BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-200

31 AUGUST 2015

Communications and Information

AIR FORCE CYBERSECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF CIO/A6SC

Certified by: SAF/CIO A6S
(Col Mary Hanson, AF SISO)

Supersedes: AFI 33-200, 23 December 2008; AFI 33-220, 21 November 2007

Pages: 50

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Assurance (IA) Program*, and establishes Air Force (AF) cybersecurity requirements for compliance with: Committee on National Security Systems Instruction (CNSSI) No. 4005, (FOUO) *Safeguarding Communications Security(COMSEC) Facilities and Materials*; Committee on National Security Systems Instruction (CNSSI) No. 4016, (FOUO), *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, CNSSP -11*; Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, *Commercial Mobile Device (CMD) Interim Policy*; DoD Directive (DoDD) 8100.2, *Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*; DoD Instruction (DoDI) 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*; DoDI 8500.01, *Cybersecurity*; DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*; DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*; DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*; DoDI 8540.01. *Cross Domain (CD) Policy;* DoDI 8520.03, *Identity Authentication for Information Systems*; DoDI O-8530.2, *Support to Computer Network Defense (CND)*; DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM);* DoDI 8580.1, *Information Assurance (IA) in the Defense Acquisition System;* DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*; and DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems*. This instruction is consistent with Chairman Joint Chiefs of Staff Instruction CJCSI 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND)*; CJCSI 6211.02D, *Defense Information Systems network (DISN) Responsibilities* and; Chairman Joint Chiefs of Staff

Manual (CJCSM) 6510.01A, *Information Assurance (IA) and Computer Network Defense (CND) Volume 1 (Incident Handling Program)*. This instruction applies to all AF military, civilian, and contractor personnel under contract by DoD, regardless of Air Force Specialty Code (AFSC), who develop, acquire, deliver, use, operate, or manage AF Information Technology (IT). This instruction applies to the Air National Guard (ANG) and Air Force Reserve Command (AFRC). The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). Use of extracts from this instruction is encouraged. CNSSI 4009, *National Information Assurance (IA) Glossary*, explains other terms. Direct questions, comments, recommended changes, or conflicts to this publication through command channels using the AF Form 847, *Recommendation for Change of Publication*, to SAF/CIO A6. Send any supplements to this publication to SAF/CIO A6 for review, coordination, and approval prior to publication. Unless otherwise noted, the SAF/CIO A6 is the waivering authority to policies contained in this publication. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document is substantially changed and should be reviewed in its entirety. The change is a result of a DoD policy directive update and establishes the AF Cybersecurity program and risk management framework as an essential element to accomplishing the AF mission.

Chapter 1

GENERAL INFORMATION

1.1. Introduction. This AFI provides general direction for implementation of cybersecurity and management of cybersecurity programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the confidentiality, integrity, and availability (CIA) of AF IT and the information they process. This AFI ensures the use of appropriate levels of protection against threats and vulnerabilities, helps prevent denial of service, corruption and compromise of information, and potential fraud, waste, and abuse of government resources.

1.1.1. The AF cybersecurity program incorporates strategy, policy, awareness/training, assessment, authorization, implementation and remediation.

1.1.2. The cybersecurity discipline aligns with the AF Cybersecurity strategy key concept that total risk avoidance is not practical and therefore risks assessment and management is required.

1.1.3. Cybersecurity encompasses the following disciplines/functions: Air Force Risk Management Framework (RMF), IT controls/countermeasures, Communications Security (COMSEC), Computer Security (COMPUSEC), TEMPEST (formerly known as Emissions Security [EMSEC]), AF Assessment and Authorization (A&A) (formerly known as Certification and Accreditation Program [AFCAP]), and Cybersecurity Workforce Improvement Program (WIP).

1.2. Applicability. This publication is binding on all military, civilian and contractors or other persons through the contract or other legally binding agreement with the Department of the Air Force, who develop, acquire, deliver, use, operate, or manage AF IT. This publication applies to all AF IT used to process, store, display, transmit, or protect AF information, regardless of classification or sensitivity. AF IT includes but is not limited to: Information Systems (Major applications & Enclaves), Platform Information Technology (PIT) & PIT systems, IT Services (Internal & External), and IT Products (Software, Hardware, Applications).

1.2.1. More restrictive Federal, DoD, and Director of National Intelligence (DNI) directive requirements governing Special Access Program (SAP) information take precedence over this publication. The latest version of all publications (e.g., Federal, Joint, DoD, AF) referenced within this publication are to be used.

1.2.2. This publication and implementation guidance identified within is not applicable to Intelligence Community ISs to include Sensitive Compartmented Information (SCI) ISs. Refer to the Intelligence Community (IC) Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation and or the Unified Cross Domain Services Management Office (UCDSMO) as applicable.

1.2.3. Authority for AF space systems rests with Air Force Space Command (AFSPC) as delegated by US Strategic Command (USSTRATCOM). AF space systems generally follow AF Cybersecurity policy and processes; where exceptions exist, this instruction is annotated accordingly. NOTE: Non-AF space systems follow cybersecurity policy and guidance in DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense.

1.2.4. Effective implementation and resultant residual risk associated with cybersecurity controls is assessed, documented, and mitigated according to DoDI 8510.01, DoD Risk Management Framework (RMF), Air Force Manual (AFMAN) 33-210, Air Force Assessment and Authorization Program, and the AF RMF Knowledge Service, for inclusion in the AF Information Technology (IT) A&A package.

1.3. Objectives. The objective of the AF Cybersecurity Program is to manage the risk presented by adversary cyber capabilities (purposeful attacks) and intelligence, environmental disruptions, human or machine errors, and to maintain mission survivability under adversary offensive cyber operations. The AF implements and maintains the Cybersecurity Program to adequately secure its information and IT assets. The Cybersecurity Program:

1.3.1. Ensures AF IT operate securely by protecting and maintaining IS / PIT resources and information processed throughout the system's life cycle.

1.3.2. Protects information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

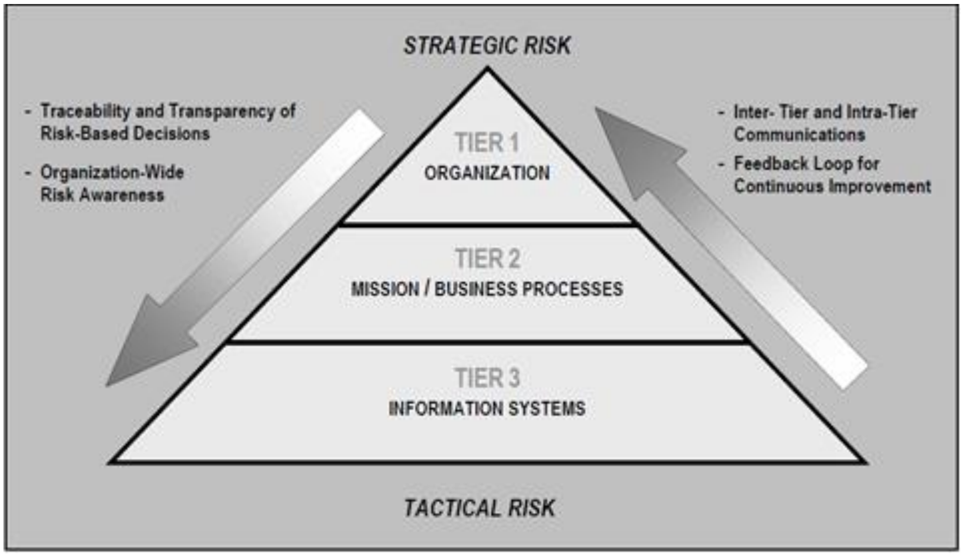
1.3.3. Leverages the multi-tiered organization-wide risk management approach defined in NATIONAL Institute of Standards and technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk (See figure 1.1).

1.3.3.1. Tier 1 – Organization: Risk management at this tier is performed through cybersecurity governance bodies at the AF enterprise level.

1.3.3.2. Tier 2 – Mission/Business Process: risk management at this tier is performed by mission owner level and is informed by the risk context, risk decisions, and risk activities at Tier 1.

1.3.3.3. Tier 3 – Information System: risk management at this tier is performed by individuals responsible for the management of individual IT and is guided by the risk context, risk decisions and risk activities at Tiers 1 and 2.

Figure 1.1. Tiered Risk Management Approach (NIST SP 800-39).


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Secretary of the Air Force, Office of Information Dominance and Chief Information Officer (SAF/CIO A6) will develop strategies, policy and programs to integrate warfighting and combat support capabilities according to DoDI 8500. 01 and AFPD 33-2. SAF/CIO A6 will:

2.1.1. Oversee the establishment of risk tolerance and baseline cybersecurity controls for the AF IT. SAF CIO A6 will provide guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff (JCS), AF baseline cybersecurity controls for IT and remain within established risk tolerance levels

2.1.2. Maintain visibility of assessment and authorization status of AF IT through automated assessment and authorization tools or designated repositories for the AF in support of DoD CIO and Principle Authorizing Officials (PAO) IAW DoDI 8500.01, Cybersecurity.

2.1.3. Provide guidance to organizations on how to implement solutions for operational requirements exceeding the established National, DoD, Joint Chiefs of Staff (JCS), AF baseline cybersecurity controls for IT and remain within established risk tolerance levels.

2.1.4. Define cybersecurity performance measures and metrics to identify enterprise-wide cybersecurity trends and status of mitigation efforts.

2.1.5. On behalf of the SECAF, and IAW AFPD 33-2, appoint all Authorizing Officials (AO).

2.1.6. Appoint an Air Force Senior Information Security Officer (SISO) to direct and oversee the Air Force Cybersecurity Program.

2.1.7. IAW AFI 33-401, Air Force Architecting, appoint the AF Chief Architect with responsibility for the AF Cybersecurity Architecture.

2.1.8. Serve as the Mission Area Owner (MAO) for the Enterprise Information Environment Mission Area (EIEMA).

2.1.9. Chair the Air Force AO Summit.

2.1.10. Represent the EIEMA in the Air Force AO Summit.

2.1.11. Provide AF Enterprise oversight of the Air Force Information Technology Asset Management (ITAM) program.

2.2. Assistant Secretary of the Air Force (Acquisition) (SAF/AQ) will:

2.2.1. Build cybersecurity into all acquisitions by ensuring all cybersecurity requirements are implemented in all phases and contracts for research, development, test, and evaluation of IT.

2.2.2. Provide streamlined guidance to enable Program Executive Officers (PEO) and Program Managers (PM) to adhere to the mandated standards outlined in this instruction, DoDI 8580.1, DoDI 8581.1, DoDI 8510.01, AFMAN 33-152, and the A&A requirements of AFMAN 33-210.

2.2.3. Ensure contracts include appropriate Defense Federal Acquisition Regulation Supplement (DFARS) clauses for safeguarding unclassified DoD information on non-DoD ISs IAW DoDI 8582.01 and DFARS 204.7304 as applicable.

2.2.4. For all space acquisitions, ensure cybersecurity requirements are implemented in all phases of acquisitions according to the provisions in DoDI 5000.02, Operation of the Defense Acquisition System. SAF/AQ will provide streamlined guidance to enable each program and system under its span of control to develop a cybersecurity strategy meeting the requirements of this instruction, DoDI 5000.02, and DoDI 8580.1, and AFMAN 33-407, Air Force Clinger-Cohen Act (CCA) Compliance Guide.

2.2.5. Manage the process for preparing and reviewing AF acquisition program strategies and ensure cybersecurity has been appropriately addressed.

2.2.6. Represent the AF on policy and procedural matters regarding cybersecurity in the acquisition system.

2.2.7. Coordinate with USAF/A2 to ensure Intelligence acquisition programs address cybersecurity life cycle requirements. SAF/AQ will coordinate with USAF/A2 assigning AF PM representatives for Intelligence systems, equipment, networks, or services on the Air Force Information Network (AFIN) or utilizing AFIN capabilities that were developed and/or acquired by non-AF entities.

2.3. Air Force Office of Special Investigations (AFOSI) will:

2.3.1. AFOSI is the office of primary responsibility (OPR) for on-hook telephone technical security matters, to include providing guidance for installing and operating telephone systems within the Air Force, and department of defense facilities occupied by Air Force personnel.

2.3.2. Provide Air Force representation to the U.S. Government intelligence community's National Telephone Security Working Group (NTSWG). **(T-0)**. The group is the primary technical and policy resource in the U.S. intelligence community for all aspect of the Technical Surveillance Countermeasures (TSCM) program involving telephone systems in areas where sensitive government information is discussed.

2.3.3. Examine the TSCM needs of the Air Force and tailor Air Force telephone security standards to those established by the NTSWG. **(T-0)**.

2.3.4. Provide guidance to Air Force organization on selecting local equipment for installing telephone systems in sensitive discussion areas in conjunction with the host base Communications and Information Systems Officer (CSO) (AFMAN 33-145, Collaboration Services and Voice Systems Management) in accordance with CNSSI No. 5006, National Instruction for Approved Telephone Equipment, and The Defense Information Systems Agency (DISA) Approved Products List Integrated Tracking System (UC system acquisition). **(T-0)**.

2.3.5. Determine the effectiveness and applicability of protective security devices and TSCM procedures for qualified facilities; when warranted provide technical threat information and briefings concerning telephone systems and the countermeasures intended to nullify existing threats. **(T-0)**. Further information on requesting TSCM services or threat briefing is contained in AFI 71-101, Volume 3, The Air Force Technical Surveillance Countermeasures Program.

2.4. Mission Area Owner (MAO). A MAO is appointed for the Air Force portion of each of the DoD MAs. MAOs will:

2.4.1. Oversee and establish direction for the strategic implementation of cybersecurity and risk management within their MAs. **(T-0)**.

2.4.2. Assist the SAF/CIO A6 and the AF SISO in assessing the effectiveness of AF cybersecurity. **(T-1)**.

2.4.3. Coordinate with the DoD PAO for cybersecurity and risk management within their MAs. **(T-0)**.

2.4.4. Represent the interest of the MA, as defined in Reference DoDD 8115.01, Information Technology Portfolio Management, and, as required issue authorization guidance specific to the MA, consistent with this instruction. **(T-0)**.

2.4.5. Resolve authorization issues within their respective MAs and work with other MAOs to resolve issues among MAs, as needed. **(T-0)**.

2.4.6. Nominate AOs for MA IS and PIT systems supporting MA COIs specified in Reference DoD 8320.02, in coordination with SAF/CIO A6, consistent with this instruction. **(T-1)**. SAF/CIO A6 will appoint those nominated by the MAO.

2.4.7. Designate information security architects or IS security engineers for MA segments (overlapping spans of influence (enclaves)) or systems of systems, as needed. **(T-1)**.

2.4.8. Work with the AF SISO and other MAOs to ensure cybersecurity checks and balances occur through the appropriate mission area governance boards. **(T-1)**.

2.5. Twenty-Fourth Air Force (24AF (AFCYBER)) will:

2.5.1. Serve as the single point of contact for processing and supporting AF cybersecurity-related intelligence requests from AF and DoD intelligence entities (e.g., threat assessment against the AFIN) for the AFIN. 24 AF (AFCYBER) will provide SAF/CIO A6 Staff with courtesy copies of requests and responses for assessment of impact on the AF cybersecurity Program.

2.5.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of cybersecurity solutions across the DODIN.

2.5.3. Provide support to national, DoD, and AF level Technical Advisory Groups (TAG) (i.e., AFIA TAG, RMF TAG, DoD PPS TAG, etc.), as requested by SAF/CIO A6.

2.5.4. Oversee, manage, and control AF enclave boundary defense activities, measures, and operations.

2.5.5. Issue time compliance technical orders and modification kits for cybersecurity and cybersecurity-enabled products or components of AF ITs.

2.5.6. Ensure Ports Protocols and Services (PPS) requirements for the AFIN are limited to only those required for official use with proper approval, PPS's not properly approved follow the deny by default, allow by exception access philosophy, and that PPS information is validated annually.

2.6. AF Senior Information Security Officer (SISO) will develop, implement, maintain, and enforce the AF Cybersecurity Program. The AF SISO will direct and coordinate any associated budgets and advocate for AF-wide cybersecurity solutions through the planning, programming, budget and execution process on behalf of the SAF/CIO A6 according to DoDI 8500.01, DoDI 8510.01, AFPD 33-2, and AFMAN 33-210. The SISO is referred to as Senior Agency Information Security Officer [SAISO] or Chief Information Security Officer [CISO] in CNSSI 4009. The AF SISO will:

2.6.1. Be a DoD official (O-6 or GS-15 at a minimum), and a United States citizen.

2.6.2. Complete training and maintain cybersecurity certifications IAW AFMAN 33-285, Cybersecurity Workforce Improvement Program.

2.6.3. Monitor, evaluate, and provide advice to the SAF/CIO A6 regarding AF cybersecurity posture.

2.6.4. Serve as the AF CIO’s primary liaison to DoD SISO, Component SISO’s, MAJCOM Cybersecurity Offices, AF AOs, and SCAs.

2.6.5. In coordination with the SAF/CIO A6 and AO’s, ensure cybersecurity risk posture and risk tolerance decisions for AF IT meet mission and business needs while also minimizing the operations and maintenance burden on the organization. The AF SISO will represent the AF at Federal, DoD, and Joint cybersecurity steering groups and forums.

2.6.6. Ensure that IT guidelines are incorporated into acquisition, implementation, and operations and maintenance functions.

2.6.7. Provide direction on how cybersecurity metrics are determined, established, defined, collected, and reported for compliance with statutory, DoD, Joint, and AF policies and directives.

2.6.8. Appoint Security Control Assessors (SCAs) for all AF IT (excluding Special-Access Program/Special Access Required [SAP/SAR], IC, Space, NC3, and Medical).

2.6.9. Perform as the SCA or formally delegate the security control assessment role for governed information technologies.

2.6.10. Provide guidance and direction on Agent of the Security Control Assessor (ASCA) establishment in support of Assessment and Authorization (A&A) requirements.

2.6.11. Oversee establishment and enforcement of the A&A process, roles, and responsibilities; review approval thresholds and milestones within the AF A&A Program.

2.6.12. Chair the Air Force Cybersecurity Risk Management Council (AFCRMC).

2.6.13. Adjudicate IT determinations, in coordination with the Air Force Risk Management Council, when there is a conflict in the IT determination process.

2.6.14. Appoint in writing the AF Certified TEMPEST Technical Authority (AF CTTA).

2.6.15. Appoint AF members to the DoD RMF TAG.

2.6.16. Review and approve Cybersecurity Strategies for all AF IT IAW DoDI 5000.02 and AFMAN 33-407, AF Clinger-Cohen Act (CCA) Compliance Guide. The approval of the Cybersecurity Strategies cannot be delegated.

2.6.17. Review and approve Privacy Impact Assessments (PIAs) submitted IAW AFI 33-332, The AF privacy and Civil Liberties Program. The approval of the PIA may be not be delegated.

2.6.18. Approve National Security System (NSS) designations for AF IT.

2.6.19. Approve Defense Industrial Base Cybersecurity/Information Assurance (DIB/CS/IA) Damage Assessment Reports (as needed) IAW DoDI 5205.13.

2.6.20. Ensure AF RMF guidance is posted to the DoD Component portion of the KS, and is consistent with DoD policy and guidance.

2.6.21. Validate and prioritize (with the support of the AF Risk Management Council (AFRMC)) all AF cryptographic certification requests prior to submission for NSA action.

2.7. Air Force Office of Cyberspace Strategy and Policy (SAF CIO A6S) will:

2.7.1. Provide cyberspace policy, guidance, & oversight. SAF CIO A6S will inform Headquarters United States Air Force, and MAJCOMs about changes to DoD and AF cybersecurity policies and procedures in accordance with HAFMD1-26 Chief, Information Dominance and Chief Information Officer.

2.7.2. Ensure AF acquisition guidance reflects national, federal, DoD, and AF cybersecurity policy and procedures.

2.7.3. Develop and evaluate cybersecurity performance measurements for compliance with statutory, DoD, Joint, and AF policies and directives.

2.7.4. Establish and enforce the RMF process, roles, and responsibilities; review approval thresholds and milestones within the AF RMF Program.

2.7.5. Provide AF IT PEO’s guidance on completion and submission of Cybersecurity Strategies and submit for AF SISO approval.

2.7.6. Collect and report cybersecurity management, financial, and readiness data to meet DoD cybersecurity and Office of Management and Budget (OMB) reporting requirements.

2.7.7. Serve as the single cybersecurity coordination point for joint or Defense-wide programs that are deploying IT (guest systems) to AF enclaves.

2.7.8. Participate in Federal, DoD and Joint cybersecurity and RMF technical working groups and forums (e.g. RMF TAG, DSAWG).

2.7.9. Develop and implement AF cybersecurity requirements planning, programming, budgeting, and execution in the AF budget process in compliance with SISO direction. Through the Air Force budget request, SAF CIO A6S will advocate for cybersecurity funding and manning with the Office of the Secretary of Defense and Congress.

2.7.10. Establish and maintain cybersecurity checklists for use with the AF Inspection Systems, currently the Management Internal Control Toolset (MICT) in accordance with AFI 90-201 Air Force Inspection System.

2.7.11. Develop concepts and establish strategy for integrated support and configuration management of cybersecurity equipment.

2.7.12. Oversee, plan, implement, manage, and support the COMSEC aspects of programs, including centralized record maintenance of COMSEC equipment, components, and material.

2.7.13. Carry out Federal Information Security Management Act of 2002 (FISMA)-related CIO responsibilities.

2.7.14. Provide detailed information on the FISMA requirements via the annual AF FISMA Reporting Guidance.

2.7.15. Manage the annual assessment of the AF Cybersecurity Programs as required by FISMA. Requests, through channels, support from AF organizations. Organizational support allows the AF SISO to answer the annual FISMA report questions posed by the OMB.

2.7.16. Ensure cybersecurity requirements are addressed and visible in all investment portfolios and investment programs according to AFI 33-401, Air Force Architecting, and AFMAN 33-210

2.7.17. Implement and enforce the education, training, and certification of AF cybersecurity professionals and users according to DoD 8570.01-M, Information Assurance (IA) Training, Certification, and Workforce Management, and AFMAN 33-285.

2.7.18. Coordinate Inspector General (IG) inspections and associated responsibilities according to and AFI 90-201.

2.7.19. Collect and report on qualification metrics and submits reports to the DoD CIO as directed such as for Federal Information Security Management Act (FISMA) reporting, standardizing reporting across Air Force.

2.7.20. Review and provide guidance in support of MAJCOM or equivalent provided commercial internet waivers and facilitates presentation to the DoDIN waiver panel; is a voting member of the DoDIN waiver panel. For additional information, AFI 33-115 and AFMAN 33-282.

2.7.21. Review Cross Domain Solution (CDS) requests and presents to the Defense Security Accreditation Working Group (DSAWG) for approval.

2.7.22. Manage the implementation of policy and standardized procedures to catalog, regulate, and control the use and management of ports, protocols, and services (PPS) in IT and applications IAW DoDI 8551.01.

2.7.23. Serve as the AF Public Key Infrastructure (PKI Management Authority (PMA). SAF CIO A6S will direct policy, requirements, and implementation of PKI integration across all AF networks. SAF CIO A6S will participate in DoD and Federal working groups and forums involved in PKI and IdAM, and is the AF OPR to DoD, NSS, and Federal PKI and Identity and Access Management (IdAM) groups.

2.7.24. Represent the AF as a voting member on DoD PPS Configuration Control Boards (CCB). Designates AF A6S as primary and one or more alternate voting representatives for the DoD PPS CCB.

2.7.25. Designate a primary and one or more alternate representatives for the DoD PPS TAG.

2.7.26. Designate points of contact to register the PPS used by AF IS in the DoD PPS Registry (also known as DoD PPS Database) according to this instruction and DoD policy.

2.7.27. Manage PPS procedures for the AF according to this instruction, DoD guidance, and USCYBERCOM orders and directives. Responsibilities include advocating issues from customers with Air Staff and the DoD PPS Program Manager at the Defense Information Systems Agency (DISA); providing guidance and support to customers; and processing waiver, deviations, and exceptions.

2.7.28. Establish a Defense Industrial Base Cyber Security/ Information Assurance (DIB CS/IA) Program Office. The DIB CS/IA Program Office works cooperatively with participating Cleared Defense Contractors (CDCs) to enhance their ability to safeguard DoD information residing on or transiting DIB unclassified networks IAW DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities. In accordance with DoDI 5205.13, the AF established the AF Damage Assessment Management Office (AF DAMO) within SAF/CIO A6.

2.7.29. The AF DAMO will conduct damage assessments on data compromised as a result of adversary intrusions into those contractor networks. AF DAMO determines the extent of intelligence obtained by adversary cyber intrusions into DIB networks, and assesses the overall impact of the data loss on current and future weapons programs, scientific and research projects, and warfighting capabilities.

2.7.30. Set policy for managing AF electronic (EM) spectrum use to support the AF mission and exercise control over the frequency management process IAW AFI 33-580, Spectrum Management

2.7.31. Upon request from the AF SISO, AF functional authorities and MAJCOMs are required to provide appropriate programmatic, operational, and technical SMEs, intelligence analysts, or cyber forces to assess the compromised information as part of Integrated Process Teams (IPTs). All IPTs convene at the DoD Cyber Crime Center (DC3) in Linthicum, MD, where AF DAMO personnel assist the IPT in the damage assessment process. The participants provide expert opinion on the extent of damage caused as a result of the compromise and make recommendations on mitigation efforts required due to the loss of that information. Damage assessment reports are drafted for each case and disseminated to the appropriate AF program offices, agencies, and stakeholders for review and possible mitigation actions.

2.8. Authorizing Official (AO). The AO is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The AO renders authorization decisions for DoD ISs and PIT systems under their purview in accordance with DoDI 8510.01. A current listing of AOs is available on the AF Cybersecurity Knowledge Service located at: **https://cs1.eis.af.mil/sites/SAFCIOA6/A6S/afcks/Compliance/AFAAP/SitePages/Home.aspx** . The AO will:

2.8.1. Be appointed from senior leadership positions within business owner and mission owner organizations to promote accountability in authorization decisions that balance mission and business needs and security concerns/risks.

2.8.2. Be a DoD official (O-7 or SES at a minimum), and be a United States citizen.

2.8.3. Complete AF AO training IAW AFMAN 33-285.

2.8.4. Be appointed by SAF CIO/A6 in coordination with the appropriate MAO. The appointment grants authority to authorize IS and PIT systems within the authorization boundary as needed.

2.8.5. Not delegate ATO granting authority. **(T-1)**.

2.8.6. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.9. AO Designated Representative (AODR) will:

2.9.1. Complete AO training and maintain cybersecurity certifications consistent with duties and responsibilities of an SCA and IAW AFMAN 33-285. **(T-1)**.

2.9.2. Perform responsibilities as assigned by the AO. NOTE: AODR's may perform any and all duties of an AO except for accepting risk by issuing an authorization decision. **(T-1)**.

2.9.3. Make recommendations to the AO to approve ATO based on input from RMF team members, and other AOs and AODRs. **(T-1)**.

2.9.4. Be appointed by the AO, and, at a minimum, be an O-5 or GS-14. **(T-1)**.

2.10. Security Control Assessor (SCA).

2.10.1. The SCA is the senior official having the authority and responsibility for the certification of all ISs and PIT systems governed by the Air Force.

2.10.2. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.11. Security Controls Assessor Representative (SCAR) will:

2.11.1. Complete training and maintain appropriate cybersecurity certification IAW AFMAN 33-285. It is highly recommended SCARs complete both the AO training module and attain the CNSSI 4016 certificate for supplemental training. Proof of training (e.g. certificate) is included as an artifact to the IS's or PIT system's A&A package.

2.11.2. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program

2.12. Agent of the Security Controls Assessor (ASCA). The ASCA is a licensed organization which may be contracted by the PM to assist in certification activities and will:

2.12.1. Report directly to the SCA for guidance related to validation activities and procedures. **(T-1)**.

2.12.2. Maintain ASCA license IAW SISO guidance and the ASCA licensing guide. **(T-1)**.

2.12.3. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program

2.13. Information System Owners (ISO). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information or PIT system. An ISO will be appointed in writing for every IS and PIT System. **(T-1).** For those systems that are Air Force-wide systems (e.g., AFNET, LOGMOD, etc.), they will be appointed by the HAF/SAF 3-letter responsible for the capability. For MAJCOM, base-level IS/PIT systems, and base enclaves, the appropriate MAJCOM 2-letter will appoint the ISO. No further appointment is necessary. The ISO will:

2.13.1. Identify the requirement for IT and requests funds, operates and maintains the IT in order to enhance mission effectiveness. (NOTE: Do not confuse this with the ISO role in TEMPEST.) **(T-2)**.

2.13.2. Identify, implement, and ensure full integration of cybersecurity into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment. **(T-0)**. Reference DoDI 8510.01, AFI 63-101, and AFMAN 33-210 for guidance.

2.13.3. Develop, maintain, and track the security plan for assigned IS and PIT systems. **(T-1)**.

2.13.4. Develop and document a system-level continuous monitoring (CM) strategy to monitor the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation. **(T-1)**. The ISO must ensure the strategy includes the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor (e.g., SCA or ASCA). **(T-1)**.

2.13.5. Ensure the PMO is resourced with individuals knowledgeable in all areas of cybersecurity to support security engineering and security technical assessments of the IS or PIT systems for the SCA's authorization determination, AOs authorization decision, and other security related assessments (e.g., Financial Improvement and Audit Readiness (FIAR) IT testing, Inspector General audits). (T-1).

2.13.6. Ensure that applicable CTO's are received and acted upon per the CTO directions. **(T-1)**.

2.13.7. Ensure stakeholders are identified that may be affected by the implementation and operation of the IT. **(T-2)**.

2.13.8. Ensure the IT has a designated Information System Security Manager (ISSM) with the support, authority, and resources to satisfy established responsibilities for managing the IT's cybersecurity posture. **(T-1)**.

2.13.9. Plan and budget for all software assurance (SwA) activities (e.g. adopt SwA best practices, third party, secure coding standards, automated scans, etc…) during all phases of the software development lifecycle (SDLC). **(T-2)**.

2.13.10. In coordination with the Information Owner/Steward, decide who has access to the system (and with what types of privileges or access rights) and ensure system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). **(T-2)**.

2.13.11. Based on guidance from the SCA and AO, inform appropriate organizational officials of the need to conduct the full RMF assessment and authorization; ensure the necessary resources are available for the effort, and provides the required IT access, information, and documentation to the SCA. **(T-2)**.

2.13.12. Receive the security assessment results from the SCA and develop a POA&M for all identified weaknesses. **(T-1)**. After taking appropriate steps to reduce or eliminate weaknesses, the ISO will assemble the authorization package and submit the package to the SCA for assessment and subsequently to the AO for an authorization decision. **(T-1)**.

2.13.13. Ensure open POA&M items are closed on time. **(T-2)**.

2.13.14. Ensure consolidated A&A documentation is maintained for systems with instances at multiple locations. **(T-2)**.

2.13.15. Ensure, with the assistance of the ISSM, the system is deployed and operated according to the approved System Security Plan (SSP) and the authorization package (i.e., the AO's authorization decision). **(T-1)**.

2.13.16. Conduct specific duties outlined in the KS. **(T-2)**.

2.14. Program Manager (PM)/System Manager (SM). PM/SMs will:

2.14.1. Identify, implement, and ensure full integration of cybersecurity into all phases of their acquisition, upgrade, or modification programs, including initial design, development, testing, fielding, operation, and sustainment IAW AFI 63-101, Acquisition and Sustainment Life Cycle Management, DoDI 8510.01 and AFMAN 33-210 for guidance. **(T-0)**.

2.14.2. Plan and coordinate for all IT cybersecurity requirements IAW applicable guidance**. (T-2)**.

2.14.3. Ensure that ISs and PIT systems under their purview have cybersecurity-related positions assigned in accordance with AFMAN 33-285. **(T-2)**.

2.14.4. Assign an ISSM for the program office and ensure they have the proper certification IAW AFMAN 33-285. **(T-1)**.

2.14.5. Ensure the IS or PIT system is registered IAW AFI 33-141, AF IT Portfolio Management and Investment Review.

2.14.6. Develop and maintain a cybersecurity strategy as applicable and IAW AFMAN 33-407.

2.14.7. Ensure operational systems maintain a current ATO. **(T-1)**.

2.14.8. Ensure all changes are approved through a configuration management process, are assessed for cybersecurity impacts and reported to the SCA as applicable. **(T-2)**.

2.14.9. Track and implement the corrective actions identified in the POA&M in the Enterprise Mission Assurance Support Service (eMASS). **(T-0)**. POA&Ms provide visibility and status of security weaknesses to the ISO, Information Owner(s), AO and AF SISO.

2.14.10. Ensure annual and milestone security reviews are conducted and selected RMF controls are tested IAW this instruction, the CM plan and OMB Circular A-130, Management of Federal Information Resources ISO FISMA. **(T-0)**. The PM/SM will brief the results of both security reviews and the RMF control tests at the governance boards for the appropriate mission area in accordance with the board requirements. **(T-0)**.

2.14.11. Report security incidents to stakeholder organizations. **(T-2)**. The PM/SM will conduct root cause analysis for incidents and develop corrective action plans. **(T-2)**.

2.14.12. Ensure the program is resourced with individuals knowledgeable in security engineering and security technical assessments IAW AFMAN 33-285. **(T-2)**. These efforts support the SCA's assessment and the AO's authorization decision for IT that is subject to the RMF process IAW AFMAN 33-210.

2.14.13. In coordination with the Information Owner/Steward, ensure that a Privacy Impact Assessment is completed for IT that process and/or stores Personal Identifiable Information (PII). **(T-0)**.

2.15. Information System Security Manager (ISSM). The ISSM is the primary cybersecurity technical advisor to the AO for AF IT. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. That program ISSM may also serve as system ISSM for the enclave and reports to the CS/CC as the PM for the base enclave. The ISSM will:

2.15.1. Act on behalf of the AO to maintain the authorization of the system throughout its lifecycle; therefore, if the ISSM is not qualified to serve, the AO or the AODR may request the PM/SM designate a suitable replacement. **(T-3)**.

2.15.2. Complete training and maintains cybersecurity certification IAW AFMAN 33-285 (Individuals in this position must be US citizens). **(T-0)**. Proof of training (e.g. certificate) is included as an artifact to the IS's or PIT systems A&A package.

2.15.3. Support the ISO on behalf of the AO in implementing the RMF. **(T-3)**.

2.15.4. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.16. Information System Security Officer (ISSO). The ISSO is responsible for ensuring the appropriate operational security posture is maintained for AF IT under their purview. This includes the following activities related to maintaining situational awareness and initiating actions to improve or restore cybersecurity posture. ISSOs (formerly system level IA Officers), or the ISSM if no ISSO is appointed, will:

2.16.1. Implement and enforce all AF cybersecurity policies, procedures, and countermeasures using the guidance within this instruction and applicable cybersecurity publications. **(T-1)**.

2.16.2. Complete and maintain required cybersecurity professional certification IAW AFMAN 33-285 (Individuals in this position must be US citizens). **(T-0)**.

2.16.3. For additional information on this position, see AFMAN 33-210, Air Force Assessment and Authorization Program.

2.17. Cybersecurity Liaison. Each organizational command or other cognizant authority (i.e., group commander, Wing Cybersecurity Office) must appoint a Cybersecurity Liaison (formerly Organizational IAO) when cybersecurity functions are consolidated to a central location or activity. **(T-1).** Additional (subordinate) cybersecurity liaison positions may be assigned for additional support at the discretion of organizations or based upon mission requirements, however, only one primary and one alternate cybersecurity liaison is mandatory. A cybersecurity liaison will:

2.17.1. Develop, implement, oversee, and maintain an organization cybersecurity program that identifies cybersecurity requirements, personnel, processes, and procedures. **(T-1)**.

2.17.2. Supervise the organization's cybersecurity program. **(T-2)**.

2.17.3. Implement and enforce all Air Force cybersecurity policies and procedures using the guidance within this instruction and applicable specialized (COMSEC, COMPUSEC, TEMPEST etc.) cybersecurity publications. **(T-1)**.

2.17.4. Assist the wing cybersecurity office in meeting their duties and responsibilities. **(T-3)**.

2.17.5. Ensure all users have the requisite security clearances, supervisory need-to-know authorization, and are aware of their cybersecurity (via cybersecurity training) before being granted access to Air Force IT according to AFMAN 33-282, chapter 4, AFI 31-501 and AFMAN 33-152. **(T-1)**.

2.17.6. Ensure all users receive cybersecurity refresher training on an annual basis. **(T-2)**.

2.17.7. Ensure IT is acquired, documented, operated, used, maintained, and disposed of properly and in accordance with the IT's security A&A documentation as prescribed by AFMAN 33-210. **(T-1)**.

2.17.8. Ensure proper CM procedures are followed. **(T-1)**. Prior to implementation and contingent upon necessary approval according to this instruction and AFMAN 33-210, the cybersecurity liaison will coordinate any changes or modifications to hardware, software, or firmware with the wing cybersecurity office and system-level ISSM or ISSO. **(T-1)**.

2.17.9. Report cybersecurity incidents or vulnerabilities to the wing cybersecurity office. **(T-3)**.

2.17.10. In coordination with the wing cybersecurity office, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered. **(T-3)**.

2.17.11. Implement and maintain required cybersecurity (COMSEC, COMPUSEC and TEMPEST) countermeasures and compliance measures IAW AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP). **(T-1)**.

2.17.12. Initiate requests for temporary and permanent exceptions, deviations, or waivers to cybersecurity requirements or criteria according to this instruction and applicable specialized cybersecurity publications. **(T-1)**.

2.17.13. When called upon to assist with an assessment conducted by the DIB CS/Cybersecurity program office, provide subject matter experts to analyze the data and provide recommendations for further action. **(T-3)**.

2.17.14. Maintain all IS authorized user access control documentation IAW the applicable Air Force records Information Management System (AFRIMS). **(T-3)**.

2.18. Information Systems Security Engineer (ISSE). The ISSE is any individual, group, or organization responsible for conducting information system security engineering activities. Reference NIST SP 800-37, *Applying the Risk Management Framework to Federal Information Systems*, for additional details.

2.18.1. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration.

2.18.2. Information system security engineers are an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems.

2.18.3. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques.

2.18.4. System security engineers coordinate their security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information system security officers.

2.18.5. IAW DoD 8570.01-M, Personnel performing any IA Workforce System Architecture and Engineering (IASAE) specialty function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. **(T-0)**.

2.19. Information Owner/Steward. An organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal as defined in CNSSI 4009, National Information Assurance Glossary. The Information Owner/Steward will:

2.19.1. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management. **(T-2)**.

2.19.2. Establish the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retain that responsibility even when the information is shared with or provided to other organizations. **(T-1)**.

2.19.3. Provide input to ISOs on the security controls selection and on the derived security requirements for the systems where the information is processed, stored, or transmitted. (A single IS may contain information from multiple information owners/stewards.) **(T-1)**.

2.19.4. Where a single IS may contain information from multiple information owners/stewards, provide input to ISO for the IS regarding security controls selection and derived security requirements for the systems where the information is processed, stored, or transmitted. **(T-1)**.

2.19.5. Thoroughly review the assessment and then releases the authorization package to the AO, thereby indicating to the AO that the system's cybersecurity posture satisfactorily supports mission, business, and budgetary needs (i.e., indicates the mission risk is acceptable); enabling the AO to balance mission risk with community risk in an authorization decision. **(T-1)**.

2.19.6. Maintain statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. **(T-0)**.

2.20. Headquarters Air Force Space Command (HQ AFSPC). As Lead Command for all Air Force Cyberspace Operations via the 24AF(AFCYBER), AFSPC is the Air Force focal point for establishment, operation, maintenance, defense, exploitation, and attack Cyberspace Operations. AFSPC coordinates the prioritization of all Cyberspace Infrastructure requirements. AFSPC will:

2.20.1. Cyber orders issued by AFSPC/CC or his/her delegated representative are military orders issued by order of the Secretary of the Air Force.

2.20.2. Support PEOs and PMs in the research, development, test and evaluation, and sustainment of cybersecurity or cybersecurity-enabled capabilities of AF space systems and products in consultation with the other MAJCOMs.

2.20.3. Develop and sustain processes for rapid cybersecurity capability insertion to address new or rapidly developing threats to the AFIN.

2.20.4. Ensure space PEOs and PMs/ISOs comply with cybersecurity requirements outlined in DoDI 8580.1, DoDI 8581.01, this instruction, and AFMAN 33-210.

2.20.5. Establish cybersecurity education and training for space PEOs and PMs/ISOs according to the requirements outlined in AFMAN 33-285.

2.20.6. Manage and advise the CDS program for space systems.

2.20.7. Manage the AF Cryptologic Modernization Program and oversees the AF COMSEC Office of Record (CoR) for COMSEC IAW AFMAN 33-283.

2.20.8. Coordinate all cryptographic equipment requests to reduce duplication of effort and ensure sustainability.

2.20.9. Manage all requests for support from NSA for cryptographic equipment certification, coordinate validation, and recommend prioritization for the AF SISO

2.20.10. Perform responsibilities IAW AFMAN 33-286, Air Force TEMPEST Program. This includes developing/managing necessary forms to include the AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Review. AFSPC will executes the TEMPEST program and coordinates with the AF CTTA, as outlined in AFSSI 7700 (to become AFMAN 33-286).

2.20.11. Establish and maintain Method and Procedure Technical Orders (MPTOs) associated with cybersecurity policies.

2.20.12. Implement the AF cybersecurity workforce certification and training program according to DoDD 8570.01, DoD 8570.01-M, and AFMAN 33-285.

2.20.13. Review, evaluate, and interpret AF cybersecurity doctrine, policy, and procedures. AFSPC will make recommendations on implementation of the doctrine, policy, and procedures to SAF/CIO A6.

2.20.14. Develop, coordinate, promulgate, and maintain AF (component-level) cybersecurity control specifications applicable to ISs residing on or connecting to the AFIN, if required.

2.20.15. Provide guidance and support to cybersecurity offices in developing, implementing, and managing their cybersecurity programs.

2.20.16. Establish a Cross Domain Solution Office (CDSO) to manage the AF CDS program.

2.20.17. Advocate issues from customers with Air Staff and the CDS Secret Internet Protocol Router Network Connection Approval Office at DISA.

2.20.18. Serve as the AF focal point for coalition networking issues specific to the command, control, communications and computers infrastructure, core e-mail, file sharing, print, collaboration tools, video teleconferencing (VTC), and web browsing capabilities. AFSPC will coordinate with focal points of other functional communities (AF/A2, etc.) on coalition networking issues for other infrastructures (intelligence, surveillance, and reconnaissance, etc.).

2.20.19. Provide the following to SAF CIO/A6 and the SISO:

2.20.19.1. Situational awareness (SA) report on the operational status and network health of the globally interconnected, end-to-end set of AF unique information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), mission, SPO and PMO managed systems and enclaves, data, and security.

2.20.19.2. SA report related to outage and other network events impacting the AFIN or the supported Combatant Command (COCOM) mission.

2.20.19.3. SA report on completion of cyber orders or inability to complete assigned tasks.

2.20.19.4. Tasks specified above do not replace any requirement for OPREP reporting outlined in AFI 10-206.

2.20.20. Manage the AF PPS program and procedures according to this instruction, DoDI 8551.01, and USCYBERCOM orders. Advocate issues from customers with AF/A3C/A6C Staff and the DoD PPS Program Manager at DISA.

2.20.21. Advocate issues from AF activities with DoD PPS Management.

2.20.22. Provide guidance and support regarding PPS policy and procedures.

2.20.23. Serve as the primary with one or more alternate AF representatives to the DoD PPS TAG according to DoD guidance.

2.20.24. Serve as the primary POC with one or more alternates to register (aka declare) and maintain PPS for AF ISs in the DoD PPS central Registry according to DoD 8551.01.

2.20.25. Support and manage the AF PKI Systems Program Office (PKI SPO) to manage AF identity credentials for human and non-person entities. AFSPC will provide guidance and support to that office in the implementation and management of PKI and other IdAM capabilities to support Air Force operational and mission needs.

2.20.26. Process requested for PPS exceptions, deviations, or waivers according to this instruction and DoD policy and guidance (e.g. DoD 8551.01, USCYBERCOM orders, PPSM Exception Management Process).

2.20.27. Execute the AF COMSEC program and perform COMSEC responsibilities IAW AFMAN 33-283, Communications Security (COMSEC) Operations.

2.20.28. Perform responsibilities IAW AFMAN 33-286. This includes developing/managing necessary forms to include AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Reviews.

2.21. MAJCOM Cybersecurity Office or Function will:

2.21.1. Support the principles of availability, integrity, confidentiality, authentication, and non-repudiation of information and information systems for the purpose of protecting and defending the operation and management of Air Force IT and National Security System (NSS) assets and operations.

2.21.2. Develop implement, oversee, and maintain a MAJCOM cybersecurity program that identifies cybersecurity architecture; requirements; objectives and policies; personnel; and processes and procedures.

2.21.3. Ensure cybersecurity workforce is identified, trained, certified, qualified, tracked, and managed IAW DoD and AF cybersecurity Workforce Improvement Program (WIP) directives and policies such as DoDD 8570.01, DoD 8570.01-M, AFMAN 33-210 and AFMAN 33-285. NOTE: If the individual is performing only COMSEC management duties, DoD 8570.01-M does not require the individual to be certified under this program.

2.21.4. Report the status of their cybersecurity workforce (civilian, military, and contractors) qualifications to the SAF/CIO A6 IAW Paragraph 7.2.of AFMAN 33-285.

2.21.5. Ensure that AF PKI Local Registration Authorities (LRAs) are established and maintained at all MAJCOM bases

2.21.6. Serve as a member of any appropriate Configuration Control Boards (CCB) or steering groups to address MAJCOM cybersecurity program issues.

2.21.7. Coordinate Inspector General (IG) inspections and associated responsibilities according to and AFI 90-201.

2.21.8. Review AF Form 4169 exception/waiver submissions, as appropriate, to maintain situational awareness

2.21.9. Ensure proper identification of manpower and personnel assigned to cybersecurity functions. MAJCOM Cybersecurity Office/Function will ensure this information is entered and maintained in the appropriate Air Force personnel databases.

2.21.10. IAW AFI 10-712, maintain organizational e-mail account with an SMTP alias of <MAJCOM>**.cybersecurity@us.af.mil**

2.22. Wing Cybersecurity Office (WCO). Develops and maintains the wing cybersecurity program. The wing cybersecurity office addresses all cybersecurity requirements on the base for IT under the control of the base Communications Squadron/Flight, including IT of tenant units (i.e., FOAs, DRUs, and other service units) unless formal agreements exist. NOTE: For bases with more than one wing, the designated host wing is responsible to provide this function. For Joint bases, the AF is responsible for all AF-owned IT and infrastructure. The WCO will:

2.22.1. IAW AFMAN 33-285, track and manage cybersecurity positions assigned by a commander which includes: system ISSMs/ISSOs assigned by PM's, COMSEC Account Managers (CAMs), COMSEC Responsible Officers (CROs), Cybersecurity Liaisons, Privileged Users, and Secure Voice Responsible Officers (SVROs).

2.22.2. Assign trained cybersecurity personnel IAW DoD requirements for IAM Level I or Level II categories and ensure certifications are also maintained IAW DoD requirements. **(T-0)**. ***NOTE:*** If the individual is performing only COMSEC management duties, refer to AFMAN 33-285 for position specific certifications.

2.22.3. Manage the overall COMSEC posture of their installation. The WCO will appoint one primary and at least one alternate COMSEC manager to oversee the wing COMSEC program and to assist and advise them in COMSEC matters IAW AFMAN 33-283, COMSEC Operations. **(T-0)**. The wing commander may delegate appointment authority to the unit commander of the supporting COMSEC account.

2.22.4. Establish COMPUSEC in the host wing cybersecurity office. **(T-1).** The cybersecurity office addresses all COMPUSEC requirements on the base, including those of tenant units (i.e. FOAs, DRUs, and other MAJCOM units) unless formal agreements exist.

2.22.5. Establish TEMPEST in the host wing cybersecurity office. **(T-1).** The cybersecurity office addresses all TEMPEST requirements on the base, including those of tenant units (i.e. FOAs, DRUs, and other MAJCOM units) unless there are other formal agreements.

2.22.6. Manage the Identity Management Program (PKI, Common Access Card (CAC), Air Force Directory Service (AFDS) Programs) IAW AFMAN 33-282.

2.22.7. Assist all base organizations and tenants in the development and management of their cybersecurity program. **(T-1).**

2.22.8. Designate a base enclave ISSM (for organization-level cybersecurity program) to develop, implement, oversee, and maintain the installation cybersecurity program. **(T-1).**

2.22.9. Provide oversight and direction to Cybersecurity Liaison (for organizational level programs) according to this instruction, AFI 33-115 and specialized cybersecurity publications. **(T-1)**. Specific responsibilities include but are not limited to the below items. The WCO will:

2.22.9.1. Ensure Cybersecurity Liaison receives proper cybersecurity training. **(T-1).**

2.22.9.2. Ensure Cybersecurity Liaisons are aware of and follow cybersecurity policy and procedures. **(T-1).**

2.22.9.3. Ensure Cybersecurity Liaison s review weekly alerts, bulletins, and advisories impacting security of an organization's cybersecurity program. **(T-1).**

2.22.10. Ensure cybersecurity guidance, and standard operating procedures (SOP) are prepared, maintained, and implemented by each unit. **(T-3).**

2.22.11. Monitor implementation of cybersecurity guidance and ensure appropriate actions to remedy cybersecurity deficiencies. **(T-3).**

2.22.12. Ensure cybersecurity inspections, tests, and reviews are coordinated. **(T-3)**.

2.22.13. Ensure all cybersecurity management review items are tracked and reported. **(T-3)**.

2.22.14. Report security violations and incidents to the AO and Air Force network operations activities according to AFI 33-115, Air Force Information Technology (IT) Service Management) and CJCSM 6510.01B, Cyber Incident Handling Program. **(T-1)**.

2.22.15. Ensure cybersecurity incidents are properly reported to the AO and the Air Force network operations reporting chain, as required, and that responses to cybersecurity related alerts are coordinated; all according to the requirements of AFI priveleged115. **(T-1).**

2.22.16. Ensure software management procedures are developed and implemented according to configuration management (CM) policies and practices for authorizing use of software on ISs. **(T-1).**

2.22.17. Serve as member of the base-level CM board or delegates this responsibility to an appropriate Action Officer. **(T-3).**

2.22.18. Maintain organizational e-mail account with an SMTP alias of <wing>**.cybersecurity@us.af.mil.** **(T-3).**

2.23. Organizational Commander. Commander will assign one Cybersecurity Liaison and at least one alternate to execute cybersecurity responsibilities protecting and defending information systems by ensuring the availability, integrity, confidentiality, authentication, and non-repudiation of data through the application of cybersecurity measures outlined herein. **(T-1).** Commanders or equivalent at all levels will maintain these responsibilities through the following programs:

2.23.1. Computer Security (COMPUSEC) Program IAW AFMAN 33-282.

2.23.2. Communications Security (COMSEC) Program IAW AFMAN 33-283.

2.23.3. TEMPEST Program Management IAW AFMAN 33-286. TEMPEST: A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

2.23.4. On-Hook Telephone Security Program. **(T-1)**. Organization commanders will ensure their program meets the following:

2.23.4.1. Ensure the number of telephones used is the minimum necessary to meet operational requirements. **(T-3)**.

2.23.4.2. Apply appropriate telephone security measures in discussion areas and ensure adequate protection for classified or sensitive discussions IAW National telephone Security Working group (NTSWG) publications. **(T-3)**.

2.23.4.3. Use physical security safeguards to prevent unauthorized personnel from obtaining clandestine physical access to the telephone system or components of the system. **(T-3)**.

2.24. Privileged User with cybersecurity responsibilities (e. g. Functional System Administrator). NOTE: Enterprise Information System (EIS) content managers and site designers (e.g. Microsoft SharePoint Site Owners, AF Portal Content Managers) who don't have administrative privileges to the overall IS are not considered Privileged Users. Additionally, AFMAN 33-285 and AFI 33-115 identify those individuals with certain elevated rights who are not considered Privileged users. Privileged users will:

2.24.1. Complete training and maintains certification IAW AFMAN 33-285.

2.24.2. Configure and operate IS according to cybersecurity policies and procedures and notify the AO, ISSM or ISSO of any changes that might adversely impact cybersecurity. **(T-1).**

2.24.3. Ensure IT under their management is properly patched per guidance from the PEO. **(T-3).**

2.24.4. Conduct and document annual cybersecurity inspection of their IT per the guidance provided the IT PEO. **(T-3).** Provides report to WCO annually.

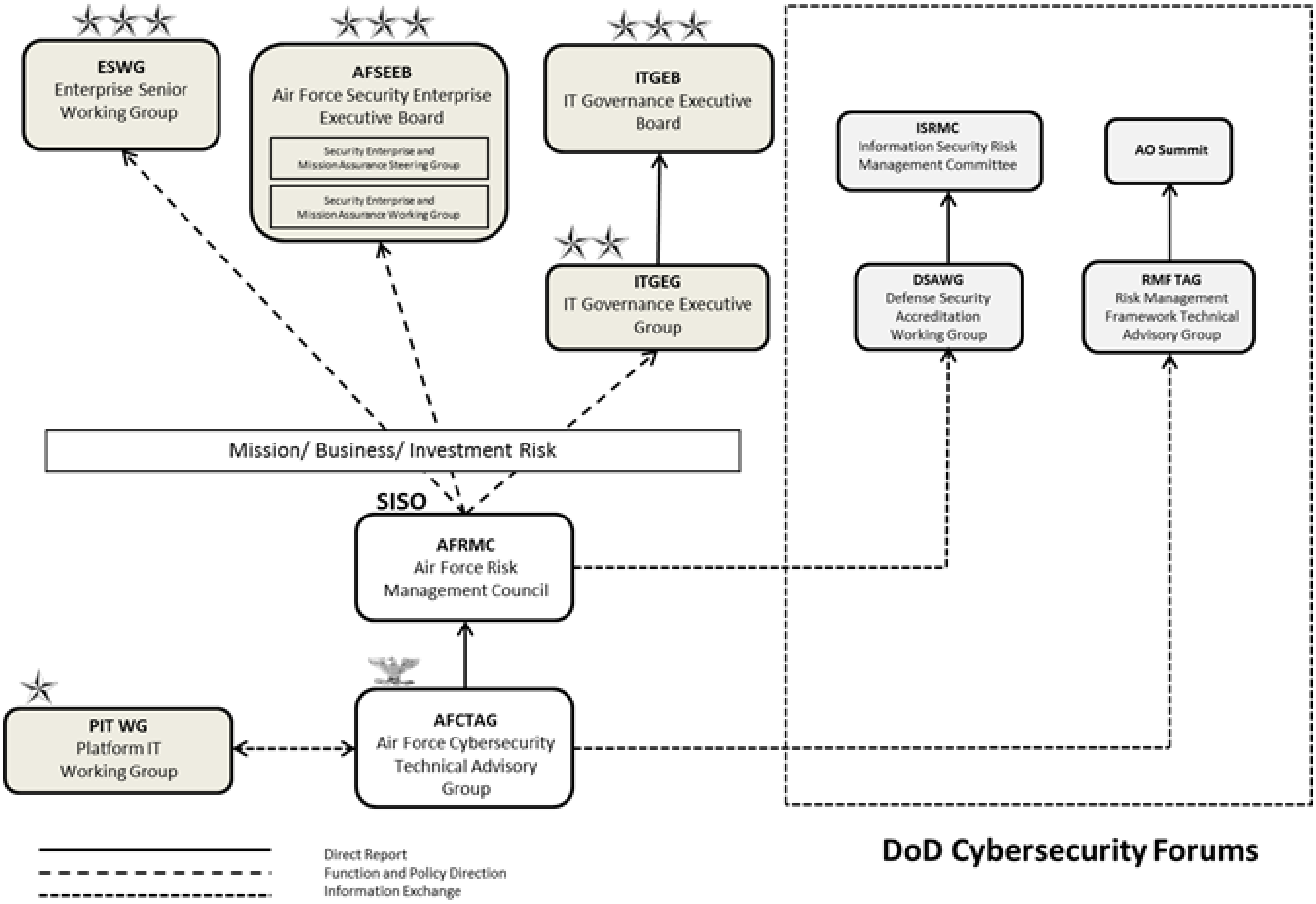
2.24.5. Establish and manage authorized user accounts for ISs, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed. **(T-3).**

Chapter 3

CYBERSECURITY GOVERNANCE

3.1. Cybersecurity Governance. Cybersecurity governance occurs at all levels of the Air Force enterprise and ensures cybersecurity strategies are aligned with mission and business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility. The Air Force Cybersecurity Governance Structure (Figure 3.1) formalizes how the AF manages cybersecurity risk with respect to the existing Air Force and DoD corporate boards and processes. The intention is to ensure cybersecurity is addressed in the appropriate forums for both mission/business risk and IT investment/portfolio management. Current governance forums do not regularly discuss cybersecurity nor the risk management process on a regular basis. These new forums ensure these topics are raised to the appropriate level and informed decisions can be made.

Figure 3.1. Air Force Cybersecurity Governance.


ESWG
Enterprise Senior Working Group
AFSEEB
Air Force Security Enterprise Executive Board
Security Enterprise and Mission Assurance Steering Group
Security Enterprise and Mission Assurance Working Group
ITGEB
IT Governance Executive Board
ITGEG
IT Governance Executive Group
ISRMC
Information Security Risk Management Committee
AO Summit
DSAWG
Defense Security Accreditation Working Group
RMF TAG
Risk Management Framework Technical Advisory Group
Mission/ Business/ Investment Risk
SISO
AFRMC
Air Force Risk Management Council
PIT WG
Platform IT Working Group
AFCTAG
Air Force Cybersecurity Technical Advisory Group
Direct Report
Function and Policy Direction
Information Exchange
DoD Cybersecurity Forums

3.2. Governance Process. The governance process ensures compliance with Title 44 United States Code (USC) § 3541, Federal Information System Management Act of 2002 (FISMA), requiring senior agency officials to provide security for information and ISs that support the operations and assets under their control.

3.3. Governance Bodies. The Air Force leverages existing Air Force and DoD governance bodies (shaded areas of Figure 3.1—AFSEEB, ITGEB, ITGEG, ESWG, etc.) to discuss cybersecurity risk topics and make organizational and mission/business area risk decisions. This instruction does not define the scope or responsibilities of these existing bodies. The following governance groups provide focused management and oversight of the Air Force Cybersecurity Program. Charters and process guides for each of these organizations are in development.

3.4. Air Force Risk Management Council (AFRMC). The AFRMC provides a forum for the senior cybersecurity professionals to validate and vet issues concerning cybersecurity risk from a mission and business perspective. The council reviews proposed Mission Area or DoD Component RMF control overlays, A&A guidance, and additional AF controls for compatibility with baseline controls and with other established control sets. They standardize the cybersecurity implementation processes for both the acquisition and lifecycle operations of Air Force Information Technology and Cyberspace systems. They advise and make recommendations as needed to existing governance bodies. Finally, they adjudicate assignment of Air Force Information Technology and Cyberspace systems to the appropriate Authorizing Official for those systems which fall outside of the defined authorization boundaries.

3.4.1. Chaired by the AF Senior Information Security Officer (AF SISO)

3.4.2. Attendees include all Air Force Security Control Assessors, 24 AF/A3, 624 OC, and SAF/CIO A6C Mission Area Integrators (MAI)

3.4.3. Monthly VTC or SIPR Defense Collaboration Services (DCS) with an annual in-person meeting

3.5. AF Cybersecurity Technical Advisory Group (AFCTAG). The AFCTAG provides technical cybersecurity subject matter experts (SMEs) from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF Cybersecurity Program. The TAG examines cybersecurity related issues common across Air Force entities and provide recommendations to the AF SISO and DSWAG on changes to the baseline security controls or configurations.

3.5.1. Co-chaired by the SAF/CIO A6S Cybersecurity Division Chief and AFSPC/A6S Division Chief

3.5.2. Attendees include all MAJCOM and functional cybersecurity subject matter experts

3.5.3. Quarterly DCS

3.6. AF AO Summit. The AO Summit is not a governance body but rather an enabler for both an enterprise-wide and converged organizational perspective to cybersecurity policy development, oversight, implementation, and training. This venue provides the CIO and Authorizing Officials an opportunity to discuss issues relevant and significant to AOs and their SCAs and develop recommended a way-forward for use by the Department.

3.6.1. Chaired by SAF CIO/A6

3.6.2. Attendees include all Air Force Authorizing Officials, Mission Area Owners (MAO), 24 AF/CC, and AF SISO

3.6.3. Quarterly VTC with an annual in-person meeting

Chapter 4

CYBERSECURITY IMPLEMENTATION

4.1. Air Force Cybersecurity Program. The AF Cybersecurity Program synchronizes and standardizes the cybersecurity requirements of AF IT.

4.1.1. Cybersecurity is integrated into all aspects of the AF Enterprise Architecture according to AFI 33-401.

4.1.2. Cybersecurity professionals coordinate cybersecurity projects across multiple investments through Portfolio Management according to AFI 33-141, Air Force Information Technology Portfolio Management and Investment Review.

4.1.3. All elements of an IT cybersecurity program are developed, documented, implemented, and maintained through the AF A&A program. Please reference AFMAN 33-210 for further information.

4.1.4. Cybersecurity professionals adhere to CJCSI 6510.01F and AFI 33-115 on use of DoD-provided, enterprise-wide automated tools/solutions (e.g., Host Based Security System (HBSS)) to ensure interoperability with DoD- and AF- provided enterprise-wide solutions for remediation of vulnerabilities for endpoint devices.

4.1.5. ISSMs and ISSOs protect ISs, their operating system, peripherals (media and devices), applications, and the information it contains against loss, misuse, unauthorized access, or modification. Ensure compliance with AFMAN 33-282 and MPTO 00-33B-5006, End-point Security for Information Systems. These procedures ensure the computing environment complements the AF IS cybersecurity program. MPTO 00-33B-5006 provides standard procedures derived from cybersecurity controls and other measures for organizations to maintain the confidentiality, integrity, and availability of any AF IS cybersecurity program

4.1.6. All authorized users ensure protection of all ISs against tampering, theft, and loss. Protect ISs from insider and outsider threats by controlling physical access to the facilities and data by implementing procedures identified in Joint, DoD, AF publications, and organizationally created procedures. Basic end point security procedures are located in MPTO 00-33B-5006.

4.2. Cybersecurity Workforce Training and Certification. This instruction and supporting cybersecurity specialized publications standardize the naming conventions and functions of AF organizational (management) and IT level (technical or system-level) Cybersecurity personnel. These documents also prescribe training and certification requirements according to national and DoD policy consistent with and supplementary to the guidance outlined in AFMAN 33-285, Information Assurance (Cybersecurity) Workforce Improvement Program.

4.3. Information Assurance Workforce System Architecture and Engineering. IAW DoD 85701-M and AFMAN 33-285, personnel required to perform any IA Workforce System Architecture and Engineering (IASAE) specialty functions (one or more functions) at any level must be certified to the highest level functions(s) performed. **(T-1)**.

4.3.1. Cybersecurity privileged user or management functions, see AFMAN 33-285.

4.3.2. AO and other A&A training requirements, see AFMAN 33-285.

4.3.3. COMPUSEC training and requirements, see AFMAN 33-282

4.3.4. COMSEC training requirements follow guidance in AFMAN 33-283

4.3.5. TEMPEST training requirements, see AFMAN 33-286.

4.4. Cybersecurity Inspections. Cybersecurity disciplines are assessed under the Air Force Inspection System (AFIS) IAW AFI 90-201 and through self-assessments communicators (SACs) located in MICT.

4.4.1. Inspectors/auditors perform inspections according to guidance in this instruction and applicable AF Cybersecurity publications for COMSEC, COMPUSEC, and TEMPEST (Formerly known as EMSEC).

4.4.2. ISOs comply with formal testing and certification activities according to AFI33-210.

4.4.3. Inspect or assess performance measures and metrics based on enterprise-wide (and individual elements where appropriate) cybersecurity performance and assess cybersecurity trends. Limit the measurements and metrics to Federal and DoD Cybersecurity reporting requirements.

4.4.4. Inspect AF PKI Local Registration Authorities (LRAs) in accordance with AFMAN 33-282 and associated MICT section.

4.5. Notice and Consent Monitoring and Certification. All AF installations, AF organizations on joint bases, circuits, and ISs must comply with DoD notice and consent certification requirements for monitoring to occur by authorized activities as well as comply with installation certification procedures IAW AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP) (to become Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process). **(T-0)**.

4.6. Connection Management.

4.6.1. AF activities must adhere to the DISA Connection Approval Process if the system is connected to the Non-Secure Internet Protocol Router Network (NIPRNET) or Secure Internet Protocol Router Network (SIPRNET). **(T-0).** Connection Approval Process information can be found at **http://www.disa.mil/connect**. For all AF ISs accessing the DISN, get appropriate service (e.g., DISA) coordination and authorization before proceeding with combatant command coordination and/or Joint Staff approval.

4.6.2. AF activities comply with AFMAN 33-210 for connection approval to the Air Force Information Networks (AFIN).

4.6.3. AF A6S provides AF representation to the DSAWG. The DSAWG represents the DISN community and advises the DISN AOs of community acceptance or rejection of risk. DISN connection decisions rest with the DISN AOs. AF A6S work with AF activities involved in the adjudication of conflicts related to DISN connection decisions.

4.7. Commercial Internet Service Providers (ISPs). The only DoD authorized access to the Internet is via a NIPRNET connection.

4.7.1. Organizations requiring a connection (wired or wireless) to the Internet via a fixed Commercial ISP solution must accredit the system and submit an AF Form 4169, Request for Waiver from Cybersecurity Criteria, through their WCO through AFSPC's Cyberspace

Support Squadron (CYSS) to SAF CIO/A6SC, the AF representative to the DoDIN Waiver Panel (GWP) IAW CJCSI 6211.02D. **(T-2)**. Use AF Form 4169 to document the request and prepare a DoDIN waiver brief in accordance with the DISA, "DISN Connection Process Guide" (**http://www.disa.mil/connect/waivers**). This applies to all Commercial ISP connection requests IAW AFI 33-115.

4.7.2. Use of mobile air cards and/or mobile hotspots for Temporary Duty (TDY)/mobile usage does not require a Commercial ISP waiver. Obtain approved devices and mobile data service through IT Commodity Council (ITCC) approved contracts. Use of these devices and services is not to be permanent. Configure all mobile hotspots and devices to applicable DISA Wireless STIGs. Use only approved encryption solutions (e.g. Cisco VPN Client, Juniper Network Connect, Citrix). Refer to DISA STIGs for use of mobile hotspot feature on Commercial Mobile Devices (CMDs)/smartphones. Organizations that use DoD devices that attach to the NIPR via these means must ensure they connect through a VPN first. **(T-2)**. Any other configuration is unauthorized.

4.8. Cross-Domain Solutions (CDS). Cross Domain Solutions (CDS). A CDS is a form of controlled interface providing the ability to manually and/or automatically access and/or transfer information between different security domains (e.g., between unclassified and classified). A CDS requires an additional approval process and authorization, separate from the review and approval for the Authorization to Connect (ATC) for the Command Communications Service Designator (CCSD). Developers and users refer to the CDS guidance, use only CDS-approved devices evaluated and validated through Certification Test and Evaluation or have a sufficient body of evidence to allow the Air Force Cross Domain Support Element (AF CDSE) to conduct a thorough risk analysis and adhere to CDS configuration guidelines. The purpose of and approval procedures for CDS are extracted from DoD, DISA, NSA, and the Unified Cross Domain Systems Management Office (UCDSMO) policies and guidance. For guidance on the most current CDS process, contact the AF CDSE, consult DoDI 8540.01, Cross Domain (CD) Policy, or visit the DISA Mission Partners website at **http://disa.mil/Services/Network-Services/Enterprise-Connections/Mission-Partner-Training-Program**.

4.8.1. Send all requests for CDSs and coalition information sharing solutions to AF CDSE at **nac.csni@us.af.mil** (**https://intelshare.intelink.gov/sites/afcdse/SitePages/Home.aspx**). This office provides the most current guidance for the CDS approval process..

4.8.2. The UCDSMO maintains a baseline list of NSA-certified solutions available for reuse contingent on approval by the DSAWG (available on SIPRNet at **https://intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx**)

4.9. Security Configuration Management and Implementation. The ISSO (or designee) will comply with the following:

4.9.1. Securely configure and implement all IT products. **(T-1).** Cybersecurity reference documents, such as NIST SPs, DISA STIGs (**http://iase.disa.mil/stigs/**),NSA Security Configuration Guides, and other relevant publications are used as security configuration and implementation guidance. ISSOs will apply these reference documents according to this policy and AFMAN 33-210 to establish and maintain a minimum baseline security configuration and posture. **(T-1)**.

4.9.2. Review all changes to the configuration of IT (i.e., the introduction of new IT, changes in the capability of existing IT, changes to the infrastructure, procedural changes, or changes in the authorized or privileged user base, etc.) for cybersecurity impact prior to implementation. **(T-2)**. Document all configuration management and security requirements in the IT A&A package according to AFMAN 33-210 and CJCSI 6510_01F. **(T-0)**.

4.9.3. NIST Cryptographic Module Validation Program (CMVP) for Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, validation. **(T-0)**: **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm**

4.9.4. Leverage and update DISA Approved Products List Integrated Tracking System (APLITS). **https://aplits.disa.mil/** **(T-1)**

4.10. IT Acquisitions and Procurement. All acquisition and cybersecurity personnel must ensure cybersecurity is implemented in all IT acquisitions at levels appropriate to the system characteristics and requirements throughout the acquisition life cycle, according to AFI 63-101 and AFMAN 33-153.

4.10.1. All acquisition and cybersecurity personnel must ensure all IT hardware, firmware, and software components or products incorporated into DoDIN comply with evaluation and validation requirements in DoDI 8500.01 and CNSSP 11. **(T-1)**. Refer to CNSSP No. 11 for the latest process and policy guidance on this subject. Limit products to those listed on any of the lists below:

4.10.1.1. NSA-certified "TEMPEST" products: **https://www.nsa.gov/applications/ia/tempest/tempestPOCsCertified.cfm**

4.10.1.2. Common Criteria Evaluation and Validation Scheme (CCEVS): **http://www.commoncriteriaportal.org/products** and **http://www.niap-ccevs.org**

4.10.1.3. DoD Unified Capabilities Approve Products List (UC APL): **https://aplits.disa.mil/**

4.10.1.4. AF Evaluated Products List (AF EPL) **https://cs.eis.af.mil/afdaa/Lists/COTSGOTS%20Software/EPL.aspx**

4.10.1.5. Product Director Automated Movement and Identification Solutions ((PDAMIS) @**http://www.pdamis.army.mil**

4.10.2. Cybersecurity and Cybersecurity-enabled products are documented within the IS A&A package according to AFMAN 33-210.

4.10.3. WCOs, ISSOs, and ISSMs must ensure the procurement activities of all IT hardware, cellular, and peripheral devices (e.g., desktops, laptops, servers, BlackBerry® devices, tablets, cell phones, printers, scanners) follow the guidance in AFMAN 33-153, and the AF ITCC guidance available on the AF Portal. **(T-2)**.

4.10.4. WCOs, ISSOs, and ISSMs must ensure the procurement of telephone/voice switches is coordinated with Air Force Office of Special Investigations (AFOSI) for Technical Surveillance Countermeasures (TSCM) program. **(T-1)**.

4.10.5. IAW AFI 71-101, Volume 3, Air Force Technical Surveillance Countermeasure Program, the acquisition of voice systems require certification through the UC APL.

4.11. Air Force KMI. The Air Force Lifecycle Management Center (AFLCMC) manages the Air Force KMI program. KMI is the framework and services that provide the generation, production, storage, protection, distribution, control, tracking and destruction for all cryptographic keying material, symmetric keys as well as public keys and PKI certificates. The KMI system is comprised of nodes that provide the means to deliver cryptographic products, key management products and services to a large and diverse community of globally distributed users. ISOs and Cybersecurity professionals implement key management procedures according to AFMAN 33-283.

4.12. Public Key Infrastructure (PKI). The AF PKI SPO (AFLCMC/HNCYP) is responsible for the integration, implementation and sustainment of the DoD PKI, NSS PKI, AF PKIs, external federated PKIs and associated identity and access control management (ICAM) technologies to deny anonymity to our adversaries within the AF and associated COCOM systems. PKI authenticates users and systems on all AF networks via multiple, interoperable PKIs. PKI digital certificates provide both human identity credentials as well as non-person entity (NPE) identity credentials for all personnel, systems, services, devices, applications and data across all AF networks. ISOs and Cybersecurity professionals implement PKI, ICAM and Identity and Access Management (IdAM) procedures in accordance with AFMAN 33-282.PKI is implemented by AF ISOs and Cybersecurity professionals through the use of hardware tokens (CAC, AFNET-S token, Alternate Login Token (ALT), and Volunteer Logical Access Credential (VoLAC)) and software certificates on both AFNET and AFNET-S according to procedures in AFMAN 33-282.

4.13. System Security Engineering (SSE). Cybersecurity is to be integrated into the overall system acquisition and engineering process throughout the entire system life cycle via the information system's security engineering (SSE), according to DoDI 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering.*

4.14. COMPUSEC. The framework of the AF COMPUSEC IA program consists of a cyclic sequential security management model for risk management. This model is specific to information processed on AF computing systems and incorporates strategy, policy, awareness/training, implementation, assessment, remediation, and mitigation controls IAW AFMAN 33-283.

4.15. Communications Security. COMSEC refers to measures and controls taken to deny unauthorized persons information derived from ISs of the United States Government related to national security and to ensure the authenticity of such ISs. COMSEC protection results from applying security measures (i.e., crypto security, transmission security, etc.) to communications and ISs generating, handling, storing, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes applying physical security measures to COMSEC information or materials. Ensure all COMSEC activities comply with AFMAN 33-283 and associated AF Cybersecurity publications.

4.16. TEMPEST. TEMPEST denies interception and exploitation of classified, and in some instances unclassified, information by containing compromising emanations within a facility where information is being processed. Refer to AFMAN 33-286 for implementing countermeasures to protect against compromising emanations.

4.17. Operations Security (OPSEC). The OPSEC program is an operations function or activity and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. To ensure effective implementation across organizational and functional lines the organization's OPSEC Program Manager (PM), Signature Management Officer (SMO), or coordinator resides in the operations and/or plans element of an organization or report directly to the commander. For additional information see AFI 10-701, Operations Security (OPSEC).

4.18. Incident Response and Reporting. An incident is defined as an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS; or the information the IS processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security polices, security, procedures, or acceptable use policies (see CNSSI 4009).

4.18.1. For reportable cyber incidents (e.g., unauthorized access, denial of service, and malicious logic) in the AF network response hierarchy, refer to AFI 10-1701.

4.18.2. For any other service incident, which is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service, contact the applicable helpdesk.

4.18.3. For COMPUSEC incidents refer to AFMAN 33-282.

4.18.4. For COMSEC incidents refer to AFMAN 33-283.

4.19. Mobile Code. Comply with DoDI 8500.01 to protect ISs from the threat of malicious or improper use of mobile code during system acquisition and fielding. System developers and implementers follow guidelines in all applicable STIGs. Additional mobile code guidance is in AFMAN 33-282.

4.20. Ports, Protocols, and Services (PPS). The AF PPS Management Program provides policy and procedures on the use of PPS across the AFIN, consistent and complementary with the implementation of DoDI 8551.01, Ports, Protocols, and Service Management (PPSM), for additional PPS requirements, see AFSSI 8551, Ports, Protocols, and Services (PPSM) Management.

4.21. Physical Security. Access to and Physical Protection of Computing Facilities. Employ physical security measures (i.e., access control, visitor control, physical control, testing, etc.) for network and computing facilities that process publicly releasable, sensitive, or classified information to only authorized personnel with appropriate clearances and a need-to-know according to AFJI 31-102, Physical Security and DoD 5200.08-R, Physical Security Program.

4.22. Information Security. Comply with AFI 16-1404 for workplace security procedures and storage of documents and IT equipment.

4.23. Malicious Logic Protection. Protect AF IT from malicious logic (e.g., virus, worm, Trojan horse) attacks by applying a mix of human and technological preventative measures according to DoD 8500.01 and AFMAN 33-282. Continuous monitoring and patching of IS and PIT systems are mandated per AFMAN 33-210.

4.24. Data Encryption. Protect sensitive information; Controlled Unclassified Information (CUI); For Official Use Only (FOUO); Personally Identifiable Information (PII); Health Insurance Portability and Accountability Act (HIPAA); Privacy Act (PA); in transit and at rest with strong encryption, IAW DoD CIO Memorandum, and USCYBERCOM CTO 08-001, Encryption of Sensitive Unclassified Data at Rest (DaR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD) and this instruction. For additional encryption requirements see, AFMAN 33-282.

4.25. Mobile Computing Devices. Mobile computing devices are IS devices such as Portable Electronic Devices (PEDs), laptops, and other handheld devices that can store data locally and authenticate to AF-managed networks through mobile access capabilities. Refer to AFMAN 33-282 for additional information on protections, deployment, use of Software Certificates and support of mobile computing devices.

4.26. Personal Activity Monitor (PAM) / Wearable Technology. Any non-stationary electronic apparatus with the capability of detecting, recording, storing, and or transmitting information about an individual's activity level, biological functions, or similar activities related to health and fitness. For additional information refer to AFMAN 33-282.

4.27. Wireless Services. WCOs, ISSOs, and ISSMs must ensure wireless services integrated or connected to AF ISs comply with DoDI 8500.01and DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). **(T-0).** Refer to AFMAN 33-282 for additional information on protections, deployment and support of wireless services.

4.28. Non-Air Force IT utilized on AF installations.

4.28.1. Privately-owned Hardware and Software. Privately-owned hardware and software connected to the AFIN and used to process unclassified and/or unclassified sensitive information requires operational mission justification and AFIN AO approval. Document the approval between the user and government organization. The organizational ISSO maintains the documentation and provides it to the system ISSM as required. For additional information see AFMAN 33-282.

4.29. Peripheral Devices. A computer peripheral is any external device that provides input and output for the computer. Inputs devices transmit data and/or commands to a desktop or laptop (e.g. mouse, scanners, Smart boards, pointers, and keyboards). Output devices receive data from the desktop or laptop providing a display or printed product (e.g. monitors, printers, and multi-function devices (MFDs)). Refer to AFMAN 33-282 for additional information on the protections for peripheral devices.

4.30. Removable Media. Removable media is any type of storage media designed to be removed from a computer. This includes external hard drives, optical media (e.g., CDs, DVDs) and flash media (e.g., memory cards, USB flash drives, and solid-state drives). Refer to AFMAN 33-282 for additional information on removable media handling, configuration and use.

4.31. Collaborative Computing. Collaborative computing provides an opportunity for a group of individuals and/or organizations to share and relay information in such a way that cultivates team review and interaction in the accomplishment of duties and attainment of mission accomplishment. Configure and control collaborative computing technologies to prevent unauthorized users from seeing and/or hearing national security information and material at another user's workstation area. Establish safeguards to ensure the integration of data from various sources does not result in the creation of a higher classified data on ISs that are not rated to store or process at the higher level. Such instances are considered spillage and WCOs, ISSOs, and ISSMs must address these. **(T-1)**. Refer to AFMAN 33-282 for additional information on collaborative computing and provisions on its deployment and use.

4.32. Spillage. This is when data is found on a system that has a lower security classification than that of the data. This term is also used when PII is found on a system that is not approved for processing, storing or transmitting of PII data. Refer to AFMAN 33-282, for additional information on spillage and incident reporting.

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

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Title 5 USC § 552a, *The Privacy Act of 1974, as amended* January 7, 2011

Title 10 USC § 2224, *Defense Information Assurance Program*, January 7, 2011

Title 44 USC § 3541, *Information Security (Federal Information System Management Act)*, December 17, 2002

Title 44 USC § 3602, *Office of Electronic Government*, December 17, 2002

OMB Circular A-130, *Management of Federal Information Resources*, November 28, 2000

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

CNSSP 26, *National Policy on Reducing the Risk of Removable Media for National Security Systems*, November 2010

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

CNSSI 4031, *Cryptographic High Value Products*, 16 February 2012

NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Rev 1, February 2010

NIST 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011

NIST-SP 800-46, *Guide to Enterprise Telework and Remote Access Security,* April 2010

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

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

NSTISSAM TEMPEST/2-95A, *Red/Black Installation Guidance*, February 3, 2000

NSTISSI 4003, (FOUO) *Reporting and Evaluating COMSEC Incidents (U)*, December 2, 1991

CNSSI 4005, (FOUO) *Safeguarding Communications Security (COMSEC) Facilities and Materials*, August 22, 2011

CNSSI No. 4016, (FOUO) *National Information Assurance Training Standard For Risk Analysis*

CNSSI 4031, *Cryptographic High Value Products (CHVP)*, February 16, 2012

CNSSP 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, June 10, 2013

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

NSA/CSS Policy Manual 9-12, *NSA/CSS Storage Device Declassification Manual,* March 13, 2006

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

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

CJCSM 6510.01B, *Cyber Incident Handling Program*, July 10, 2012

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, December 15, 2014

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

FIPS140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001

DoDM 1000.13 v1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, DISA Security Technical Implementation Guides (STIGs), **http://iase.disa.mil/stigs/**

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

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

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

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

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

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

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

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

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

DoDI 5200.02,*DoDPersonnel Security Program (PSP),* March 21, 2014

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

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, January 24, 2012

DoDI 3200.12, *DoD Scientific and Technical Information Program (STIP),* August 22, 2013

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

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

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, August 18, 1995

DoDD 5400.7, *DoD Freedom of Information Act (FOIA) Program*, July 28, 2011

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009

DoDD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, April 14, 2004

DoDD 8500.01, *Cybersecurity*, March 14, 2014

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

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

DoDI 1100.21, *Voluntary Services in the Department of Defense*, December 26, 2002

DoDI 5134.16, *Deputy Assistant Secretary of Defense for Systems Engineering* (DASD(SE)),” August 19, 2011

DoDI 5205.08, *Access to Classified Cryptographic Information*, November 8, 2007

DoDI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/Cybersecurity) Activities*, January 29, 2010

DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, November 3, 2009

DoDI 8510.01, *DoD Risk Management Framework (RMF)*, March 12, 2014

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

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

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

DoDI 8540.01, *Cross Domain (CD) Policy*, May 8, 2015

DoDI 8550.01, *DoD Internet Services and Internet-based Capabilities*, September 11, 2012

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM),*May 28, 2014

DoDI 8580.1, *Information Assurance (Cybersecurity) in the Defense Acquisition System*, July 9, 2004

DoDI 8581.01, *Information Assurance (Cybersecurity) Policy for Space Systems Used by the Department of Defense*, June 8, 2010

DoDI 8582.01, *Security of Unclassified DoD Information on Non-DoD Information Systems,* June 6, 2012

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

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

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

AFI 10-710, Information Operations Condition (INFOCON), August 10, 2006

AFI 10-712, Telecommunications Monitoring and Assessment Program (TMAP), June 8, 2011

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

AFI 16-201, Air Force Foreign Disclosure and Technology Transfer Program, July 23, 2014

AFJI 31-102, *Physical Security*, May 31, 1991

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

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

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

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

AFI 33-115, Information Technology Service Management

AFMAN 33-283, *Communications Security (COMSEC) Operations*, September 3, 2014

AFMAN 33-210, *Air Force Assessment and Authorization (A&A) Program (AFAAP), TBD),* December 23, 2008

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

AFI 33-360, Publications and Forms Management, September 25, 2013

AFI 33-401, Air Force Architecting, May 17, 2011

AFI 36-2201, Air Force Training Program, September 15, 2010

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

AFI 63-101/20-101, Integrated Life Cycle Management, March 7, 2013

AFI 71-101 Volume 3, The Air Force Technical Surveillance Countermeasures Program, January 16, 2013

AFI 90-201, The Air Force Inspection System, August 2, 2013

AFKAG-2L, (FOUO) *Air Force COMSEC Accounting Manual*, May 15, 2007

AFMAN 33-145, *Collaboration Services and Voice Systems Management,* September 6, 2012

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

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

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

AFMAN 33-407, *Air Force Clinger-Cohen Act (CCA) Compliance Guide,* 24 October 2012*Air Force Records Information Management System Records Disposition Schedule (RDS)*

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

624 OC TASKORD 2012-76-014, *Classified Message Incident (CMI) Declaration Authority & Handling Procedures*

MPTO 00-33A-1109, *Vulnerability Management*

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

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

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

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

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

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

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

Prescribed Forms:

AF Form 4167, Two-Person Control (TPC) COMSEC Material Inventory

AF Form 4170, Emission Security Assessments/Emission Security Countermeasures Reviews

Adopted Forms:

SF 312, Nondisclosure Agreement

SF 700, Security Container Information Form

DD Form 2875, System Authorization Access Request (SAAR)

DD Form 2946, DoD Telework Agreement

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

AF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

AF —Air Force (as used in forms)

AF CTTA —Certified TEMPEST Technical Authority (CTTA)

AFCTAG -- AF —Cybersecurity Technical Advisory Group

AFI —Air Force Instruction

AFIA —Air Force Inspection Agency

AFIN —Air Force Information Networks

AFIS —Air Force Inspection Service

AFKAG —Air Force Cryptographic Aid, General

AFMAN —Air Force Manual

AFNET —The Air Force’s underlying Non-Secure Internet Protocol Router Network (NIPRNet)

AFNET-S —The Air Force’s underlying Secure Internet Protocol Router Network (SIPRNet)

AFNIC —Air Force Network Integration Center

AFOSI —Air Force Office of Special Investigations

AFPC —Air Force Personnel Center

AFPD —Air Force Policy Directive

AFRIMS —Air Force Records Information Management System

AFRMC —Air Force Risk Management Council

AFSC —Air Force Specialty Code

AFSPC —Air Force Space Command

AFSSI —Air Force Systems Security Instruction

ALT —Alternate Logon Token

ALTSECID —Alternate Security Identification

AIS —Automated Information System

AO —Authorizing Official

ATO —Authorization to Operate

A&A —Assessment & Authorization (formerly C&A)

C2 —Command and Control

CA —Certificate Authority

CAC —Common Access Card

CAM —COMSEC Account Manager

CAP —Cryptographic Access Program

CCB —Configuration Control Board

CCEVS —Common Criteria Evaluation and Validation Scheme

CDC —Cleared Defense Contractors

CDS —Cross-Domain Solutions

CDSE —Cross Domain Service Element

CDSO —Cross Domain Solution Office

CE —Computing Environment

CHVP —Cryptographic High Value Products

CI —Counterintelligence

CIA —Confidentiality, Integrity, Availability

CIO —Chief Information Officer

CITS —Combat Information Transport System

CJCSI —Chairman of the Joint Chiefs of Staff Instruction

CJCSM —Chairman of the Joint Chiefs of Staff Manual

CM —Configuration Management

CMI —Classified Message Incident

CMVP —Cryptographic Module Validation Program

CND —Computer Network Defense

CNSSI —Committee on National Security Systems Instruction

CNSSP —Committee on National Security Systems Policy

COCOM —Combatant Command

COI —Community of Interest

COMPUSEC —Computer Security

COMSEC —Communications Security

CoN —Certificate of Networthiness

CTO —Communications Tasking Order

CTS —Computerized Telephone Switch

CTTA —Certified TEMPEST Technical Authority

CUI —Controlled Unclassified Information

Cybersecurity —Information Assurance

CybersecurityAP —Cybersecurity Assessment and Assistance Program

CYSS —Cyberspace Support Squadron

DAMO —Damage Assessment Management Office

DaR —Data at Rest

DC3 —Department of Defense Cyber Crime Center

DCS —Defense Collaboration Services

DFARS —Defense Federal Acquisition Regulation Supplement

DIB —Defense Industrial Base

DISA —Defense Information Systems Agency

DoD —Department of Defense

DoDD —Department of Defense Directive

DoDI —Department of Defense Instruction

DoDIN —Department of Defense Information Network

DRU —Direct Reporting Unit

DSAWG —Defense Information Assurance Security Accreditation Working Group

DSS —Defense Security Service

DVD —Digital Versatile Disc

EIEMA —Enterprise Information Environment Mission Area

EITDR —Enterprise Information Technology Data Repository

eMASS —Enterprise Mission Assurance Support Service

EMSEC —Emission Security

EPL —Evaluated Products List

FAR —Federal Acquisition Regulation

FIPS —Federal Information Processing Standards

FISMA —Federal Information Management Security Act

FOA —Field Operating Agency

FOIA —Freedom of Information Act

FOUO —For Official Use Only

GIG —Global Information Grid

GWP —GIG Waiver Panel

HAF —Headquarters Air Force

HBSS —Host Based Security System

HIPAA —Health Insurance Portability and Accountability Act

HQ —Headquarters

HQ AETC —Headquarters Air Education and Training Command

HQ AFSPC —Headquarters Air Force Space Command

IAM —Information Assurance Manager

IAO —Information Assurance Officer

IAW —In accordance with

ICD —Intelligence Community Directive

ID —Identification

IMT —Information Management Technology

INFOCON —Information Condition

IPT —Integrated Process Teams

IS —Information System

ISSM —Information System Security Manager

ISO —Information System Owner

ISSE —Information System Security Engineering/ Engineer

ISSM —Information System Security Manager

ISSO —Information System Security Officer

IT —Information Technology

JP —Joint Publication

KMI —Key Management Infrastructure

KS —Knowledge Service

LRA —Local Registration Authority

MAO —Mission Area Owner (Component [AF] level PAO)

MAJCOM —Major Command

MFD —Multifunction Device

MICT —Management Control Internal Tool

MOU —Memorandum of Understanding

MPTO —Methods and Procedures Technical Orders

NC3 —Nuclear Command Control and Communications

NIPRNet —Non-Secure Internet Protocol Router Network

NIST —National Institute of Standards and Technology

NSTISSI —National Security Telecommunications and Information Systems Security Instruction

NSTISSP —National Security Telecommunications and Information Systems Security Policy

NTSWG —National Telephone Security Working Group

NSA —National Security Agency

NSA/CSS —National Security Agency/Central Security Service

NSS —National Security System

OMB —Office of Management and Budget

OPR —Office of Primary Responsibility

OPSEC —Operations Security

OSI —Office of Special Investigations

PAO —Principle Authorizing Official

PED —Portable Electronic Device

PEO —Program Executive Officer

PII —Personally Identifiable Information

PIN —Personal Identification Number

PIT —Platform Information Technology

PIV —Personal Identity Verification

PIV-I —Personal Identity Verification-Interoperable

PK —Public-Key

PKCS —Public-Key Cryptography Standards

PKI —Public Key Infrastructure

PM —Program Manager

PMO —Program Management Office

POA&M —Plan of Actions and Milestones

PPS —Ports, Protocol, and Services

PPSM —Ports, Protocol, and Services Management

RDS —Records Disposition Schedule

RMF —Risk Management Framework

SAAR —System Authorization Access Request

SACs —Self-Assessments Communicators

SAF —Secretary of the Air Force

SAISO —Senior Agency Information Security Officer

SAP/SAR —Special-Access Program/Special Access Required

SCA —Security Control Assessor

SCAR -- SCA —Representatives

SCI —Sensitive Compartmented Information

SCIF —Sensitive Compartmentalized Information Facility

SDLC —Software Development Life Cycle

SECAF —Secretary of the Air Force

SF —Standard Form

SIPRNet —Secret Internet Protocol Router Network

SISO —Senior Information Security Officer

SME —Subject Matter Expert

SME PED —Secure Mobile Environment Portable Electronic Device

SPO —System Program Office

SP —Special Publications

STIG —Security Technical Implementation Guide

STIP —Scientific and Technical Information Program

SVRO —Secure Voice Responsible Officers

SwA —Software Assurance

TAG —Technical Advisory Group

TDY —Temporary Duty

TMAP —Telecommunications Monitoring and Assessment Program

TO —Technical Order

TSCM —Technical Surveillance Countermeasures

UC —Unified Capabilities

UC APL —Unified Capabilities Approved Products List

UCDSMO —Unified Cross Domain Services Management Office

US —United States

USB —Universal Serial Bus

U.S.C. —United States Code

USCYBERCOM —United States Cyber Command

USSTRATCOM —United States Strategic Command

USM —Unit Security Manager

VoLAC —Volunteer Logical Access Credential

VPN —Virtual Private Network

VTC —Video Teleconferencing

WCO —Wing Cybersecurity Office

WIP —Workforce Improvement Program

WLAN —Wireless Local Area Network

Terms

AF CTTA —(Air Force Certified TEMPEST Technical Authority) An experienced, technically qualified government employee who has met established certification requirements according to CNSS-approved criteria (see CNSSP-300 and CNSSI 7000 (C/REL)), and is appointed by SAF/CIO A6 SISO to fulfill CTTA responsibilities. (AFMAN 33-286).

AFCTAG —(Air Force Cyber Security Technical Advisory Group) provides technical cybersecurity subject matter experts (SMEs) from across the MAJCOMs and functional communities to facilitate the management, oversight, and execution of the AF Cybersecurity Program. (See Figure 3.1).

AFIN —(Air Force Information Network) 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, policy-makers, 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. (AFI 10-1701).

AFRMC —(Air Force Risk Management Council) Provides a forum for senior cybersecurity professionals to validate and vet issues concerning cybersecurity risk from a mission and business perspective. (See Figure 3.1).

ALT —(Alternate Logon Token) A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions. (AFMAN 33-282).

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

ATO —(Authorization to Operate) The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST 800-37, Rev. 1).

A&A —(Assessment & Authorization) (formerly C&A) The process by which organizations: (i) categorize information and information systems; (ii) select security controls; (iii) implement security controls; (iv) assess security control effectiveness; (v) authorize the information system; and (vi) [conduct] ongoing monitoring of security controls and the security state of the information system. (NIST 800-37, p. 4 *adapted*).

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

CTO —(Cyber Tasking Order) An operational type order issued to perform specific actions at specific time frames in support of AF and Joint requirements. (AFI 10-1701).

Cybersecurity —(Information Assurance) 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. (CNSSI 4009).

CYSS —(Cyberspace Support Squadron) Provides cyber networking expertise to AFSPC for Cyberspace Lead MAJCOM activities and functions.

DAMO —(Damage Assessment Management Office) Conducts damage assessments by collaboratively analyzing information compromised as a result of cyber intrusions to Defense Industrial Base information systems to determine overall impact to current and future Air Force weapons programs, scientific and research projects, and warfighting capabilities. (DoDI 5205.13, *adapted*).

DaR —(Data at Rest) Information that resides on electronic media while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. Data at rest can be archival or reference files that are changed rarely or never. Data at rest also includes data that is subject to regular but not constant change. (DoDI 8580.02-R).

DC3 —(Department of Defense Cyber Crime Center) Provides digital and multimedia (D/MM) forensics, cyber investigative training, research, development, test and evaluation (RDT&E), and cyber analytics for the following DoD mission areas: information assurance (IA) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT). (**https://www.dc3.mil/index/about-dc3**).

EIEMA —(Enterprise Information Environment Mission Area) IEMA is the DoD information (IT) portfolio that manages investments in the current and future integrated information sharing, computing and communications environment of the Air Force Information Network (AFIN). The IE comprises AFIN assets that operate as, provide information transport for, perform enterprise management of, and assure various levels and segments of the enterprise network, ranging from local area to wide area networks and from tactical to operational and strategic networks. The domains are Communications, Computing Infrastructure, Core Enterprise Services, and Information Assurance. (DoD CIO Memorandum, *Enterprise Information Environment Mission Area (EIEMA) Domain Owner Designations*, dated July 14, 2004).

EITDR —(Enterprise Information Technology Data Repository) EITDR is the Air Force IT Portfolio Management system of record. EITDR is accessible through the Air Force Portal. EITDR contains a current inventory of initiatives, systems, and system-related data and is used for internal management and oversight as well as to provide information to external sources to satisfy statutory and regulatory requirements. (AFI 33-141)

eMASS —(Enterprise Mission Assurance Support Service) eMASS is a government-owned, government-off-the-shelf (GOTS) web-based application, which supports cybersecurity program management. EMASS is fully compliant with security controls-based cybersecurity.

eMASS is designed to operate in either the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) enclave or the Secret Internet Protocol Router Network (SIPRNet) enclave. eMASS is public-key enabled (PKE) and all data in transit is fully encrypted. (**https://emass-airforce.csd.disa.mil/Content/Help/eMASS%205.1%20User%20Guide.pdf**).

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

ISSE —(Information System Security Engineering/ Engineer) Individual assigned responsibility for conducting information system security engineering activities. (NIST 800-37).

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

ISSO —(Information System Security Officer) Individual assigned responsibility by the senior agency information security officer (SISO), authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (CNSSI 4009).

IT —(Information Technology) (A) The term "information technology," with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (40 U.S.C., Sec. 1401)

MAO —(Mission Area Owner) The person responsible for a defined area of responsibility with functions and processes that contribute to mission accomplishment. (DoDD 8115.01).

PED —(Portable Electronic Device) Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders. (ICS 700-1)

PIT —(Platform Information Technology) IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. (DoDI 8500.01).

RMF —(Risk Management Framework) A structured approach used to oversee and manage risk for an enterprise. (CNSSI 4009).

SCA —(Security Control Assessor) The individual, group, or organization responsible for conducting a security control assessment. (NIST 800-37).

Security Control Assessment —The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST 800-37).

SISO —(Senior Information Security Officer) Official responsible for carrying out the chief information officer (CIO) responsibilities under the Federal Information Security Management Act (FISMA) and serving as the CIO's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers. (CNSSI 4009).