersecurity under the risk management framework. Approved products are listed on the DISA Unified Capabilities Approved Products List and should be added to the enclave security authorization package and assessed for cybersecurity through the risk management process (*see* **Table A.2–URLs**).

3.5.3.2. As a general rule, Section 508-compatible Voice over Internet Protocol devices are not listed on the DISA 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 DISA Unified Capabilities Certification Office for inclusion in the certification. The DISA 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.

3.5.4. Foreign-produced products. Section 4862 of Title 10, U.S. Code requires that the DAF generally use products made in the United States. This statute is implemented by Subpart 25.1 of the Federal Acquisition Regulation (FAR) and Subpart 225 of the Defense Federal Acquisition Regulation (DFAR) Supplement. Section 4862 of Title 10, U.S. Code, the FAR, and the DFAR all provide for exceptions that in certain circumstances allow for the purchase of foreign-made commercial technology. Contact your servicing legal office for guidance. *See* the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement (under "Supplemental Regulations"); and **Table A.2–URLs**.

3.5.4.1. Use an approved importer or through a World Trade Organization Government Procurement Agreement country. General Services Administration offer foreign-made products secured from an approved importer or World Trade Organization Government Procurement Agreement. **(T-1)**.

3.5.4.2. 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 (*see* **Table A.2–URLs**).

3.6. Configuration Management. Cybersecurity reference documents, such as National Institute of Standards and Technology (NIST) Special Publications (SP), DISA STIGs and SRGs, National Security Agency (NSA) Security Configuration Guides, DAF Technical Orders/Methods and Procedures, TASKORDs, and other specialized publications are used for the security configuration and implementation guidance as applicable. Apply these reference documents according to DoDI 85xx.xx series and DAFI 17-xxx series publications to establish and maintain a minimum baseline security configuration and posture. Document all configuration changes with the enclave/system ISSM in the information system security authorization package according to AFI 17-101 and secure approval for implementation via the system's configuration management process. Additionally, refer to the MPTO 00-33A-1101 *AFNET Asset and Configuration Management Process* for further guidance.

3.6.1. The MilSuite collaborative environment 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 (*see* **Table A.2–URLs**).

3.6.2. PPS Category Assurance List, Vulnerability Assessments, Component Local Service Assessment, and exception management guidance are available on the DoD Cyber Exchange (*see* **Table A.2–URLs**).

3.7. Ports, Protocols, and Services Identification, Declaration, and Registration. Identify the use of internal and external PPS through the assessment and authorization process as prescribed by DoDI 8510.01. The *Ports, Protocols, and Services Management Boundaries Information (PPSMBI) Workbook* template serves as a supporting assessment and authorization artifact for PPS documentation, along with service level agreements for connections/interfaces, functional dataflow diagrams, and topology diagrams. The latest *PPSMBI workbook* can be downloaded from the Enterprise Mission Assurance Support Service (eMASS). Further guidance can be found on the DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**).

3.7.1. The ISSM has the primary responsibility for populating the *PPSMBI workbook* 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 in declaring the PPS properly. Use the Category Assurance List, Vulnerability Assessment reports, and Component Local Service Assessments provided by the DoD Cyber Exchange to determine DoD-authorized PPS.

3.7.2. DISA Storefront provides online PPSM training for PPSM overview, registry, network boundaries, and using the Category Assurance List (*see* **Table A.2–URLs**).

3.7.3. Cybersecurity and Infrastructure Security Agency (CISA) Learning hosts various courses for understanding firewalls, network security devices, protocols, and other IT-related content (*see* **Table A.2–URLs**).

3.8. Defense Information Systems Agency Resources. DISA operates websites providing STIGs, SRGs, PPSM, the DoD Unified Capabilities Approved Products List, Cloud Computing Security, online cybersecurity training, and other related guidance. *See* **Table A.2–URLs** for the DoD Cyber Exchange website addresses on the Non-classified Internet Protocol (IP) Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet).

Chapter 4

ENDPOINT SECURITY

4.1. Introduction. Endpoint security provides the basis for the overall protection of DAF-controlled IT assets. Except where specifically called out, ISSMs, 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 (CJCSI) 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 DoD and DAF provided enterprise-wide solutions for remediation of vulnerabilities for endpoint devices. Refer to Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems from Insider Threat*, and CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems* for guidance on protecting national security systems from insider threats and reducing the risk of removable media. Additionally, consult publications used by DISA during the Cyber Operational Readiness Assessment (CORA) inspections, including Tab F to Appendix 16 to Annex C to Joint Force Headquarters–Department of Defense Information Network (JFHQ-DODIN) Operations Order (OPORD) 8600-24, *Endpoint Security Operations* and DISA Comply to Connect (C2C) Step 1 Reporting Guide V1 or the latest for endpoint security.

4.2. General Protection. All authorized users should protect networked information systems, standalone information systems, or both against tampering, theft, and loss. Protect information systems from insider and external threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, DAF publications, and organizationally created procedures. *See* DAFI 31-101, *Integrated Defense (ID)*, for physical access security guidance. Contact the DAF COMPUSEC Field Support office via email at **daf.compusec.field.support@us.af.mil** for procedural guidance to endpoint security.

4.2.1. ISSMs/Information System Security Officers provide protection from threats by ensuring proper configuration of technical security mechanisms and establishing physical controls for the removal and secure storage of information from unattended information systems (e.g., Common Access Card removal lock feature, keyboard locks, secure screen savers, and security software). **(T-1)**. This is done according to the DISA *Operating Systems* STIGs and the system authorization package. **(T-1)**. *See* NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations.*

4.2.2. Treat devices released to or potentially accessed by unauthorized personnel (outside DoD control) as untrusted devices until an ISSM/Information System Security Officer re-establishes and validates the information system security policy requirements of the system.

4.2.3. Protect devices at the applicable security classification of the information stored in the device according to CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)* and this publication. For handling devices affected by a data spillage, refer to **paragraph 4.5** and **paragraph 4.9.9**.

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

4.2.5. Control viewing of United States-only information systems and equipment by foreign nationals/local nationals according to CJCSI 6510.01F; *see* the DISA *Traditional Security Checklist*. URL is available in **Table A.2**.

4.2.6. Ensure transmission of sensitive information is encrypted using NIST-certified cryptography at a minimum according to CJCSI 6510.01F. Ensure sensitive information is marked appropriately and meets CUI requirements, IAW DoDI 5200.48, *Controlled Unclassified Information*.

4.2.7. Ensure the transmission of classified information is encrypted using NSA-endorsed Type 1 product according to AFMAN 17-1302-O, *Communications Security (COMSEC) Operations,* and CJCSI 6510.01F. **(T-0)**.

4.2.8. Ensure information systems meet TEMPEST requirements according to Air Force Systems Security Instruction (AFSSI) 7700, Emission Security, and all other AF TEMPEST policies, Emission Security and TEMPEST Information Messages in areas where classified information is processed; *see* **paragraph 4.7.4**.

4.2.9. Appropriately mark and label IT devices according to the highest level of classification processed or displayed on the device according to DoDM5200.01v2_AFMAN16-1404v2, *Information Security Program: Marking of Classified Information,* DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information,* and 32 CFR Part 117, *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, and mouse (KVM) devices 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, and mouse switches (regardless of classification environment) to identify the switch position and the associated classification of the connected systems according to the DISA Traditional Security Technical Implementation Guide, V-245822. Ensure the KVM User Agreement is signed and tracked.

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 WCO 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 DoDM5200.01v3_AFMAN16-1404v3. For remanence security guidance, *see* Chapter 5.

4.2.11. Follow the guidance in the current 616 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 AFIN.

4.3. Software Security. The ISSM ensures all software is included in the information system security authorization package according to AFI 17-101 and CJCSI 6510.01F. Comply with DAFMAN 17-1203 for software accountability guidance. *Also see* **paragraph 4.10.3,** assistive technology.

4.3.1. Freeware, public domain software, shareware originating from questionable or unknown sources (e.g., worldwide 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 DAF 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 NIST SP 800-53, Rev. 5, DISA STIGs, SRGs, and CJCSI 6510.01F. All cybersecurity IT and cybersecurity-enabled IT products must meet the evaluation and validation requirements of CNSSP #11 per DoDI 8500.01, requiring the use of validated COTS products from the NIAP PCL. *See* **paragraph 3.5** for additional guidance.

4.4.1. Information systems security sustainment must be achieved by adhering to current industry best practices, as recommended by the NIST guidelines, STIGs and SRGs. This includes establishing an effective vulnerability management process. This process includes verifying that authorized software applications in information systems are updated to the correct version and protected against malicious logic. Security patches for new vulnerabilities will be promptly made available and applied by specified suspense dates, per relevant directives.

4.4.2. Implement antivirus software with current signature files according to NIST SP 800-83 Rev 1, Guide to Malware Incident Prevention and Handling of Desktops and Laptops and applicable STIGs. The ISSM documents the 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 NIST SP 800-53, Rev. 5.

4.4.3. Ensure the use of only AO authorized antivirus applications, security patches, signature files, and data files, or those from the Defense Asset Distribution Systems hosted at the DoD Patch Repository (*see* **Table A.2–URLs**).

4.4.4. Configure virus scanning frequency and real-time protection according to the applicable DISA Security Technical Implementation Guide; document scanning frequency in the system authorization package according to NIST SP 800-53, Rev. 5. **(T-0)**.

4.4.5. 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.

4.4.6. Implement malicious logic protection for Mobile Code Technologies according to the DISA *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 DoDM5200.01v3_DAFMAN16-1404v3, *Information Security Program: Protection of Classified Information*, DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* and the current 616 Operations Center Tasking Order.

4.5.1. If an individual in the organization discovers the event, initial notification should be sent to the head of their local activity and to the activity security manager, IAW DoDM5200.01v3_DAFMAN16-1404v3. Discovering unit reports suspected incident IAW current 616 Operations Center Tasking Order available on ESD. Organizations may use locally developed emergency response aids to inform users of the correct procedures. Contact the AF Network Mission Assurance Center for guidance.

4.5.2. IAW DoDM5200.01V3_AFMAN16-1404V3, sanitization software may be used for secret-level spills and below, after which the contaminated media can be re-entered into service. There is no approved overwriting or sanitization procedure for media that has been contaminated with top secret, SAP, or Sensitive Compartmented Information (SCI) data, short of physical destruction. However, such media may continue to be used if (re)classified at the higher level, where appropriate.

4.5.3. IAW CNSSP 11 and DoDI 8500.01, sanitization software must be listed on the NIAP PCL for (COTS) or evaluated and approved by the NSA (GOTS) and added to the enclave authorization package for cognizant AO approval IAW CJCSI 6510.01F Enclosure C. Certification and testing information must be provided for consideration during system or enclave ATO process.

4.5.4. If there is no sanitization software listed on the NIAP PCL or NSA approved, then a risk acceptance issued at the SAF level for the entire DAF or by the cognizant AO for their boundary is required. If there is no risk-accepted software for sanitization, the contaminated media must be either destroyed IAW NSA/CSS Policy Manual 9-12 or re-used at highest classification level.

4.6. Data Encryption. Encrypt sensitive information - e.g., CUI (includes and supersedes For Official Use Only), Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), Privacy Act, and Proprietary information. **(T-1)**.

4.6.1. Validate cybersecurity/cybersecurity-enabled IT products providing encryption according to DoDI 8500.01. **(T-1)**.

4.6.2. Verify that cybersecurity/cybersecurity-enabled IT products have been certified and listed on the NIAP/CCEVS website IAW CNSSP 11 (*see* **Table A.2–URLs**). **(T-1)**. The NIST and the NSA developed the Common Criteria program as part of the National Information Assurance Partnership, establishing an organizational and technical framework to evaluate the

trustworthiness of IT products and protection profiles. Cryptographic modules and algorithms are evaluated according to the NIST Cryptographic Algorithm Validation Program and the Cryptographic Module Validation Program. The Cryptographic Algorithm Validation Program provides validation testing of Federal Information Processing Standards-approved and NIST-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.

4.6.3. Follow additional guidance in United States Cyber Command (USCYBERCOM) Communications Tasking Order 08-001, *Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the DoD,* and the CNSSP No. 15, *Use of Public Standards for Secure Information Sharing.*

4.6.4. 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 NSA-approved cryptographic systems for classified data according to CJCSI 6510.01F, and National Security Systems (NSS) per CNSSP 15.

4.6.4.1. Use NIAP-validated products or NIST-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)**.

4.6.4.2. Ensure that sensitive DAF data managed on contractor owned resources is protected by encryption at rest and in transit, IAW this section.

4.6.5. Classified Data-At-Rest. Protect classified national security information at rest according to CJCSI 6510.01F using NSA-approved cryptographic and key management systems offering appropriate protection levels and approved for protecting classified data at rest.

4.6.6. Only approved universal serial bus removable media devices that have Federal Information Processing Standards (FIPS) certification under the NIST Cryptographic Module Validation Program for encryption (*see* **Table A.2–URLs**) are authorized for purchase and use on the AFIN; vendor information is available at the referenced NIST website. Classified removable media must meet the requirements established by the NSA's Commercial Solutions for Classified (CSfC). Capability Packages and the CSfC Components List can be found by visiting the CSfC Components List page. NIAP-validated products can be found at the NIAP Product Compliant List page (*see* **Table A.2–URLs**). Contact the NSA for approved implementation details at **CSfC@nsa.gov**.

4.7. Personally owned hardware and software. Processing of DoD information is limited to wired connections and authorized hardware and software. The use of Bluetooth® or other wireless connections and personally owned hardware and software is not authorized without a waiver approved by a cognizant AO, with mission justification **(T-0)**. The ISSM/Information System

Security Officer maintains approval and inventory documentation (except as noted in **paragraph 4.10.1**) between the user and government organization in the information system security authorization package.

4.7.1. Government Furnished Equipment (GFE) shall be used for official use and authorized purposes only according to DoDI1035.01_AFI36-816, *Civilian Telework Program* (renamed DoDI1035.01_AFI 36-143, *Telework Program*, per DAF Guidance Memorandum 2023-01)**.** Personnel may connect wired, personally owned basic computer peripherals (e.g., monitors, keyboards, mice, and headsets/headphones) to DAF-issued computers in telework environments connecting to unclassified DoD networks following the DAF and DoD guidelines. IAW DODI 8500.01, telework solutions involving the use of DoD-owned, government-furnished equipment for remote access will comply with the requirements of the applicable security controls defined in the authorization package. In a teleworking setting, users must establish a connection to the DoD network using approved methods such as virtual private networks or transport layer security. Users should only connect personally owned devices that are compliant with the Trade Agreement Act (TAA). For TAA compliance requirements, refer to **paragraph 3.5.4.1**. TAA compliance ensures the product was manufactured either in the United States or a designated country. To verify compliance, consult the "Look up Trade Agreements Act-designated countries" resource on the GSA website (*see* **Table A.2**). Users must provide this information to the cognizant ISSM.

4.7.2. The introduction of personally owned hardware, software, or both to an information system without cognizant AO approval is a violation of the information system user agreement and subject the user to repercussions outlined in the information system authorization package and may result in the loss of user access.

4.7.3. Do not introduce personally owned/developed software or connect personally owned Media, Internet of Things (IoT) devices, or peripherals with volatile or non-volatile memory (including, but not limited to wearable smart technology devices, smart appliances, tablets, e-readers, recording devices, Bluetooth®, other wireless devices, music/video compact disc/digital versatile disc, commercial portable media players, and universal serial bus drives) to either the DAF information systems or government furnished equipment. **(T-2)**.

4.7.4. Prior to the introduction of personally owned devices into classified processing areas, ensure compliance with DoDM5200.01V(x)_AFMAN16-1404V(x) Volumes 1-3, *Information Security Program*, AFI 17-101, Department of Defense Directive (DoDD) 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid*, and CJCSI 6510.01F. This applies to fitness monitors, wearable smart technology devices, smart appliances, Internet of Things devices, tablets, e-readers, recording devices (audio, video, etc.), Bluetooth®, and other wireless devices. Personable Wearable Devices (PWDs) may only be authorized to be in classified spaces by the Cognizant Security Authority (CSA) or cognizant AO, after consulting with the Certified TEMPEST Technical Authority (CTTA). **(T-0)**.

4.8. Wireless Services. Comply with DoDI 8500.01 and DoDD 8100.02 for wireless services (radio frequency and infrared) integrated with or connected to DAF information systems.

4.8.1. Implement wireless peripheral devices, including keyboard, mouse, Common Access Card reader, and pointer devices, according to requirements outlined in the DISA STIGs. Acquire wireless peripheral devices according to DAFMAN 17-1203.

4.8.2. Wireless capabilities in areas where classified information is discussed or processed require compliance with DoDM5200.01V(x)_AFMAN16-1404V(x) Volumes 1 and 2, *Information Security Program,* and DoDD 8100.02. Adhere to TEMPEST guidance within classified processing areas. The applicable AO is determined by considering each authorization boundary (reference AFI 17-101) impacted by the introduction of classified wireless capabilities into the classified processing area.

4.8.3. Configure wireless network solutions according to the DISA STIGs and CJCSI 6510.01F; document wireless configurations in the information system security authorization package for DAF Enterprise AO (or applicable AO if the wireless capabilities fall entirely within their boundary and do not touch the AFIN) approval according to DoDD 8100.02. **(T-1)**.

4.8.4. Configure all unclassified wireless peripheral devices (e.g., keyboards, mice, pointers/forwarders, handheld terminals, etc.) with Federal Information Processing Standards validated encryption modules according to CJCSI 6510.01F. **(T-0)**. Products that advertise compliance with Federal Information Processing Standards must provide the certification number.

4.8.5. Implement end-to-end data encryption for unclassified information over an assured channel and certify under the NIST Cryptographic Module Validation Program to meet requirements of Federal Information Processing Standards according to DoDD 8100.02. **(T-0)**. Secure classified information within NSA-approved encryption solutions according to CJCSI 6510.01F. *See* paragraph 4.6.4 and paragraph 4.6.5 for additional guidance. **(T-0)**.

4.8.5.1. 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 DAF Enterprise AO (or applicable AO if the wireless capabilities fall entirely within their boundary and do not touch the AFIN) **(T-2)**; see boundary specific appointment letters on the DoD Risk Management Framework Knowledge Service; URL is available at **Table A.2**. Navigate to the Collaboration tab and select Air Force from the Component Workspaces option.

4.8.5.2. Wireless infrared devices (i.e., infrared pointers and keyboards) require AO approval and inclusion in the system authorization package; for use in classified processing areas, implement applicable TEMPEST countermeasures. **(T-2)**.

4.9. 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 the DAF-managed networks through mobile access capabilities.

4.9.1. Configure and handle all devices according to applicable DISA Mobility STIG, Mobile Device Policy STIG (sunset), any updated/newly released mobile operating system STIG (e.g., Apple, Android, Windows Phone, etc.), and CJCSI 6510.01F. **(T-0)**. Obtain AO approval for all non-compliant Security Technical Implementation Guide configuration standards.

4.9.2. Prior to issuance of each commercial mobile device, the Commander’s Support Staff/Communications Focal Point/Client Support Technician verifies user compliance with the DISA DoD mobile devices (or its replacement) training (under Training Catalog, Cybersecurity Awareness at DoD Cyber Exchange website) or similar training module in the

DAF myLearning, the DAF's digital learning services technologies and operating environment when available (*see* **Table A.2–URLs**). Commercial mobile device users complete annual training according to DISA Mobility STIGs and SRGs.

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

4.9.4. Mobile computing devices within areas where classified information is discussed or processed require compliance with DoDM5200.01V(x)_AFMAN16-1404V(x) Volumes 1 and 2, and DoDD 8100.02. Adhere to TEMPEST guidance within classified processing areas. The applicable AO is determined by considering each authorization boundary (reference AFI 17-101) impacted by the introduction of the device into the classified processing area. This includes but is not limited to receive-only pagers, Global Positioning System receivers, hearing aids, pacemakers, and Telehealth Monitoring Devices. **(T-1)**.

4.9.5. 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)**. Encrypt classified data stored on secure (classified) mobile computing wireless devices using NSA-approved cryptographic and key management systems according to CJCSI 6510.01F. *See* paragraph 4.6 for additional guidance. **(T-0)**.

4.9.6. Users should immediately report any lost or stolen device to the issuing organization and system ISSM/Information System Security Officer, *see* DAFMAN 17-1203. Consult the applicable user guide or DAF Mobile website (URL is available at **Table A**) for guidance on remotely wiping lost or stolen commercial mobile devices and suspending the corresponding service plan.

4.9.7. 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/Blu-ray disc drives, power accessories, etc.) that may accompany the mobile computing device. **(T-1)**.

4.9.8. Non-Enterprise Activated Commercial Mobile Devices/cellular telephones acquired through the 771st ESS Enterprise Hardware Commodity Acquisition Programs are approved for use within the DAF for any non-sensitive unclassified DoD tasks. (For more information on IT asset procurement, refer to **paragraph 3.5.1**.). These 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)**.

4.9.8.1. Non-enterprise-activated commercial mobile devices/cellular telephone devices acquired through the 771st ESS Enterprise Hardware Commodity Acquisition Programs may not store and/or process classified information, CUI, PII, HIPAA, Privacy Act, and other sensitive information. **(T-1)**.

4.9.8.2. Configure government-owned non-enterprise-activated commercial mobile devices/cellular telephones according to the current DISA Security Technical Implementation Guide/Security Requirements Guide.

4.9.8.3. Track and manage all government-owned non-enterprise activated commercial mobile devices/cellular telephones according to DAFI 17-210, *Long Haul Radio Management,* and DAFMAN 17-1203.

4.9.9. Consult the current 616 Operations Center Tasking Order for handling, reporting, and sanitizing commercial mobile devices data spillage events involving classified CUI, PII, Privacy Act, and HIPAA data on government-issued and personally owned devices. **(T-1)**. *See* paragraph 4.5 for additional guidance.

4.9.10. When utilizing Mi-Fi or Wi-Fi hotspots, it is crucial to adhere to DoD policy as outlined in DODI 8420.01. WLAN client NICs must integrate AES-CCMP encryption within hardware, validated under the NIST Cryptographic Module Validation Program (CMVP) as meeting FIPS 140 standards. Regarding non-DoD unclassified WLAN systems, DoD employees or contractors must ensure compliance with DoDI 8420.01 standards and employ controls validated IAW the same directive as practical. When connected to a non-DoD WLAN, users must promptly establish a connection to the DoD network via approved methods such as virtual private networks or transport layer security. Additionally, users of non-DoD WLAN systems must implement controls in line with DoDI 8500.01, DoDI 1035.01, and DoDI 8582.01. If unable to enforce these controls, it is advised not to utilize the external WLAN system.

4.10. Peripheral Devices. A peripheral is any external device that provides input and/or output for a computing device. Input devices allow data such as text, images, video or sound to be entered into a computing device. Examples of 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); *see* **paragraph 4.12**.

4.10.1. Use of basic peripherals such as wired headsets, mice, and keyboards does not require individual authorization (i.e., in the system authorization package) as long as they are not programmable, do not contain persistent storage capabilities, and do not require additional software (excluding device drivers for devices procured through GSA AF Advantage). Refer also to the DAF Collaboration Peripherals supplemental memorandum, *Security Guidance for the use of Collaboration Peripherals and Capabilities in Secure Spaces*.

4.10.2. Non-basic peripherals such as wireless devices, cameras, and microphones usage on any information system requires documentation in the system authorization package. Use of collaboration peripherals in classified environments requires physical security countermeasures, TEMPEST countermeasures, or both. Refer also to the DAF Collaboration Peripherals supplemental memorandum.

4.10.3. Assistive Technology (“Section 508” devices). Assistive technology refers to a service or device that is used to increase, maintain, or improve the 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 AO’s office (or applicable cognizant AO’s Office) for authorization guidance. For more information, *see* AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508.*

4.10.3.1. Wounded Warrior Program. The Computer/Electronic Accommodations Program conducts needs assessments, procures and delivers assistive technology to

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

4.10.3.1.1. DoDI 6025.22 requires all Computer/Electronic Accommodations Program activities to meet applicable acquisition, confidentiality, privacy, security, and disclosure requirements according to DoDI 5400.11 and DoD 5400.11-R, *Department of Defense Privacy Program.* For more information, see the *Handbook for Providing Assistive Technology to Wounded Service Members*; URL is available at **Table A.2**.

4.10.3.1.2. The enclave or system ISSM may submit any non-cybersecurity/cybersecurity-enabled software to the Software and Application Certification Assessment (SACA) office (**ccc.saca@us.af.mil**) for certification; refer to AFI 17-101 for guidance on software assessment. Once certified (or if there is no software to certify), the ISSM in coordination with the Security Control Assessor (SCA) conducts a risk assessment to determine the overall impact on the enclave/system security posture and adds it to the information system/enclave security authorization package, providing a risk recommendation to the AO.

4.10.4. Configure multifunction devices and networked printers/scanners/plotters according to the DISA *Multifunction Device and Network Printers* Security Technical Implementation Guide. **(T-0)**. Only use NIAP-certified multifunction devices according to CNSSP No. 11 and DoDI 8500.01. **(T-0)**. Products available on the GSA AF Advantage website have been NIAP/CCEVS evaluated and certified (*see* **Table A.2–URLs**).

4.10.4.1. Refer to **paragraph 3.5.1** for guidance on procurement activities and specific acquisition programs.

4.10.4.2. Document, configure, and implement devices utilizing cybersecurity-enabled functions (e.g., scan to email/network drive) in the information system security authorization package for approval by the AO. **(T-1)**.

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

4.10.6. Software accepted by The Defense Information Systems Agency Joint Service Provider (DISA JSP) and documented on their Software Product List (SPL) is authorized for use within the DAF. Major Commands, Field Commands, and their equivalent can rely on the approval process conducted by DISA JSP to determine the suitability of adaptive technology software for use on the DAF Network. The DISA JSP SPL website contains the latest in approved software; URL is available at **Table A.2**. This reciprocity is appropriate for NIPRNet only.

4.10.7. Adaptive technology for information systems operating on other networks and classifications must be coordinated with the local ISSM(s), and appropriate AO.

4.10.8. Wing-level ISSMs, IT asset management equipment custodians, and Software License Managers (SLMs) must track all software and IT products acquired IAW DAFMAN 17-1203.

This includes maintaining accurate records of licenses, monitoring compliance, and ensuring proper tracking of usage and life cycle updates.

4.11. 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.).

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

4.11.2. Configure and manage all approved removable media devices according to all applicable DISA STIGs and CJCSI 6510.01F.

4.11.3. Protect removable media containing PII, HIPAA, Privacy Act, and CUI taken outside organizational networks according to CJCSI 6510.01F, DoDI 5200.48, *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)**.

4.11.3.1. The ISSM/Information System Security Officer informs users about data at rest requirements, ensuring stored information on removable media complies with the requirements outlined in **paragraph 4.6**.

4.11.3.2. Report any lost or stolen removable media containing CUI, HIPAA, PII, or Privacy Act information to the privacy monitor immediately, according to AFI 33-332, *Air Force Privacy and Civil Liberties Program.* **(T-0)**.

4.11.4. Ensure the proper classification, safeguarding, marking, labeling, storing, and transportation of all media IAW the requirements for the highest level of information ever contained on the media, as specified in DoDM5200.01v2_AFMAN16-1404v2 and DoDM 5200.01, Volume 2.

4.11.4.1. Ensure the destruction and disposal of removable media, to include flash media devices, according to DoDM5200.01V(x)_AFMAN16-1404V(x) Volumes 2 and 3, and DoDM 5200.01, Volumes 2 and 3, alongside protocols for remanence security; *see* Chapter 5.

4.11.4.2. Unclassified media introduced into a classified information system becomes classified according to CJCSI 6510.01F and the AF Enterprise AO (EAO) Memorandum, *Implementation Guidance for United States Cyber Command (USCYBERCOM) CTO 10-084 and CTO 10-133 and Manual Data Transfers Across Security Domains*, unless a DAF EAO-approved write protection mechanism or write protection process is used. Refer to the cognizant AO guidance for other DAF boundaries. (*see* **Table A.2–URLs**). **(T-2)**. Contact the DAF Cross Domain Support Element (**HQCCC.CZZE.CSNI-CDSE@us.af.mil**) for guidance on data transfers across security domains.

4.11.4.3. Disable "write" mechanisms for all forms of removable media on both SIPRNet and NIPRNet according to USCYBERCOM Communications Tasking Order 10-133, *Protection of Classified Information on DoD Secret Internet Protocols Router Network (SIPRNet)*, CNSSD 504 and CNSSP 26. **(T-0)**.

4.11.4.4. Organizations with a mission requirement to write to removable media submit requests for a waiver to the AO or alternate approving authority (e.g., Delta or Squadron Commander) according to current Data Loss Prevention TASKORD (*see* **Table A.2–URLs**).

4.11.4.5. Wing or Delta cybersecurity offices verify that organization commanders review all approved data loss prevention exemptions according to the current data loss prevention exemption TASKORD to validate the mission requirement. The system Information System Security Manager submits a request to remove the device/user account from the exemption when it is no longer required due to a change in mission, role, or assignment. Refer to the *Implementation Guidance for United States Cyber Command (USCYBERCOM) CTO 10-084 and CTO 10-133 and Manual Data Transfers Across Security Domains* memo (or its successor) on the DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**) for additional information.

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

4.11.4.7. System ISSMs validate the approved exemptions against the whitelist according to the current data loss prevention exemption TASKORD, verifying the removed devices/user accounts. Manually verify the removal of write capabilities on each device on systems unable to implement automated verification. See the latest TASKORD found on the DISPATCH website concerning data loss prevention exemptions for procedures and templates (*see* **Table A.2–URLs**).

4.11.5. 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)**.

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

4.11.7. Whitelist all approved external storage media (to include memory sticks, thumb drives, camera memory cards, digital cameras, smartphones, media players, external storage devices, flash media, and similar technologies) prior to connection via universal serial bus ports to AFIN systems. Submit the whitelist waiver according to the current Tasking Order and/or TASKORD found on the DISPATCH website (*see* **Table A.2–URLs**).

4.11.8. Removable flash media can be used with approval from designated authorities, and only USB devices with specific encryption certifications are permitted on the AFIN network; s*ee* paragraph 4.6.6.

4.11.9. Account for all removable media devices in the Defense Property Accountability System or the most current, mandated DAF IT inventory control system according to DAFMAN 17-1203.

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

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

4.12. Collaborative Computing. Collaborative computing provides an opportunity for a group of individuals, organizations, or both 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., Microsoft Teams, Global Video Service, SharePoint®, etc.) to prevent unauthorized users from seeing or

hearing national security information and material at another user's workstation area. Refer also to the DAF Collaboration Peripherals supplemental memorandum; *see* paragraph 4.10.

4.12.1. The system ISSM ensures the use of cameras/microphones in unclassified and classified environments is documented and approved in the information system security authorization package. Protect collaborative computing devices used in classified environments; *see* paragraph 4.2.

4.12.2. Configure webcams and attached microphones and control the projection of information viewable by webcams according to the DISA *Enterprise Voice, Video, and Messaging (EVVM) SRG*. 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 DISA *EVVM SRG*.

4.13. Contractor-Owned Information Systems. Contractor-owned hardware and software used to process DoD information on behalf of the DoD requires mission justification and AO approval, as required by DoDI 8510.01, DoDI 8010.01 and the Defense Information Systems Network (DISN) Connection Process Guide (CPG). Contractor-owned information systems implement security requirements for connection to the AFIN according to CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities,* and DoDM5200.01V(x)_DAFMAN16-1404V(x). Interconnection with the AFIN is accomplished according to DoDI 8510.01, DoDI 8010.01, the DISN CPG and configured using the appropriate DISA STIGs. Ensure that any foreign IT and services utilized by DAF are in compliance with current legal or policy acquisition prohibitions.

4.13.1. Externally owned information systems and platform IT systems that are dedicated to processing DoD information and are effectively under DoD configuration control require authorization, according to DoDI 8510.01, DoDI 8010.01 and the DISN CPG.

4.13.2. Off-base, non-DoD-owned facilities require the Defense Counterintelligence and Security Agency (DCSA) approval to process classified DoD information according to the *32* C.F.R. Pt. 117, *National Industrial Security Program Operating Manual (NISPOM),* DoDI 8510.01 and DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*.

4.13.3. On-base contractors within DAF-controlled facilities comply with the Federal Acquisition Regulation, Defense Federal Acquisition Regulation Supplement, and DoDI 4161.02, *Accountability and Management of Government Contract Property,* as required by contract.

4.13.4. ISSMs/Information System Security Officers/organizations maintain a listing of all contractor-owned or operated information system equipment within DAF facilities.

4.13.5. IAW DoDI 8010.01, DoD Components must "implement and register all connections to the DISN, including DoD Component and Mission Partner systems connected to DISN gateways, in the DODIN tracking and management repository IAW the DCPG." DISA currently implements this policy using the Defense Information Systems Agency (DISA) Systems/Network Approval Process (SNAP) database on NIPRNet and the SIPRNet GIAP System (SGS) database on SIPRNet to track connections to DISN (*see* **Table A.2–URLs**).

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

4.14. 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* CJCSI 6211.02D, CJCSI 6510.01F, and DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, for more information.

4.15. 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 AFIN as defined in AFI 17-101 and DoDI 8510.01. Follow reciprocity and reuse procedures according to DoDI 8510.01 and AFI 17-101. PPS registration for other Service or Agency-owned information systems will follow component-specific PPS guidance. Contact the applicable DoD Component PPSM Technical Advisory Group representative for assistance registering PPS for other Service or Agency information systems; find the DoD Component PPSM Configuration Control Board or Technical Advisory Group Representative contact list at the DoD PPSM website (*see* **Table A.2–URLs**).

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 (including 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, CJCSI 6510.01F, and NIST SP 800-88, Rev. 1, *Guidelines for Media Sanitization.*

5.1.1. DAF 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, ISSMs, Information System Security Officers, WCOs, 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, ISSMs, Information System Security Officers, Information System Owners, WCOs, 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 NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments.*

5.1.2.2. The Information System Security Officer, assisted by the WCO, assesses the risks in consultation with the Wing Information Protection Office before deciding whether to sanitize for reuse or disposal. See the current 616 Operations Center Tasking Order for guidance about reuse after Negligent Discharge of Classified Information sanitization actions. The AFIN Mission Assurance Center (AMAC) established the risk identification, management, and mitigation measures identified for Negligent Discharge of Classified Information events. The EAO memo addresses end-of-life, reclassification, sanitization software criteria, and handling of classified data on unclassified media within their boundary.

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, ISSM, 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 ISSM/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 the 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 memory, random access memory and read-only memory, optical disks, solid state drives, magnetic disks, and hard disk drives, etc.) are dependent upon the classification of data contained within the device.

5.2.1. Sanitization of unclassified devices follows NIST SP 800-88, Rev. 1. The term "sanitization" is defined in NIST SP 800-88, Rev.1 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 classified media requires 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 NSA/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 NSA Evaluated Products List or received approval from the NSA may be used to destroy classified information (to include media and devices) per NSA/Central Security Service Policy Manual

9-12. Contact the NSA/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, IT 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 IT storage media cannot be declassified by overwriting per DoDM5200.01v3_DAFMAN16-1404v3 and 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; versatile digital discs and Blu-Ray discs have information layers in the middle of the disc, 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 DoDM5200.01v3_DAFMAN16-1404v3 and DoDM 5200.01, Volume 3.

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 that does not contain sensitive data before reuse; purge media containing sensitive data prior to reuse. Reference NIST SP 800-88, Rev. 1. **(T-0)**.

5.3.2. Ensure removal of data from the 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., clear, or purge), rendering stored information unrecoverable. **(T-0)**

5.3.3. Clear classified media before reuse and reuse only in a classified environment according to CJCSI 6510.01F. Classified storage media may not be sanitized and declassified for reuse in an unclassified environment (*see* Enclosure C of CJCSI 6510.01F). **(T-0)**.

5.3.4. Devices involved in secret level spills and below may be reused at the original classification level if sanitized by an approved sanitization software, labeled as NDCI, and properly tracked; *see* **paragraph 4.5**. Otherwise, it must be either used at the higher classification level or destroyed IAW NSA/CSS Policy Manual 9-12. See the current 616 Operations Center Tasking Order.

5.3.5. Before media can be reused in a classified environment or released from organizational control, complete a separate administrative procedure for declassification. Refer to NSA/CSS Policy Manual 9-12 for declassification procedures. 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 DoDM5200.01v1_AFMAN16-1404v1, *Information Security Program: Overview, Classification, and Declassification,* and DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, or contact the system/enclave ISSM for a copy.

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 DoDM 4160.21, Volume 4, *Defense Materiel Disposition Manual: Instructions for Hazardous Property and Other Special Processing Materiel,* and DoDM 4160.21, Volume 2, *Defense Materiel Disposition Manual: Property Disposal and Reclamation.* **Note:** Disposal of records data on government hardware and software is per the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Unauthorized disposition of records data can result in a lost records incident per AFI 33-322 and may be reported to the National Archives and Records Administration (NARA).

5.4.1. Purge or destroy all unclassified information system storage media before leaving the control of the DoD, according to NIST SP 800-88, Rev. 1 and **paragraph 5.2.1**.. **(T-1)**.

5.4.1.1. Dispose of unclassified electronic media according to NIST SP 800-88, Rev. 1. Dispose of unclassified computing systems and hard drives according to DoDM5200.01v3_DAFMAN16-1404v3 and DoDM 5200.01, Volume 3, Enclosure 7. When no longer needed, unclassified computer systems and hard drives may be disposed of outside the DoD. In some circumstances, the equipment may be provided to non-government entities for reutilization. For devices involved in secret-level spill events and lower, ensure the device has been properly marked as NDCI and tracked, and destroyed upon reaching end of life. See the current 616 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 DoD, then transferred to other Federal agencies or donations to state/local

governments and other qualified organizations. The de-manufacture 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* **Table A.2–URLs**).

5.4.1.3. For unclassified information systems, track and dispose of storage media previously contaminated with classified data as classified media according to CJCSI 6510.01F. (**T-0**). Additionally, reference DoDM5200.01v3_DAFMAN16-1404v3 and DoDM 5200.01, Volume 3, Enclosure 3 for disposal and destruction guidelines. For classified information, follow the procedures outlined in NSA/Central Security Service Policy Manual 9-12 for destruction and declassification. Additionally, seek guidance from the DAF COMPUSEC Field Support office at **daf.compusec.field.support@us.af.mil** for document destruction procedures.

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 CJCSI 6510.01F and the sanitization/declassification procedures of NSA/Central Security Service Policy Manual 9-12 and **paragraph 5.2.2**. **(T-0)**. Follow DoDM 4160.21 Volumes 2 and 4 for de-manufacture (precious metals recovery) procedures. For installations without the means to sanitize or verify sanitization, the NSA does accept and will destroy some classified media. Follow the guidance on the NSA Classified Materiel Conversion for packaging, documenting, and shipping devices at NSA Classified Materiel Conversion (CMC) website (*see* **Table A.2–URLs**). 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. Hardware with multiple or mixed media types must be treated appropriately to ensure thorough sanitization. Follow the classification and sanitization methods outlined in the NSA/CSS Policy Manual 9-12 or NIST SP 800-88, Rev. 1 for each media type. Complete sanitization involves addressing all media within the device. Devices like computers, routers, switches, and multifunction devices may harbor diverse media types, necessitating tailored sanitization methods based on media type and operational environment classification. Most network architecture devices are equipped with solid-state storage devices such as random-access memory, read-only memory, field programmable gate array, smart cards, and flash memory. Specific sanitization protocols exist for 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.

Chapter 6

PORTS, PROTOCOLS, AND SERVICES MANAGEMENT

6.1. Introduction. Ports, Protocols, and Services (PPS) require association with the applicable hardware or software discovered during the PPS declaration activity during the risk management framework process. PPS used throughout AFIN require compliance with DoDI 8170.01, *Online Information Management and Electronic Messaging*. **(T-0)**. The declaration of PPS is based upon official business or AO-determined requirements. PPS registration in the DoD Ports, Protocols, and Services Management (PPSM) 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 ISSM. Except where specifically called out, ISSMs, 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 AO approves the use of PPS via the assessment and authorization process, and once the new system has been authorized, the ISSM requests registration. The authorization and registration process should be considered in mapping efforts for cyber mission relevant terrain.

6.1.2. Reauthorization of an existing system: The ISSM reviews the PPS, documents any changes, and requests an update to the existing PPS registration upon reauthorization.

6.1.2.1. Review boundary protection device rules annually, at a minimum, for compliance with CJCSI 6510.01F, DoDI 8551.01, and this manual. **(T-1).**

6.1.2.2. Monitor implementation of PPS based upon continuous monitoring guidance, IAW NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Step 6, Monitor Security Controls.

6.1.3. Modifications to the PPS registration: The requestor contacts the system ISSM to initiate a change request to modify the PPS for a registered system. The ISSM reviews the request, conducts a risk assessment, generates the security impact assessment, and submits a request to update the existing PPS registration, if applicable.

6.1.3.1. If the ISSM 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 ISSM follows DoDI 8510.01 for monitoring security controls if the residual risk adversely affects the security posture of the system.

6.1.3.2. Consult the DoD PPS Category Assurance List and PPS 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 ISSM; follow Methods and Procedures Technical Order 00-33A-1100.

6.1.4. Protect and regulate the use of PPS through interconnection agreements, access control mechanisms, and boundary protection devices according to DoDI 8551.01, Cybersecurity Service Provide (CSSP), internal cybersecurity, and this manual.

6.1.4.1. Applications and platform IT 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 PPSM Tracking Identifier for each information system. **(T-1).**

6.2. Ports, Protocols, and Services Management. PPS for information systems connecting to, operating on, or traversing across the AFIN follow policies to catalog, regulate, and control their use based on vulnerabilities and risk. Approval for the use of PPS by an information system only occurs through the risk management framework process, according to AFI 17-101. The ISSM has the responsibility of ensuring that the PPS used by the information system is compliant with DoD PPSM policies. **(T-0)**.

6.2.1. Limit the use of PPS 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 PPS within the authorization boundary of the information system according to the following conditions:

6.2.2.1. Associate the PPS with hardware and software listed in the component inventory for the information system.

6.2.2.2. Attribute the ports, protocols, and services to each network service "listening" for client connection on only the necessary TCP/UDP ports, if possible, 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, including the PPS, 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 PPS within the authorization boundary of the information system do not duplicate the PPS under the control and cognizance of another DoD information system.

6.2.2.6. Use the DAF *PPSMBI Workbook* to document these communications interfaces. This document will serve as an artifact for the risk management framework and document compliance with DoD PPSM standards.

6.2.2.7. PPS documentation must be consistent with functional dataflow diagrams and network topology diagrams. **(T-1).**

6.2.3. Implement PPSM standards for software and hardware using the DoD PPSM Category Assurance List and applicable DoD PPS Vulnerability Assessment reports available from the DoD Cyber Exchange Category Assurance List; URL is available at **Table A.2**. **(T-0)**.

6.2.3.1. The use of PPS not listed on the DoD PPSM Category Assurance List (e.g., no applicable DoD PPS Vulnerability Assessment Report) is not authorized and does not comply with DoD policy requiring risk assessment. Follow the applicable DoD process for Component Local Service Assessment (CLSA) or risk assessment and PPS guidance on

the DAF Cybersecurity Collaborative Environment for documenting and assessing the vulnerabilities for the use of these unknown and/or unevaluated PPS.

6.2.3.2. Changes to published DoD PPS Vulnerability Assessment reports require supporting documentation, review, and approval. **(T-0)**. Follow the guidance on the DAF Cybersecurity Collaborative Environment for PPS to submit requests for changes to the Vulnerability Assessment reports issued by DoD.

6.2.4. After approval from an AO, the PPS registration actions formally declare the use of the PPS for the associated information system within DoD-level databases available to all DoD Components.

6.2.4.1. Registration enables the regulation and control of PPS 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 PPS using eMASS workflow process (*see* **Table A.2–URLs**). PPS registrations will be managed through the RMF Step 3/Step 5 or IATT workflows.

6.2.4.3. Upon successful registration, each information system receives a unique, 9-character alpha-numeric DoD PPSM Tracking Identifier. PPSM 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 PPS registration for an information system should follow the configuration management plans, security impact assessment processes, and continuous monitoring activities for the information system under the risk management framework, *see* AFI 17-101.

6.2.4.5. Registration confirmation notices and the PPS details generated from the DoD PPSM 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 PPS associated with interconnected information systems according to the following conditions:

6.2.5.1. Applies to PPS 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 PPS do not exist within the authorization boundary of the subject information system since the hardware and software fall under the configuration control of a different Information System Owner.

6.2.5.2. Verify all PPS within the authorization boundary of the information system do not duplicate the PPS under the control and cognizance of the interconnected information systems. Only one information system may declare the "listening" service or service of hardware and/or software based on 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 the risk management framework.

6.2.6. Exceptions to DoD PPSM standards follow the DoD PPSM Exception Management Process and guidance on the DAF Cybersecurity Collaborative Environment for PPS.

6.2.6.1. Exceptions apply to the use of a PPS already evaluated by DoD PPSM with deviations to the standards specified in the applicable DoD PPS Vulnerability Assessment report. This process provides the Information System Owner with the ability to use non-standard PPS based upon an operational need. The DoD PPSM 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 DAF Cybersecurity Collaborative Environment, submission of the exception request will use the eMASS workflow process (*see* **Table A.2–URLs**).

6.2.6.3. Any exceptions under the purview of USCYBERCOM must first follow the DoD PPSM Exception Management Process (*see* **Table A.2–URLs**). **(T-0)**.

6.2.7. For time-sensitive operational interoperability in support of operations with limited duration, Information System Owners and AOs may request temporary use of PPS not listed on the DoD PPSM Category Assurance List according to DoDI 8551.01. Follow the DoD PPSM Exception Management Process and PPS guidance on the DAF Cybersecurity Collaborative Environment.

6.2.8. Records in the DoD PPSM Registry require review on an annual basis, at a minimum, to validate system information, points of contacts, and ensure that all communications interfaces remain accurate and up to date. Failure to keep records current will result in removal from the DoD PPSM 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 AO approval for the information system, connection authorization, and DoD PPS registration. **(T-0)**.

6.2.9.2. Changes to rules under the applicability of DoDI 8551.01 require the DoD PPS 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 PPS, follow the guidance in the DISA Cloud Computing Security Requirements Guide and procedures on the DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**).

6.2.11. Information systems with a public component, a public-facing presence, or Internet-facing applications require review and approval through the DoD DMZ whitelist process. Follow the guidance on the DAF Cybersecurity Collaborative Environment (*see* **Table A.2–URLs**).

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

6.4. Ports, Protocols, and Services Declaration. Implement PPS according to DoD PPS standards using the applicable DISA STIGs, DoD PPS Category Assurance List, DoD PPS Vulnerability Assessment reports, and DAF Component Local Service Assessments. **(T-0)**. Additional requirements may be provided via JFHQ-DODIN, USCYBERCOM, and Sixteenth Air Force (Air Forces Cyber) tasking orders or other directives as situations arise.

6.4.1. Comply with CJCSI 6211.02D for "tunneling" across the AFIN and ensure declaration of the PPS to include PPS within the tunnel. **(T-0)**.

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

6.4.1.2. PPS documentation and associated PPS registration must declare the PPS required to establish the tunnel and also the PPS used within the tunnel pursuant to the purposes and applicability of DoDI 8551.01. **(T-0)**.

6.4.2. PPS associated with information system connections by mission partners require compliance with DoDI 5530.03, *International Agreements,* and Approval to Connect guidance in AFI 17-101.

6.4.2.1. Mission partner information systems require a DoD PPSM Tracking Identifier for operation on, operation through (e.g., encrypted tunnels), and/or connection to the AFIN. For more information about mission partner environments, *see* DoDI 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 PPS within an enclave or hosting environment. **(T-2)**.

6.4.3. Declare PPS on the Air Force *PPSMBI workbook* available in eMASS under the help menu.

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, Protocols, and Services Registration. Registration of PPS occurs after authorization of the system. Once registered, a PPSM 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. PPS 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 a Non-classified Internet Protocol Router Network to any other network including 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 DMZ to include computers on the Internet connecting to any computer on the *.mil* domain.

6.5.2. PPS 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, Protocols, and Services Review. Review mandated changes to PPS security measures (i.e., USCYBERCOM orders, DoD PPSM Configuration Control Board results) and determine impact, compliance, and remediation actions for the applicable PPS 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, Protocols, and Services Updates/Change Management. PPS updates require a current authorization for the system and a DoD PPSM Tracking Identifier that indicates the system has been registered. Coordinate all updates, modifications, additions, and deletions through the system ISSM. See the Air Force Change Process guidance on MilSuite and the AF-PPS Wiki; URLs available at **Table A.2**.

6.8. Decommissioning Strategy. Include PPS 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 PPSM Registry, coordination with the Cybersecurity Service Provider and/or hosting environment to remove associated boundary protection device rules, and the termination of PPS exceptions for the system. **(T-1).**

Chapter 7

APPROVED MOBILE DEVICE

7.1. Individuals shall not place DoD Controlled Unclassified Information on a personal mobile device except as part of a SAF/CN AMD (formerly known as BYOAD) program. AMD is a device- and Operating System-agnostic mobile solution that enables a user with a personally owned device to securely access government information while maintaining user privacy. Government information is maintained either in a managed container stored on the device or in a virtual machine within a Zero Trust, unmanaged, containerized app that keeps the user's personal data separate from government data. When using an unmanaged solution, the government cannot access the user's personal data and apps, and in the event of a spillage, the user's personal device does not have to be confiscated or wiped; it is just where the app displaying the virtual machine is installed. **(T-1)**. To establish or locate an AMD program, DAF personnel should initiate the process through their respective WCO.

7.2. A SAF/CN-approved AMD program: Will have EITHER a Mobile Device Management (MDM) technical solution that provides a Managed Mobile Service (MMS) OR a Zero Trust-based VMI solution, enabling user access to Unclassified DOD Information while ensuring separation from personal information, and when removed will not impact personal information. **(T-1)**. If using an MDM solution, the MMS mandates personally-owned mobile devices that access DoD information and/or DoD IS:

7.2.1. Must be managed and configured IAW appropriate STIGs and Security Recommendation Guides, monitored by an MMS, and validated against appropriate NIAP Protection Profile(s). **(T-0)**.

7.2.2. Must have an Authority to Operate (ATO) by an AO, accomplished per the requirements and process in AFI 17-101; *see* **paragraph 1.3**. Mobile devices and solutions without an ATO cannot be used until they obtain an ATO. **(T-0)**.

7.2.3. Must ensure automated monitoring, compliance, and validation mechanisms are implemented by the MMS to ensure security/configuration settings of AMD 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-0)**.

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-0)**.

7.2.5. Must monitor for violations of defined rules such as violations of application whitelists, Subscriber Identification Module (SIM) changes, and roaming state changes. **(T-0)**.

7.2.6. Must validate the device is running the latest approved Operating System/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 the capability to provide reports on the number of users to SAF/CN every six months. **(T-1)**.

7.3. The AMD program is: Voluntary and for the employee's convenience, not a cost-saving measure. It is not a substitute for government devices, and employees cannot have both a device participating in the AMD program and a government device simultaneously, as this policy also aims to improve compliance with the Clinger-Cohen Act by reducing duplicative services. **(T-0)**.

7.4. All Users who choose to participate in the program must comply with the terms of both the DAF Form 4433 and DAF Form 4394 User Agreements that are signed. Failure to observe this paragraph (7.4) by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92(1), Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action IAW DAFI 36-147 without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. **(T-0)**.

7.5. All users must: Follow the approved process for obtaining and deleting the MMS OR VMI solution as outlined by SAF/CN, including completing the user training. **(T-0)**.

7.6. Failure to observe the following 7.6 subparagraphs by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92(1), Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action IAW DAFI 36-147, without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contactor personnel may be handled according to applicable laws and the terms of the contract. **(T-0)**.

7.6.1. All users who participate in this program shall only use a device for the AMD program that is validated and certified NIAP compliant or is both part of a pre-existing NIAP compliant device family and is undergoing NIAP product evaluation for trusted device status. **(T-0)**.

7.6.2. Only the aforementioned devices may be used to participate in the AMD program to ensure the separation and protection of DOD information. Devices that fail to achieve trusted device NIAP-compliant status are not eligible for AMD program use. The NIAP Product Compliant List and NIAP Product in Evaluation List can be found at the NIAP website (*see* **Table A.2–URLs**). For the AMD VMI program, the list of approved mobile hardware devices and associated operating systems and Windows patch levels is updated frequently and is located in **Table A.2–URLs** listed as VMI Approved Device and Operating System. **(T-0)**.

7.6.3. Has device-unlock passcode, Personal Identification Number (PIN), or biometric access control enabled on the device. **(T-0).**

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 and Certified Technical TEMPEST Authority (CTTA). **(T-0).**

VENICE M. GOODWINE, SES, DAF
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 U.S.C.

10 U.S.C. 4862.

10 U.S.C. 2533a, *Requirement to Buy Certain Articles from American Sources; Exceptions*.

29 U.S.C. 201 – 219 (75 Pub. L. 718, 52 Stat. 1060, *Fair Labor Standards Act of 1938*, as amended).

37 C.F.R. Part 117.

FAR Subpart 25.1, *Buy American – Supplies,* 25.103 *Exceptions,* current edition.

DFARS Part 225 – *Foreign Acquisition,* Subpart 225.1, *Buy American – Supplies,* 225.103 *Exceptions,* current edition.

DoD PPSM CAL, *Ports, Protocols, and Services Management Category Assurance List (See* the latest CAL found at DoD Cyber Exchange).

DoDD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* 7 November 2023.

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid,* 23 April 2007.

DoDD 8140.01, *Cyberspace Workforce Management*, 5 October 2020.

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

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

DoDI 5400.11, *DoD Privacy and Civil Liberties Programs,* 29 January 2019.

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

DoD 5500.7-R, *Joint Ethics Regulation (JER),* 15 May 2024.

DoDI 5530.03, *International Agreements,* 4 December 2019.

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

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

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

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

DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD,* 30 June 2021.

DoDI 8170.01, *Online Information Management and Electronic Messaging*, 24 August 2021.

DoDI 8310.01, *Information Technology Standards in the DoD*, 31 July 2017.

DoDI 8500.01, *Cybersecurity*, 7 October 2019.

DoDI 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022.

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*, 31 May 2023.

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

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

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

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information*, February 24, 2012.

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, February 24, 2012.

DoDM 5205.07, Volume 1, *Special Access Program (SAP) Security Manual: General Procedures*, June 18, 2015.

DoDM 5205.07, Volume 2, *Special Access Program (SAP) Security Manual: Personnel Security*, 24 November 2015.

DoDM 5205.07, Volume 3, *Special Access Program (SAP) Security Manual: Physical Security*, 23 April 2015.

DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program*, 15 Feb 2023.

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

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

DoDI 1035.01_AFI 36-816, *Civilian Telework Program*, 29 October 2018

DODI 1035.01_DAFI 36-143, *Telework Program*, 12 February 2024

DAFI 17-210, *Long Haul Radio Management*, 31 July 2023.

DAFI 31-101, *Integrated Defense (ID)*, 11 April 2023.

DAFI 36-147, *Civilian Conduct and Responsibility*, 11 January 2023.

DAFI 36-148, *Discipline and Adverse Actions of Civilian Employees*, 27 September 2022.

DAFI 63-101/20-101, *Integrated Life Cycle Management*, 16 February 2024.

DAFI 90-160, *Publications and Forms Management*, 14 April 2022.

DAFI 90-302, *The Inspection System of the Department of the Air Force*, 5 October 2023.

DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability*, 13 September 2022.

DAFMAN 17-1304, *Identity, Credential, and Access Management (ICAM),* 28 December 2023.

DAFMAN 17-1305, *Cyberspace Workforce Management*, 7 June 2024.

DAFMAN 90-161, *Publication Processes and Procedures,* 18 October 2023.

DAFMAN DoDM5200.01V1_AFMAN16-1404V1, Volume 1, *Information Security Program: Overview, Classification, and Declassification,* 06 April 2022.

DAFMAN DoDM5200.01V2_AFMAN16-1404V2, Volume 2, *Information Security Program: Marking of Classified Information,* 07 January 2021.

DAFMAN DoDM5200.01V3_DAFMAN16-1404V3, Volume 3, *Information Security Program: Protection of Classified Information,* 12 April 2022.

DAF Zero Trust Strategy, DAF CIO, 14 June 2024.

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

AFI 10-701, *Operations Security (OPSEC),* 23 July 2019.

AFI 17-101, *Risk Management Framework (RMF) for the Department of the Air Force Information Technology (IT),* 06 Feb 2020.

AFI 17-130, *Cyber Security Program Management,* 13 February 2020.

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

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

AFI 33-393, *Electronic and Information Technology Accessible to Individuals with Disabilities Section 508,* 3 July 2019.

AFI 38-206, *Additional Duty Management*, 3 April 2020.

AFMAN DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* 8 May 2020

AFMAN 17-1302-O, *Communications Security (COMSEC) Operations*, (CUI), 9 April 2020.

AFMAN 17-1402, *Cyberspace, Clinger-Cohen Act (CCA) Compliance,* 20 June 2018.

AFMAN 17-2101, *Long-Haul Communications Management,* 22 May 2018.

AFSSI 7700, *Emission Security*, October 24, 2007.

AF Enterprise AO Memorandum *Combined Implementation Guidance for USCYBERCOM CTO 10-084 and 10-133 Memorandum,* 16 December 2013.

AF Enterprise AO Memorandum, *Guidance for Manual Data Transfers Across Security Domains,* 11 October 2022.

AF SIPR Write and Manual Cross Domain Transfer Memorandum (for AF enterprise users), *Implementation Guidance for United States Cyber Command (USCYBERCOM) CTO 10-084 and CTO 10-133 and Manual Data Transfers Across Security Domains*, 11 October 2022.

DAF Collaboration Peripherals (supplemental) memorandum, *Security Guidance for the use of Collaboration Peripherals and Capabilities in Secure Spaces*, 10 February 2022.

SORN: F017 SAF CN A, *Bring Your Own Approved Device (BYOAD)*; 85 FR 19932, April 9, 2020.

CNSSD 504, *Directive on Protecting National Security Systems from Insider Threat*, 30 September 2016.

CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, 2 March 2022.

CNSSP No. 15, *5. National Security Agency (NSA)-approved cryptography will be used to protect NSS,* 20 October 2016.

CNSSP No. 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems*.

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

CNSSP No. 15, *Use of Public Standards for Secure Information Sharing,* 20 October 2016.

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

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

DISA *Application Security and Development* Security Technical Implementation Guide (cyber.mil).

DISA *Keyboard Video and Mouse Switch* Security Technical Implementation Guide (cyber.mil).

DISA *Multifunction Device and Network Printers* Security Technical Implementation Guide (cyber.mil).

DISA *Enterprise Voice, Video, and Messaging (EVVM) Security Requirements Guide (SRG)* (cyber.mil).

DISA *Traditional Security Technical Implementation Guide*, V-245822.

DoD Joint Special Access Program (SAP) Implementation Guide (JSIG), 11 April 2016.

DoD Memorandum: *Revised Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments*, 05 June 2020.

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

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010.

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

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

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

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

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems, and Organizations,* 30 September 2011.

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments,* September 2012.

NIST SP 800-41, Revision 1, *Guidelines on Firewalls, and Firewall Policy,* 28 September 2009.

NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, 20 February 2007.

NIST SP 800-46, Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* July 2016.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* September 2020.

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

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

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

USCYBERCOM CTO 10-133, *Protection of Classified Information on Department of Defense (DoD) Secret Internet Protocols Router Network (SIPRNet),* 27 November 2010.

Prescribed Forms

DAF Form 4433, *The Department of the Air Force Mobile Device User Agreement*

DAF Form 4394, *The Department of the Air Force User Agreement Statement - Notice and Consent Provision*

Adopted Forms

DD Form 2987 (DD2987), *Computer/Electronic Accommodations Program (CAP) Accommodation Request*

DAF Form 847 (DAF847), *Recommendation for Change of Publication*

Abbreviations and Acronyms

AES—Advanced Encryption Standard

AF—Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFMAN—Air Force Manual

AFNet—Air Force Network

AFR—Air Force Reserve

AFSSI—Air Force Systems Security Instruction

AMAC—Mission Assurance Center

AMD—Approved Mobile Device

ANG—Air National Guard

AO—Authorizing Official

AT—Assistive Technology

ATO—Authorization to Operate

BYOAD—Bring Your Own Approved Device

BYOD—Bring Your Own Device

CAP—Computer/Electronic Accommodations Program

CCA—Clinger-Cohen Act

CCEVS—Common Criteria Evaluation and Validation Scheme

CCS-3—Client Computing Solutions III

CIO—Chief Information Officer

CISA—Cybersecurity and Infrastructure Security Agency

CISO—Chief Information Security Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CCTL—Common Criteria Testing Laboratories

CLSA—Component Local Service Assessment

CND—Computer Network Defense

CNSS—Committee on National Security Systems

CNSSD—Committee on National Security Systems Directive

CNSSI—Committee on National Security Systems Instruction

CNSSP—Committee on National Security Systems Policy

COMPUSEC—Computer Security

COMSEC—Communications Security

CORA—Cyber Operational Readiness Assessment

COTS—Commercial Off-The-Shelf

CSA—Cognizant Security Authority

CSE—Cyber Security Event

CSS—Central Security Service

CSSP—Cybersecurity Service Provide

CTO—Communications Tasking Order

CTTA—Certified TEMPEST Technical Authority

CUI—Controlled Unclassified Information

DAA—Designated Accrediting Authority

DAF—Department of the Air Force

AFIN—Department of the Air Force Information Networks, which includes all DAF, AF and USSF networks.

DAFMAN—Department of the Air Force Manual

DAFPD—Department of the Air Force Policy Directive

DAR—Data at Rest

DCSA—Defense Counterintelligence and Security Agency

DISA—Defense Information Systems Agency

DISA JSP—Defense Information Systems Agency Joint Service Provider

DISN—Defense Information Systems Network

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDIN—Department of Defense Information Network

DoDM—Department of Defense Manual

EAO—Enterprise Authorizing Official

EVVM—Enterprise Voice, Video, and Messaging

eMASS—Enterprise Mission Assurance Support Service

FIPS—Federal Information Processing Standards

GFE—Government Furnished Equipment

GIG—Global Information Grid

GOTS—Government Off-The-Shelf

HIPAA—Health Insurance Portability and Accountability Act

HQ—Headquarters

IA—Information Assurance

IAW—In Accordance With

ICAM—Identity, Credential, and Access Management

ID—Integrated Defense

IoT—Internet of Things

IP—Internet Protocol

ISCM—Information Security Continuous Monitoring

IS—Information System

ISSM—Information Systems Security Manager

ISSO—Systems Security Officer

ITAM—Information Technology Asset Management

IT—Information Technology

JFHQ—Joint Force Headquarters

JFHQ-DODIN—Joint Force Headquarters–Department of Defense Information Network

JITC—Joint Interoperability Test Command

JSIG—Joint Special Access Program (SAP) Implementation Guide

KVM—Keyboard Video Mouse

MDM—Mobile Device Management

MICT—Management Internal Control Toolset

MMS—Managed Mobile Service

MPE—Mission Partner Environment

MPTO—Methods and Procedures Technical Order

NDCI—Negligent Discharge of Classified Information

NIAP—National Information Assurance Partnership

NIPRNet—Non-classified Internet Protocol (IP) Router Network

NISPOM—National Industrial Security Program Operating Manual

NIST—National Institute of Standards and Technology

NSA—National Security Agency

OPR—Office of Primary Responsibility

OPORD—Operational orders

OPSEC—Operations Security

OS—Operating System

OTA—Over-The-Air

PCL—Product Compliant List

PII—Personally identifiable information

PIN—Personal Identification Number

POA&M—The Plan of Action and Milestones

PPS—Ports, Protocols, and Services

PPSM—Ports, Protocols, and Services Management

PPSMBI—Ports, Protocols and Services Management Boundaries Information

PPSM-C—Ports, Protocols, and Services for Classified Systems

PPSM-U—Ports, Protocols, and Services for Unclassified Systems

PWDs—Personable Wearable Devices

RMF—Risk Management Framework

SACA—Software and Application Certification Assessment

SAC—Self-Assessment Checklists

SAP—Special Access Program

SCA—Security Control Assessor

SCI—Sensitive Compartmented Information

SES—Senior Executive Service

SGS—SIPRNet GIAP System

SHS—Secure Hash Standard

SIM—Subscriber Identification Module

SLM—Software License Managers

SIPRNet—Secret Internet Protocol Router Network

SNAC—System and Network Analysis Center

SORN—System of Record Notice

SP—Special Publications

SPL—Software Product List

SRGs—Security Requirements Guides

STIGs—Security Technical Implementation Guides

TAA—Trade Agreement Act

TASKORD—Tasking Order

UCMJ—Uniform Code of Military Justice

UC—Unified Capabilities

UDCI—Unauthorized Disclosure of Classified Information

USAF—United States Air Force

USCYBERCOM—United States Cyber Command

USSF—United States Space Force

VMI—Virtual Mobile Infrastructure

WCO—Wing Cybersecurity Office

WIPO—Wing Information Protection Office

Office Symbols

ACC—Headquarters Air Combat CommandACC/A6—Communications Directorate

ACC/CCC—Cyberspace Capabilities CenterSAF/CN—Department of the Air Force Chief Information Officer

SAF/CNZ—Department of the Air Force Office of Chief Information Security Officer

SpOC—Space Operations Command

DEL 6—Space Force Delta 6

Sixteenth Air Force (16AF)—Air Forces Cyber (AFCYBER)

Terms

Air Force Information Network (AFIN)—The DAF provisioned portion of the Department of Defense Information Network (DoDIN). The AFIN is defined as the globally interconnected, end-to-end set of Air Force information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policymakers, and support personnel, including owned, leased, and contracted communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. The terms AF Network (AFNET) and AF Network-Secure (AFNET-S) are introduced to refer to the Air Force's underlying Non-Secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). (AFPD 10-17 and AFI 10-1701).

DAF IT—" . . . is any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services, and related resources). IT is equipment used by the DoD directly or is used by a contractor under a contract with the DoD that requires the use of that equipment. IT does not include any equipment acquired by a federal contractor incidental to a federal contract." (AFMAN 17-1402, paragraph 3.1.1).

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. (DoDM 8140.03).

Classified information—See classified national security information.

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 or different security category. Spillage encompasses this term. (CNSSI No. 4009).

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.). (DoDM5200.01v1_AFMAN16-1404v1).

Classified national security information—Information that has been determined pursuant to Executive Order (E.O.) 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. (E.O. 13526)

Clear—A method of sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; 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). (CNSSI No. 4009).

Collaborative Computing—Applications and technology (e.g., whiteboarding, group conferencing) that allow two or more individuals to share information in real-time in an inter- or intra-enterprise environment. (CNSSI No. 4009).

Common Criteria—Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (CNSSI No. 4009).

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

Computer security (COMPUSEC)—Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer. Term has been replaced by the term "cybersecurity". (CNSSI No. 4009).

Countermeasures—Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (CNSSI No. 4009).

Controlled unclassified information (CUI)—Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. **Note:** The CUI categories and subcategories are listed in the CUI Registry. (CNSSI 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. **Note:** The term cybersecurity replaced the term information assurance (IA) in the DOD and most USG policy documents in 2014.The term information assurance, in turn, previously replaced the terms information security and computer security in the same way. However, the terms information security and computer security are still used in the USG and elsewhere depending on scope and intent. (CNSSI No. 4009).

Cybersecurity—enabled Information Technology Product— A product or technology whose primary role is not security, but that provides security services as an associated feature of its intended operating capabilities. To meet the intent of Committee on National Security Systems Policy (CNSSP) 11, acquired CS-enabled products must be evaluated if the CS features are going to be used to perform one of the security services (availability, integrity, confidentiality, authentication, or nonrepudiation). **Note:** Examples include such products as security-enabled web browsers and screening and security-enabled messaging systems. (CNSSI No. 4009).

Cybersecurity IT product—A product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, nonrepudiation of data), correct known vulnerabilities, or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.

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

Data Spillage—Security incident that results in the transfer of classified information or Controlled Unclassified Information onto an information system not authorized to store or process that information. (CNSSI No. 4009).

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

Degauss—1. To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. (NIST SP 800-88, Rev. 1). 2. Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. (NSA/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 is inserted as a "neutral zone" between an organization's private network and the Internet. (NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*). 3. 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. (NIST SP 800-41, Rev. 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. (NIST SP 800-88, Rev. 1).

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, policymakers, 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).

Device Family—Includes all versions of a single make and model device. Example – Apple ®, iPhone ®.

Information systems—" . . . as defined in 44 U.S.C. § 3502, are a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." (AFMAN 17-1402, paragraph 3.1.3)

Mobile Code—Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. (CNSSI No. 4009).

Mobile code technologies—Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). (NIST SP 800-53, Rev. 5).

Mobile Device—A portable computing device that has a small form factor such that:

it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, nonremovable/removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features that synchronize local data with remote locations. Examples include smartphones, tablets, and E-readers. Also known as a "portable computing device." **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. (CNSSI No. 4009).

National Security Systems— ". . . as defined in 44 U.S.C. § 3552, are telecommunications or information systems operated by or on behalf of the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or, is critical to the direct fulfillment of military or intelligence missions. National Security Systems do not include systems that are used for routine administrative and business applications (including payroll, finance, and personnel management applications)." (AFMAN 17-1402, paragraph 3.1.2).

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).

Non-repudiation—Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. (NIST SP 800-53, Rev. 5).

Overwriting—The process of writing data on top of the physical location of data stored on the media. (NIST SP 800-88, Rev. 1).

Personally identifiable information—Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Portable storage device—A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory). (CNSSI No. 4009).

Privilege—A right that, when granted to an entity, permits the entity access and/or authorization to an otherwise restricted object, state, or resource. **Note:** Privileges represent the authorized behavior of a subject. They are defined by an authority and embodied in policy or rules. (CNSSI No. 4009).

Privileged account—A system account with authorizations of a privileged user. (CNSSI No. 4009).

Privileged user—A user that is authorized (and therefore, trusted) to have access to perform system control, monitoring, administration functions, or security-relevant functions that ordinary users are not authorized to perform. (CNSSI No. 4009). Privileged users have the same requirements as authorized users but have additional permissions to configure information assurance– enabled software products and systems. These users must hold baseline commercial certifications according to DoDM 8140.03 and be placed in unit manning documented positions that require privileged access. (DoDI 8500.01).

Remanence—Residual information remaining on data media after clearing. See *Clear* (CNSSI No. 4009).

Remote Access—The ability for an organization’s users to access its non-public computing resources from external locations other than the organization’s facilities. (NIST SP 800-46, Rev. 2).

Removable Media—Portable data storage medium that can be added to or removed from a computing device or network. **Note:** Examples include, but are not limited to: optical discs; external/removable hard drives; external/removable solid-state disc drives; magnetic/optical tapes; flash memory devices; flash memory cards; and all other external/removable disks. (CNSSI No. 4009).

Removable media device—See portable storage device.

Sanitization—See sanitize.

Sanitize—1. A process to render access to target data on the media infeasible for a given level of effort. Clear, Purge, Damage, and Destroy are actions that can be taken to sanitize media. 2. The removal of extraneous or potentially harmful data (e.g., malware) within a file or other information container (e.g., network protocol packet). 3. 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. (CNSSI No. 4009).

Sensitive Information—See controlled unclassified information.

Spillage—Security incident that results in the transfer of classified information or Controlled Unclassified Information onto an information system not authorized to store or process that information. (CNSSI No. 4009).

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

Telework—The ability for an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities. (NIST SP 800-46, Rev. 2).

Tunneling—Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. (CNSSI 4009-2015).

TEMPEST—A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. (CNSSI No. 4009).

Vulnerability—1. A known weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system-resulting in a security incident or a violation of the system's security policy. 2. Characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation. (CNSSI No. 4009).

Weakness—An attribute or characteristic that may, under known or unknown conditions, render an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

Whitelist—A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline. **Note:** Whitelist is also known as "allow list/allowlist." (CNSSI No. 4009).

Whitelisting—A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites. **Note:** Whitelisting is also known as "allow listing/allowlisting." (CNSSI No. 4009).

Attachment 2

REFERENCE UNIFORM RESOURCE LOCATORS (URLS)

Table A.2. List of referenced URLs

616 Operations Center Tasking Order	**https://esd.us.af.mil/ESDPortal/DocFrame.aspx?DOCID=TASKORD-22-20221625**
AF PPS Wiki	**https://usaf.dps.mil/teams/IACE/Wiki/AF%20PPS.aspx**
Air Force Change Process Guidance on MilSuite	https://milsuite.mil/wiki/Air_Force_Change_Process
Air Force e-Publishing Website	**https://www.e-publishing.af.mil/**
Air Force Directory Services (AFDS)	**https://epi.afds.af.mil/nonaf**
Capability Packages and the CSfC Components List	**https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/**
CISA Learning	https://niccs.cisa.gov/education-training/cisa-learning
Client Computing Solutions III (CCS-3) SharePoint Site	**https://usaf.dps.mil/sites/aficc/afcc/AFICC/771ESS/SitePages/Client-Computing-Solutions-(CCS-3).aspx**
Common Criteria (CC) Portal	https://www.commoncriteriaportal.org/
Cross Domain Solutions (CDS) Office, DAF	**https://usaf.dps.mil/teams/ccc/fpu/air-force-cross-domain-support-element.aspx**
CNSSI 4009, Committee on National Security Systems (CNSS) Glossary	https://www.cnss.gov/CNSS/ or the latest
CTO 10-084 and CTO 10-133 Memorandum	**https://usaf.dps.mil/teams/EAO/issm/Pages/writewaiver.aspx**
CUI Registry	https://www.archives.gov/cui
DAF Cybersecurity Collaborative Environment	**https://usaf.dps.mil/teams/IACE/**
DAF Cybersecurity Collaborative Environment (SIPRNet)	https://intelshare.intelink.sgov.gov/sites/af_cybersecurity/SitePages/Home.aspx
DAF myLearning	**https://lms-jets.cce.af.mil/moodle/**
DAF Mobile Site	**https://www.safcn.af.mil/Mobile**
DAF SAP Cybersecurity Office MilSuite	https://www.milsuite.mil/book/groups/usaf-cybersecurity-for-sap
Defense Logistics Agency Disposition Services	https://www.dla.mil/DispositionServices.aspx
Defense Procurement and Acquisition Policy	https://www.acq.osd.mil/asda/dpc/cp/index.html
DISA DMZ Whitelist Database	https://niprdmzwhitelist.csd.disa.smil.mil
DISA DoD Mobile Devices (or its replacement) Training	https://cyber.mil (under Training Catalog, Cybersecurity Awareness)
DISA JSP SPL Website	https://jsp.sp.pentagon.mil/spl/Pages/default.aspx
DISA Traditional Security Checklist	https://cyber.mil/stigs/

DISA Unified Capabilities Approved Products List	https://aplits.disa.mil/processAPList.action
DISPATCH	NIPR: See ESD Portal SIPR: compliance/acknowledgement of published PLANORDs/TASKORDs. **https://elicsar.af.smil.mil/dispatch/**
DoD Component PPSM Configuration Control Board; Technical Advisory Group Representative Contact List	https://cyber.mil/ppsm
DoD Cyber Exchange (NIPRNet)	https://cyber.mil
DoD Cyber Exchange (SIPRNet)	https://cyber.smil.mil
DoD Cyber Exchange Category Assurance List	https://cyber.mil/ppsm/cal/
DoD Cyber Exchange Category Assurance List/DoD PPS Vulnerability Assessment Reports ***Note:*** *PKI is required for access.*	https://dod365.sharepoint-mil.us/:f:/r/Sites/DISA-Ports-Protocols-Services-Management/External/Knowledge_Service/Vulnerability_Assessment/Category%20Assurance%20List?csf=1&web=1&e=cStpLp
DoD Cyber Exchange Qualification Matrices	https://public.cyber.mil/wid/dod8140/qualifications-matrices/
DoD Issuances	https://www.esd.whs.mil/Directives/issuances/dodi/
DoD Patch Repository	https://patches.csd.disa.mil/
DoD PPSM Configuration Control Board Charter	https://cyber.mil/ppsm/
DoD PPSM Exception Management Process	https://cyber.mil/ppsm
DoD PPS Vulnerability Assessment reports	https://cyber.mil/ppsm/
DoD Risk Management Framework Knowledge Service	https://rmfks.osd.mil
eMASS Workflow Process	**https://airforce.emass.apps.mil**
Enhanced Technical Information Management System	**https://etims.cce.af.mil/ETIMS/index.jsp**
Enterprise Information Technology Service Management Remedy, Air Force Change Process	https://www.milsuite.mil/wiki/Air_Force_Change_Process
Enterprise Information Technology Service Management Systems	**https://eitsm25.eitsm2.us.af.mil/**

Enterprise Information Technology Service Management Systems (SIPRNet)	**https://eitsm2.us.af.smil.mil/**
Enterprise Mission Assurance Support Service (eMASS)	**https://airforce.emass.apps.mil**
ESD Portal	**https://esd.us.af.mil/esdportal**
Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement	https://www.acquisition.gov/
GSA AF Advantage	https://www.afadvantage.gov/advantage/ws/main/home?store=AIRFORCE
Guest Access with the Tenant	https://usaf.dps.mil/sites/TipsToolsApps/SitePages/GuestAccess.aspx
Guest Access Article on milBook	https://www.milsuite.mil/book/docs/DOC-1212009
Handbook for Providing Assistive Technology to Wounded Service Members	https://www.cap.mil
JFHQ-DODIN OPORD (SIPRNet)	https://intelshare.intelink.sgov.gov/sites/jfhq-dodin/
NDCI Workflow (ESD Portal Self Help)	**https://esd.us.af.mil/ESDPortal/** Search for "NDCI Workflow"
NIAP FAQ, NIAP Product Compliant List and NIAP Product in Evaluation List	https://www.niap-ccevs.org/
NIST Cryptographic Module Validation Program	https://csrc.nist.gov/projects/cryptographic-module-validation-program
NIST Publications	https://csrc.nist.gov/publications/PubsSPs.html
NSA Classified Materiel Conversion for Packaging, Documenting, and Shipping Devices	https://www.nsa.gov/cmc/
NSA's Commercial Solutions for Classified (CSfC)	https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/
PPS Lessons Learned	**https://usaf.dps.mil/teams/IACE/Wiki/PPS-Lessons-Learned.aspx**
PPSM Training for PPSM Overview, Registry, Network Boundaries, and Using the Category Assurance List	https://cyber.mil/connect/mptp/
SORN	https://dpcld.defense.gov/Privacy/SORNs/
SNAP and SGS Database	NIPRNet SNAP: https://snap.dod.mil

	SIPRNet SGS: https://giap.disa.smil.mil
Software and Application Certification Assessment (SACA)	**https://usaf.dps.mil/teams/ccc/fpu/CZZE_TE_SACA.aspx**
Security Technical Implementation Guides (STIGs)	https://cyber.mil/stigs/
Security Requirements Guides (SRGs)	https://cyber.mil/stigs/
Trade Agreement Act (TAA)–Designated Countries	https://www.gsa.gov/buy-through-us/purchasing-programs/multiple-award-schedule/help-with-mas-contracts-to-sell-to-government/roadmap-to-get-a-mas-contract/readiness-assessment-for-mas-offerors/look-up-trade-agreements-actdesignated-countries