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