BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 17-130

13 FEBRUARY 2020

Cyberspace

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/CNZ

Certified by: SAF/CNZ
(Ms. Wanda Jones-Heath, SES)

Supersedes: AFI33-200, 31 August 2015

Pages: 21

This instruction implements Air Force Policy Directive 17-1, *Information Dominance Governance and Management* and is consistent with Headquarters Mission Directive 1-26, *Chief, Information Dominance and Chief Information Officer*, and Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*; these documents should be reviewed to understand the Cybersecurity Program. The National Institute of Standards and Technology Special Publication (NIST SP) 800-39 was also used in developing the cybersecurity program. This publication applies to all civilian employees and uniformed members of the Regular Air and Space Forces, Air and Space National Guard, Air and Space Force Reserve, as well as to Department of the Air Force contractors when required by the terms of their contracts. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Refer recommended changes and questions to the Office of Primary Responsibility on AF Form 847, *Recommendation for Change of Publication*. Route AF Forms 847 through the appropriate functional chain of command to the Office of the Chief Information Security Officer (SAF/CNZ), **usaf.pentagon.saf-cn.mbx.cnz-worflow@mail.mil**. Any level may supplement this publication, but must route all direct supplements to the Office of Primary Responsibility of this publication for coordination prior to certification and approval. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*,

and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System.

SUMMARY OF CHANGES

This document is substantially changed and must be reviewed in its entirety. The document collapses previous technical and redundant information into functions. The short paragraphs reference specific instructions, policy, directives, issuances, and guides for the technical details. The document introduces the Cybersecurity Framework as the basis for the cybersecurity program.

Chapter 1

OVERVIEW

1.1. Threats and vulnerabilities: Are found every day that provide unauthorized access to information technology (IT). Cybersecurity represents the measures taken to protect Air Force information on information technology from criminal or unauthorized use. A cybersecurity program must incorporate many functions in order to balance the cybersecurity risk with the capabilities required for mission success. Each program must maintain a planned program lifecycle from the initial requirement that creates the program through decommissioning and disposal of the program. The program lifecycle must prepare for the changing cybersecurity environment to ensure hardware and software transition to a continuous risk monitoring environment, else the risk becomes too great. Throughout the IT's lifecycle, the cybersecurity risk must be continuously monitored to balance capability for the mission while minimizing risk to the overall cyber ecosystem or environment. This publication applies to all IT that receives, processes, stores, displays, or transmits Air Force information to protect the device and prevent information from misuse.

1.2. Cybersecurity threats: Affect all forms of IT from traditional office IT (networked, closed network, and standalone) to non-traditional IT like weapon systems and control systems (e.g., utility generation or distribution, access control, building automation, etc.) with embedded network-enabled IT, operational capabilities, and automation. A cybersecurity program must consider the distinct, traditional and non-traditional cybersecurity factors.

1.3. The cybersecurity program provides: Authorizing Officials (AOs), Information System Owners, Program Managers, Information System Security Managers, mission owners, and authorized users a way to balance the confidentiality, integrity, availability, and non-repudiation of Air Force information with the threats, vulnerabilities, and risk to the IT's capabilities. This balance provides a way for all stakeholders to accept a level of risk while maintaining the capability for the mission.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Deputy Chief Information Officer (SAF/CN). Appointed by the Under Secretary of the Air Force, the Chief Information Officer (CIO).

2.1.1. Coordinates with the Under Secretary of the Air Force, on cybersecurity matters.

2.1.2. Represents the cybersecurity interests in the Air Force Risk Executive Function.

2.2. Chief Information Security Officer (SAF/CNZ). Appointed by the Under Secretary of the Air Force. Monitors and maintains an effective Air Force-wide cybersecurity program aligned with the Department of Defense Instruction 8500.01, *Cybersecurity*.

2.2.1. Oversees cybersecurity coordination for non-Air Force programs deploying information systems, known as a guest system, to an Air Force enclave.

2.2.2. Facilitates the management and implementation for identity and access management processes and procedures in accordance with the DoD *Identity and Access Management Strategy* and Identity and Access Management website: **https://public.cyber.mil/idam/**.

2.2.3. Oversees Air Force Damage Assessment Management Office analysis and assessment of compromised Air Force data lost through cyber incidents involving Defense Industrial Base unclassified systems (reference Department of Defense Instruction 5205.13, *Defense Industrial Base (DIB) Cyber Security (CS) Activities*).

2.3. Risk Executive Function. The Risk Executive is a functional role that provides a comprehensive, Air Force-wide approach to risk management. The Risk Executive Function is led by the CISO on behalf of the CIO. The Risk Executive serves as the common risk management resource for senior leaders, executives, managers, mission and business owners, Deputy CIO, CISO, Enterprise AO, functional AOs, senior agency officials for privacy, system owners, common control providers, enterprise architects, security architects, privacy officer, and any other stakeholders having a vested interest in the mission and business success of the organization (adapted from NIST SP 800-39, *Managing Information Security Risk*, para 2.3.2.).

2.4. Authorizing Official. Official responsible for accepting IT risk balanced with the mission requirements. Issues authorization decisions for IT with "moderate" or "low" risk posture. IT with unmitigated "Very High" and "High" risk will be reviewed by the Deputy CIO.

2.5. The 16th Air Force. Issues network orders for cybersecurity, compliance, maintenance, and time sensitive changes to maintain the AFIN.

2.6. MAJCOM Cybersecurity Office. This office supports the CISO's cybersecurity program for the MAJCOM's bases.

2.6.1. Ensures the cybersecurity workforce is qualified and requirements are tracked.

2.6.2. Ensure AF Public Key Infrastructure Local Registration Authorities are established and maintained at the MAJCOM bases

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

2.7. Communications Squadron Commander. The Communications Squadron Commander will monitor and maintain the Wing's cybersecurity program. The Wing Commander (or equivalent) will be briefed monthly, at minimum, on the status of the cybersecurity program **(T-3)**. The brief should address the graded areas from the Defense Information Systems Agency's (DISA) Command Cyber Readiness Inspection (CCRI) providing the cybersecurity status for all IT (high risk issues, fix actions and milestones, mission impact, and estimated completion dates). Local standard operating procedures will define the details of the brief. Reference DISA's CCRI site, **https://disa.deps.mil/ext/cop/FS-CCRI/inspections/SitePages/Command_Cyber_Readiness_Inspection_(CCRI)_Program.aspx**.

2.8. Unit Commander. Implements the cybersecurity program for all IT under their purview. The commander should consult the Wing Cybersecurity Office for assistance with their cybersecurity program efforts.

2.9. Information System Owner (ISO) or Program Manager of AF IT. Responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. This includes traditional acquisition category programs and non-traditional acquisition category programs. The ISO or Program Manager shall:

2.9.1. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management **(T-1)**.

2.9.2. Appoint an Information System Security Manager **(T-1)**.

2.9.3. Ensure authorized users and support personnel receive appropriate cybersecurity training for the IT **(T-1)**.

2.10. Information System Security Manager (ISSM). Responsible for the IT's cybersecurity program within a program, organization, information system, or enclave.

2.10.1. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures **(T-1)**.

2.10.2. Maintain awareness of program's cybersecurity risk posture based on current threats. The program should maintain a level of resilience defined by the mission owner **(T-2)**.

2.10.3. Ensure implementation of IT security measures and procedures, including reporting incidents to the Authoring Official and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures **(T-2)**.

2.10.4. Ensure the secure configuration and approval of IT below the system level (e.g., products and IT services) prior to acceptance into or connection to an AF IT or Platform IT system **(T-2)**.

2.11. Wing Cybersecurity Office. 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, including IT of tenant units (e.g., Field Operating Agencies, Direct Reporting Unit, 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 Wing Cybersecurity Office shall:

2.11.1. Manage Communications Security (COMSEC), Computer Security (COMPUSEC), and TEMPEST programs (reference, AFMAN 17-1301, *Computer Security (COMPUSEC)*, AFMAN 17-1302-O, *Communications Security (COMSEC) Operations* **(T-3)**.

2.11.2. Ensure cybersecurity inspections, tests, and reviews are coordinated with leadership and Inspector General's office, as necessary **(T-3)**.

2.11.3. Report security violations and cybersecurity incidents to AOs according to their reporting procedures and criteria **(T-3)**.

2.12. Authorized User. Every authorized user accessing IT that stores or processes Air Force information will operate the device within the guidelines provided in the annual cyber awareness training and any supplemental training provided **(T-1)**. Unusual behavior will be reported in accordance with local Communications Focal Point's standard operating procedures (or appropriate help desk) **(T-3)**.

2.13. Air Force Risk Management Council. This council is organized and operated by the Headquarters Air Force (HAF) and provides a forum for the senior cybersecurity professionals to validate issues concerning cybersecurity risk from a mission and business perspective. The council reviews topics like proposed Risk Management Framework control overlays, authorization decision guidance, and baseline controls. They adjudicate assignment of Air Force Information Technology to the appropriate AO for those systems which fall outside the defined authorization boundaries.

2.14. Air Force Cybersecurity Technical Advisory Group. This group is organized and operated by the HAF and provides technical cybersecurity subject matter experts from across the Major Commands and functional communities to facilitate the management, oversight, and execution of the Air Force Cybersecurity Program. The technical advisory group examines cybersecurity related issues common across Air Force organizations.

2.15. Authorizing Official Summit. The summit is organized and operated by the HAF and provides the Deputy Chief Information Officer, Chief Information Security Officer, and AOs an opportunity to discuss issues relevant to authorization boundaries, mission capabilities, threats, and the affects. The summit presents information and develops courses of action for AOs to maintain relevance about their boundary while maximizing mission capabilities.

Chapter 3

CYBERSECURITY FRAMEWORK

3.1. Overview. The Cybersecurity Framework is organized according to the *NIST Cybersecurity Framework*, which provides a standard for understanding, managing, and expressing cybersecurity risk. The Framework is a structure for aligning policy, business, and technological approaches to managing that risk (reference *NIST Cybersecurity Framework*, **https://www.nist.gov/cyberframework**). The link to The NIST Cybersecurity Framework is **https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework**. The five core functions of the Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover) are not intended to form a serial path or define a static end state. Rather, these functions should be performed concurrently and as part of a system's cybersecurity program that continuously monitors the cybersecurity risk. If any of the five core functions require additional clarification, local leadership (defined as Squadron Commander, Division Chief, or higher), with oversight of the IT, will decide the way forward. Process or procedure may be delegated by leadership but leadership still has ultimate responsibility. Any changes to the risk posture of the IT will be assessed and approved by the AO. The Enterprise AO will assess and approve any changes to the risk posture for network connected IT.

3.2. Identify. Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. This function will:

3.2.1. Implement the Risk Management Framework to receive the IT's Authorization to Operate or approval of the IT's Assess Only from the AO. Implement the Fast Track or Continuous Authorization to Operate, if applicable. Reference NIST SP 800-37 Rev.2, *Risk Management Framework for Information Systems and Organizations*, DoDI 8510.01, *Risk Management Framework (RMF) for Department of Defense Information Technology* AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT)*, and Air Force RMF Knowledge Service, **https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce** (T-1**)**.

3.2.2. Maintain and validate an accurate hardware and software listing monthly to ensure items are accounted for, replaced, and disposed of properly. The hardware and software listing is the IT's baseline (reference AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)* and Notice to Airmen 2018-242-005) **(T-3)**.

3.2.3. Perform a cybersecurity Functional Mission Analysis to identify how IT are interconnected and what the mission impacts are in the event of degradation or outages. The analysis will include understanding how the IT interacts, affects, and is affected by other IT and countermeasures passively and actively operating with the IT. Reference NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*. Validate the Functional Mission Analysis annually and when a major change occurs **(T-3)**. Reference the Functional Mission Analysis – Cyber course from Air University and the All Partners Access Network link: **https://community.apan.org/wg/air_university/af-cyber-college/fma-c/**

3.2.4. Identify the IT hardware and software vulnerabilities on a continual basis and scan monthly, at minimum. All vulnerabilities will be mitigated. Vulnerabilities not remediated must document the level of vulnerability mitigation, if any, and receive approval by the AO **(T-1)**. Vulnerabilities not remediated will be documented and reviewed by leadership characterizing the risk to the mission, risk to the network, identify who is responsible to mitigate the vulnerability, and estimate the time to complete the mitigation effort. Leadership will be updated regularly on the status of all known vulnerabilities. Reference **paragraph 3.3.4** below and *Methods and Procedures Technical Order* 00-33A-1109, *AF Information Network (AFIN) Vulnerability Management*, AFI 17-201, *Command and Control for Cyberspace Operations,* and Joint Federated Assurance Center, **https://jfac.navy.mil**.

3.2.5. Work through the MAJCOM Trusted Systems and Networks focal point to identify supply chain risks and develop strategies to mitigate risks. Perform a regular review for supply chain risks (reference Trusted Systems and Networks in DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, AFI 63-101_20-101, *Integrated Lifecycle Management*, and AF Pamphlet (AFPAM) 63-113, *Program Protection Planning for Life Cycle Management*) **(T-2)**.

3.2.6. Identify and maintain the program's lifecycle management plan that may include system security engineering, acquisition life cycle, and middle-tier acquisition (reference AFI 63-101_20-101, *Integrated Lifecycle Management*) **(T-2)**.

3.3. Protect. Develop and implement appropriate safeguards to ensure delivery of critical services. The protect function supports the ability to limit or contain the impact of a potential cyber incident. This function will:

3.3.1. Implement identity, credential, and access management for physical and remote access for all users including privileged users **(T-1)**. Limit IT access to least privilege that permits the user to accomplish the assigned work role (reference Office of Management and Budget M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, DoDI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, DoDI 8520.03, *Identity Authentication for Information Systems*, and AFI 36-3026V1_IP, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*).

3.3.2. Maintain annual cyber awareness training **(T-1)**. Provide any additional training for authorized users and privileged users **(T-2)**. Unusual IT behavior will be reported in accordance with the Communications Focal Point's standard operating procedures (or appropriate help desk). All users will receive device-specific training and awareness to include role-based training (reference Department of Defense Directive 8140.01, *Cyberspace Workforce Management,* and AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*) **(T-2)**.

3.3.3. Require submission of a Privacy Impact Assessment for the program and may require submission of a System of Record Notification. Protect Air Force Information with encryption while at rest and during transportation based on the information's requirement for confidentially, integrity, and availability. Reference NIST SP 800-53 Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*, DoDI 5400.11, *DoD Privacy and Civil Liberties Programs*, AFI 33-332, *Air Force Privacy and Civil Liberties Program,* and AFMAN 17-1301, *Computer Security (COMPUSEC)* **(T-1)**.

3.3.4. Establish and utilize an effective Configuration Management process, and maintain the IT's secure configuration baseline. This includes implementing all United States Cyber Command, DISA, and AFCYBER configurations for the IT. This includes but is not limited to applicable Standard Desktop Configuration, Security Technical Implementation Guide (STIG), security requirement guides, orders, and special instructions. Reference Technical Order 00-33A-1109 for the full list of orders and instructions. Deviations from United States Cyber Command or DISA requirements must be documented and approved by the AO or Headquarters Air Force Deputy Chief Information Officer **(T-1)**. For information about STIG and security requirements guides see the DISA website **https://public.cyber.mil/stigs/**. For information about network configuration see Technical Order 00-33A-1106, *Air Force Information Network (AFIN) Network Management.*

3.3.5. Use the standardized cross domain solution. If the Information System, IT, or program uses a cross domain solution, or requires a new cross domain solution, the AF Cross Domain Support Element guidance will be used to deploy and support a cross domain solution which complies with National Cross Domain Solution Management Office requirements **(T-1)**. The AF Cross Domain Support Element can be contacted by email at **afnic.csni@us.af.mil**, commercial phone 618-229-6498, or DSN 312-779-6498. Also reference DoDI 8540.01, *Cross Domain (CD) Policy*.

3.3.6. Implement information protection and physical protection measures. The protections will be assessed and reviewed yearly, at minimum **(T-2)**. Leadership will be briefed after each assessment (reference DoDM 5200.08-R, *Physical Security Program*, DoDM 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, DoDM 5200.01 Volume 2, *DoD Information Security Program: Marking of Information*, DoDM 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*, DoDM 5200.01 Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*and AFI 16-1404, *Air Force Information Security Program*).

3.3.7. Develop secure software applications that test software code using a test environment and pre-production environment prior to introducing the software to the production environment on an operational network. No application will be installed to the production environment without a vulnerability assessment **(T-1)**. The software will be tested before each version release and annually, for programming vulnerabilities and functional exploits to maintain a secure software baseline **(T-1)**. In the instance where a DevSecOps pipeline is utilized (with approved Continuous Authorization to operate), software testing will be continuous during development. Critical vulnerabilities will be remediated. Vulnerabilities not remediated must be mitigated and approved by the AO or Headquarters Air Force Deputy Chief Information Officer before introducing the software to the production environment **(T-1)**. Reference the Secure Development Operations Playbook and Kessel Run Playbook for additional information on developing secure software applications. The Chief Software Office (in SAF/AQ) and Chief Innovation Office (in SAF/CN) work together and with the PEOs and DevSecOps communities to continuously innovate and transform the way the Air Force does software development, including better integrating security, best practices, best in class tools, and knowledge sharing across the community (reference **https://software.af.mil**).

3.3.8. Protect the IT from insider threat (reference DoDD 5205.16, *The DoD Insider Threat Program*, AFI 16-1402, *Insider Threat Program Management*, and TASKORD 14-0184).

3.3.9. Secure government-owned Portable Electronic Device (PED) and National Information Assurance Partnership approved personal devices under the SAF/CN approved Bring Your Own Device program, using the CYBERCOM, DISA, and/or AFCYBER standard operating procedures (Reference AFMAN 17-1301_AFGM 19-01, *Computer Security*) **(T-1)**.

3.3.10. Document and standardize devices as much as possible to conform to the enterprise-wide standard, if one exists; this will reduce cost and achieve a more effective cybersecurity program (reference AFI 17-140, *Architecting*).

3.3.11. Comply with Financial Improvement and Audit Remediation requirements, if the IT processes financial data (reference DoD Instruction 7000.14, *DoD Financial Management Policy and Procedures*).

3.3.12. Register all IT programs in Information Technology Investment Portfolio Suite (ITIPS) (reference AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*). Register all IT devices in Enterprise Mission Assurance Support Service (eMASS) **(T-1)**. The National Security System IT will be reported in the annual Headquarters Air Force Federal Information Security Management Act report (reference Public Law 107-347, *E-Government Act of 2002*, and Committee on National Security Systems Policy (CNSSP) 11, *Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*).

3.3.13. Maintain Clinger-Cohen Act compliance for formal acquisition programs (reference AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*) **(T-1)**.

3.3.14. Comply with the *Federal IT Acquisition Reform Act (FITARA)* requirements. The SAF/CN team tracks and reports FITARA metrics. Program Managers must maintain updated points of contact information in ITIPS and eMASS to ensure accurate reporting **(T-1)**.

3.3.15. Dispose of IT information by using remanence security procedures. Use local disposal procedures in accordance with defense reutilization marketing office procedures to reuse, recycle, and dispose of IT (reference NIST SP 800-88 Rev.1, *Guidelines for Media Sanitization*, AFMAN 17-1301 and **https://cs2.eis.af.mil/sites/10060**).

3.4. Detect. Develop and implement appropriate activities to identify the occurrences of a cyber incident. This function will:

3.4.1. Implement tools that monitor and detect anomalies and events. Document procedures to react to an IT anomaly or event. When an anomaly or event occurs, assess the risk and impact to the mission and notify the key stakeholders (e.g., leadership, AO, ISO, Program manager, ISSM, base enclave manager, Trusted Systems and Networks focal point, and authorized users). Coordinate with the mission owners to determine what events will trigger a response action and what action to take, if any (report incident to Air Force Office of Special Investigations and any applicable operational reporting procedures). Reference **paragraph 3.5.1** below. IT connected to the AFIN will reference the AFCYBER Incident Response plan to determine what events trigger a response action, if any.

3.4.2. Implement a continuous monitoring capability to observe changes to the IT's cybersecurity risk since a cyber incident may change the risk posture for the IT. Implement regular scanning, patching, penetration testing, and near-real time monitoring tools like anti-virus and host-based security service, to provide an active defense-in-depth posture for the IT (reference NIST SP 800-137, DoDI 8500.01 and AFI 17-101).

3.4.3. Require a Cybersecurity Service Provider (CSSP) for IT that connects to the AFIN (AFCYBER is the CSSP for all IT that connects to the AFIN). Enter into an agreement with the AFIN CSSP or appoint a CSSP for IT not connected through AFCYBER. Enter into an agreement with an approved CSSP for IT that processes Air Force information that does not connect to the AFIN (reference DoD Instruction 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* and DoD O-8530.1-M, *Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program*) **(T-1)**.

3.4.4. Inspect and log network traffic for unauthorized and malicious actions. Mitigate network traffic risk with tools that perform packet inspection and produce event logs. Applications that produce event logs will provide some mitigation of network traffic risks if the logs are properly reviewed by the system administrator. Regularly request a list of vulnerabilities from the service provider, if the services are provided **(T-3)**.

3.4.5. Detect anomalous behavior. Require all users to report anomalous behavior according to the local Communications Focal Point procedures (or appropriate help desk). Report anomalous behavior to the DoD Cyber Crime Center using the Mandatory Incident Report for IT operating in the defense industrial base (reference DoD Instruction 5205.13) **(T-1)**.

3.5. Respond. Develop and implement appropriate activities to take actions regarding a detected cybersecurity incident. This function will:

3.5.1. Document procedures that describe how to react during and after a cyber incident. The procedures will include notification for leadership, law enforcement, Office of Special Investigations, Wing Cybersecurity Office, and any other applicable operational reporting procedures. The procedures will detail what actions to take (e.g., quarantine, disconnect, no action, etc.). See Committee on National Security Standards Instruction (CNSSI) 1010, *Cyber Incident Response*, Chairman of the Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program*, NIST SP 800-61 Rev.2, *US-CERT Federal Incident Notification Guidelines, Computer Security Incident Handling Guide* **https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf**, AFMAN 10-206, *Operational Reporting (OPREP)*, and AFI 17-203, *Cyber Incident Handling* **(T-2)**.

3.5.2. Respond immediately upon notification of a cyber incident using procedures from **Paragraph 3.5.1**.

3.5.3. Perform a review after a cyber incident to capture any lessons learned. Implement improvements, based on the lessons learned, that are determined relevant to improve the cybersecurity posture of the IT. Notify and brief leadership on lessons learned and improvements. Document and incorporate the lessons learned and improvements into the IT's lifecycle and Configuration Management.

3.5.4. Perform cyber intrusion damage assessment of compromised Air Force data lost through cyber incidents involving Defense Industrial Base unclassified systems. Notify Air Force leadership and stakeholders of damage assessment results in accordance with DoD guidance and SAF/CNZ processes (questions about SAF/CNZ processes can be sent to **usaf.pentagon.saf-cio-a6.mbx.saf-cio-a6-af-damo-mbx@mail.smil.mil**; reference DoDI 5202.13, Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting*, **https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf**) **(T-1)**.

3.6. Recover. Develop and implement approporiate actions to maintain plans for resilience and to restore any capabilities or services that were impacted due to a cyber incident. This function will:

3.6.1. Document and test annually a recovery plan that implements processes and procedures to restore the IT to its pre-affected capabilities; the recovery plan may be incorporated into a continuous monitoring plan, contingency of operations plan, or similar (reference NIST SP 800-53, NIST SP 800-34 rev 1, *Contingency Planning Guide for Federal Information Systems* and DoDI 8500.01) **(T-2)**.

3.6.2. Integrate IT changes into the documentation and lifecycle management of the IT to maximize cybersecurity and recovery efforts.

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

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 107-347, *E-Government Act of 2002*

40. U.S.C. § 1401, *United States Code, 1994 Edition, Supplement 4, Title 40 – Public Buildings, Property, and Works*

40 U.S.C. § 11101, *United States Code, 2012 Edition, Supplement 5, Title 40 – Public Buildings, Property, and Works, Subtitle III, Information Technology Management*

44 U.S.C. § 3502, *United States Code, 2012 Edition, Supplement 5, Title 44 – Public Printing and Documents, Chapter 35 – Coordination of Federal Information Policy Subchapter 1 – Federal Information Policy*

Office of Management and Budget M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, 21 May 2019

NIST SP 800-30, *Risk Management guide for Information Technology Systems*, July 2002

NIST SP 800-34 Rev.1, *Contingency Planning Guide for Federal Information Systems*, May 2010

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

NIST SP 800-37 Rev.2, *Risk Management Framework for Information Systems and Organizations*, December 2018

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, 1 August 2002

NIST SP 800-53 Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

NIST SP 800-61 Rev.1, *Computer Security Incident Handling Guide*, March 2008

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

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

Committee on National Security Standards Policy 11, *Acquisition of Information, Assurance (IA) and IA-Enabled Information Technology (IT) Products*, 1 June 2003

Committee on National Security Standards Instruction (CNSSI) 1010, *Cyber Incident Response*, 16 December 2016

Chairman of the Joint Chiefs of Staff Manual 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

Joint Publication 3-0, *Joint Operations*, 17 January 2017

Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines*, 1 April 2017

DoD *Identity and Access Management Strategy*

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

DoDM 5200.08-R, *Physical Security Program*, 9 April 2007

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

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

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

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

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, 5 November 2012

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting*,

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

DoDD 5205.16, *The DoD Insider Threat Program*, 30 September 2014

DoDI 5230.09, *Clearance of DoD Information for Public Release*, 25 January 2019

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

DoDI 7000.14, *DoD Financial Management Policy and Procedures*, 3 March 2006

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

DoDD 8140.01, *Cyberspace Workforce Management*, 11 August 2015

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoDI 8510.01, *Risk Management Framework (RMF) for Department of Defense Information Technology (IT)*, 12 March 2014

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

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

DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*, 7 March 2016

DoD O-8530.1-M, *Department of Defense Computer Network Defense (CND) Service Provider Certification And Accreditation Program*, 17 December 2003

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

DISA Command Cyber Readiness Inspection website

Air Force Notice to Airmen 2018-242-005

AFMAN 10-206, *Operational Reporting (OPREP)*, 18 June 2018

AFPD 16-14, *Security Enterprise Governance*, 24 July 2014

AFMD 1-26, *Chief, Information Dominance and Chief Information Officer*, 5 February 2015

AFI 16-1402, *Insider Threat Program Management*, 05 August 2014

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

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

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

AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*, 23 May 2018

AFI 17-140, *Architecting*, 29 June 2018

AFI 17-201, *Command and Control For Cyberspace Operations*, 5 March 2014

AFI 17-203, *Cyber Incident Handling*, 16 March 2017

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

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

AFMAN 17-1302-O, *Communications Security (COMSEC) Operations*, 3 February 2017

AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, 20 March 2015

AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 20 June 2018

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

AFI 33-360, *Publications and Forms Management*, 01 December 2015

AFI 36-3026V1_IP, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 4 August 2017

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

AFI 36-703, *Civilian Conduct and Responsibility*, 30 August 2018

AFI 36-3026V1_IP, *Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 4 August 2017

AFI 63-101_20-101, *Integrated Life Cycle Management*, 9 May 2017

MPTO 00-33A-1109, *Air Force Information Network (AFIN) Vulnerability Management*

AFPAM 63-113, *Program Protection Planning for Life Cycle Management*, 17 October 2013

MPTO 00-33A-1106, *Air Force Information Network (AFIN) Network Management*

MPTO 00-33A-1109, *AF Information Network (AFIN) Vulnerability Management*

Defense FAR Supplement (DFARS), 28 June 2019

CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015

NSPD 54, *National Security Presidential Directive 54*, January 2008

IETF RFC 4949 V2, *Internet Security Glossary, Version 2,* August 2007

ICS 700-1, *Intelligence Community Standard 700-1, Glossary of Security Terms, Definitions, and Acronyms*, 4 Apr 2008

HSPD 23, *Homeland Security Presidential Directive 23, Cyber Security and Monitoring*, Jan. 2008

U.S. Air Force Doctrine, *Air Force Glossary* – **https://www.doctrine.af.mil/**

FIPS 200, *Federal Information Processing Standard, Minimum Security Requirements for Federal Information and Information Systems*, March 2006

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFIN—Air Force Information Network

AFCYBER—Air Force Cyber

AFMAN—Air Force Manual

AFPAM—Air Force Pamphlet

AFPD—Air Force Policy Directive

ATO—Authorization to Operate

AO—Authorizing Official

CCRI—Commander's Cyber Readiness Inspection

CISO—Chief Information Security Officer

CJCS—Chairman of the Joint Chief of Staff

COMSEC—Communications Security

COMPUSEC—Computer Security

CNSSI—Committee on National Security Standards Instruction

CSSP—Cybersecurity Service Provider

DCIO—Deputy Chief Information Officer

DISA—Defense Information Security Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

eMASS—Enterprise Mission Assurance Support Service

FITARA—Federal IT Acquisition Reform Act

HAF—Headquarters Air Force

ISO—Information System Owner

ISSM—Information System Security Manager

IT—Information Technology

ITIPS—Information Technology Investment Portfolio Suite

MAJCOM—Major Command

MPTO—Methods and Procedures Technical Order

NIAP—National Information Assurance Partnership

NIST SP—National Institute of Standards and Technology Special Publication

PED—Portable Electronic Device

RMF—Risk Management Framework

STIG—Security Technical Implementation Guide

Terms

Air Force information—Any information not cleared for public release in accordance with DoDI 5230.09, *Clearance of DoD Information for Public Release*, and is collected, developed, received, transmitted, used, or stored by AF, or by a non-AF entity in support of an official AF activity. Source: DoDI 8500.01 (adapted).

Application—A software program hosted by an information system.

Source—NIST SP 800-37 Rev.2 and CNSSI 4009, (**http://www.cnss.gov/CNSS/issuances/Instructions.cfm**).

Countermeasures—Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Source—NIST 800 SP 800-37 Rev.2, FIPS PUB 200, and CNSSI 4009.

Cyber Incident—Actions taken using an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.

Source—CNSSI 4009.

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

Source—NSPD-54, HSPD-23, CNSSI 4009, and DoDI 8500.01.

Data—Information in a specific representation, usually as a sequence of symbols that have meaning.

Source—IETF RFC 4949 Ver 2 and CNSSI 4009.

Event—Any observable occurrence in a network or system.

Source—NIST SP 800-61 Rev.2 and CNSSI 4009.

Privileged User—A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Source—CNSSI 4009.

Incident—An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source—FIPS PUB 200 (adapted) and CNSSI 4009.

Information—1. Facts and ideas, which can be represented (encoded) as various forms of data.

2. Knowledge -- e.g., data, instructions, etc. -- in any medium or form that can be communicated between system entities.
Source: IETF RFC 4949 Ver 2 and CNSSI 4009.

Information System (IS)—A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Source—44 U.S.C. Sec 3502, CNSSI 4009, and DoDI 8500.01.

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

Source—NIST SP 800-37 Rev.2, NIST SP 800-53, and DoDI 8500.01.

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

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Source—40 U.S.C. Sec. 11101 (adapted), 40 U.S.C. Sec. 1401 (adapted), CNSSI 4009, and DoDI 8500.01.

Least Privilege—The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Source—CNSSI 4009.

Mission Owner—The unit assigned, responsible, and accountable for a duty or task. The unit understands the task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task.

Source—Joint Publication 3-0, *Joint Operations* (adapted) and U.S. Air Force Doctrine, Air Force Glossary (adapted).

Mitigate—make less severe, serious, or painful; lessen the gravity of. For example, mitigating a vulnerability by blocking the Simple Network Management Protocol on the network so the vulnerability cannot be exploited.

Non-Traditional Acquisition Category Program—Purchases made through non-acquisition means typically without an established program office, program manager, budget, lifecycle management plan, and long-term sustainment. This includes but is not limited to IT purchases made using government purchases card, Contracting Squadron purchases, unfunded purchases, and end-of-year purchases.

Portable Electronic Device (PED)—Electronic devices having the capability to perform at least one of the following: store, record, 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 or recorders, portable digital assistants, audio devices, watches with input capability, and reminder recorders.

Source—ICS 700-1 and CNSSI 4009.

Remediate—Provide a remedy for or to make right. For example, remediating a vulnerability is performed by installing a patch, updating software, or replacing hardware, which eliminates the presence of the vulnerability.

Risk—A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

Note:- Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.
Source: FIPS PUB 200 (adapted), NIST SP 800-37, and CNSSI 4009.

Software—Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source:—IETF RFC 4949 Ver 2 and CNSSI 4009.

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

Source—NIST SP 800-30 Rev 1 and CNSSI 4009.

Traditional Acquisition Category Program—Purchases that follow the acquisition integrated life cycle management instruction, AFI 63-101_20-101.

Vulnerability—Weakness in an information system, system security procedures, internal controls, or implementation that is susceptible to exploitation by a threat source.

Source—NIST SP 800-30 Rev 1 and CNSSI 4009.