DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

DAFGM2026-32-01

7 August 2026

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FLDCOMs/FOAs/DRUs

FROM: HQ USAF/A4
1030 Air Force Pentagon
Washington DC 20330-1030

SUBJECT: Department of the Air Force Guidance Memorandum, *Civil Engineer Control Systems Cybersecurity*

ACCESSIBILITY: Publication 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.

Office of Primary Responsibility (OPR): AF/A4CP, Technical & Data Integration Branch

By order of the Secretary of the Air Force, this Department of the Air Force Guidance Memorandum (DAFGM) re-issues the June 2024 DAFGM that establishes cybersecurity policy for Civil Engineer (CE)-owned control systems and these systems' associated components, devices, networks, applications and/or data (hereinafter referred to as "control systems"). This Memorandum details the unique operational characteristics of control systems, implements policy for securing and mitigating cybersecurity risk to control systems, and outlines roles and responsibilities for managing risk under the Risk Management Framework (RMF) pertaining to control systems. 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 Department of the Air Force (DAF).

This guidance memorandum applies to all DAF civilians and uniformed members of the United States Space Force, Regular Air Force, the Air Force Reserve, the Air National Guard, and those with a contractual obligation to abide by the terms of DAF issuances.

Compliance with this memorandum is mandatory. To the extent its direction is inconsistent with other DAF publications, the information herein prevails, in accordance with (IAW) Department of the Air Force Instruction (DAFI) 90-160, *Publications and Forms Management*. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. The authorities to waive wing/delta unit level requirements in this publication are identified with a tier ("T-0, T-1, T-2, T-3") number following the

compliance statement. See DAFI 90-160, *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's waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items.

Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed IAW the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. This memorandum becomes void after one year has elapsed from the date of this memorandum or upon the publication of a new Instruction permanently establishing the guidance, whichever is earlier.

KENYON K. BELL, Lieutenant General, USAF
DCS/Logistics, Engineering & Force Protection

Chapters:

Attachments:

Chapter 1
OVERVIEW

1.1. Control Systems Background.

1.1.1. Operational Technology[1] (OT) has become ubiquitous and integrated into every piece of modern life. Throughout the DAF, control systems[2] (a subset of operational technology) are extensively used to monitor, operate, and/or control equipment, infrastructure, and their associated devices (e.g., power generation and distribution, air conditioning, water and wastewater plants, natural gas distribution).

1.1.2. A control system is a collection of technological components that monitor, manage, and/or control the behavior of people, devices, and systems. Control systems can take various forms according to size, complexity, function, or configuration. Some types of control systems may exist such as building automation systems, airfield lighting control systems, fire alarm reporting or industrial control systems. Typically, they consist of components that can be categorized as inputs, controllers, actuators, sensors, and outputs.

1.1.3. Control systems support nearly all aspects of DAF core mission areas; by extension, if the control systems can be compromised, so can the mission(s) they support. Unmitigated vulnerabilities can be exploited (1) potentially leading to mission failure, extended operational impacts, and physical damage to critical infrastructure, and/or (2) providing an attack vector into the broader Air Force Information Network and business systems.

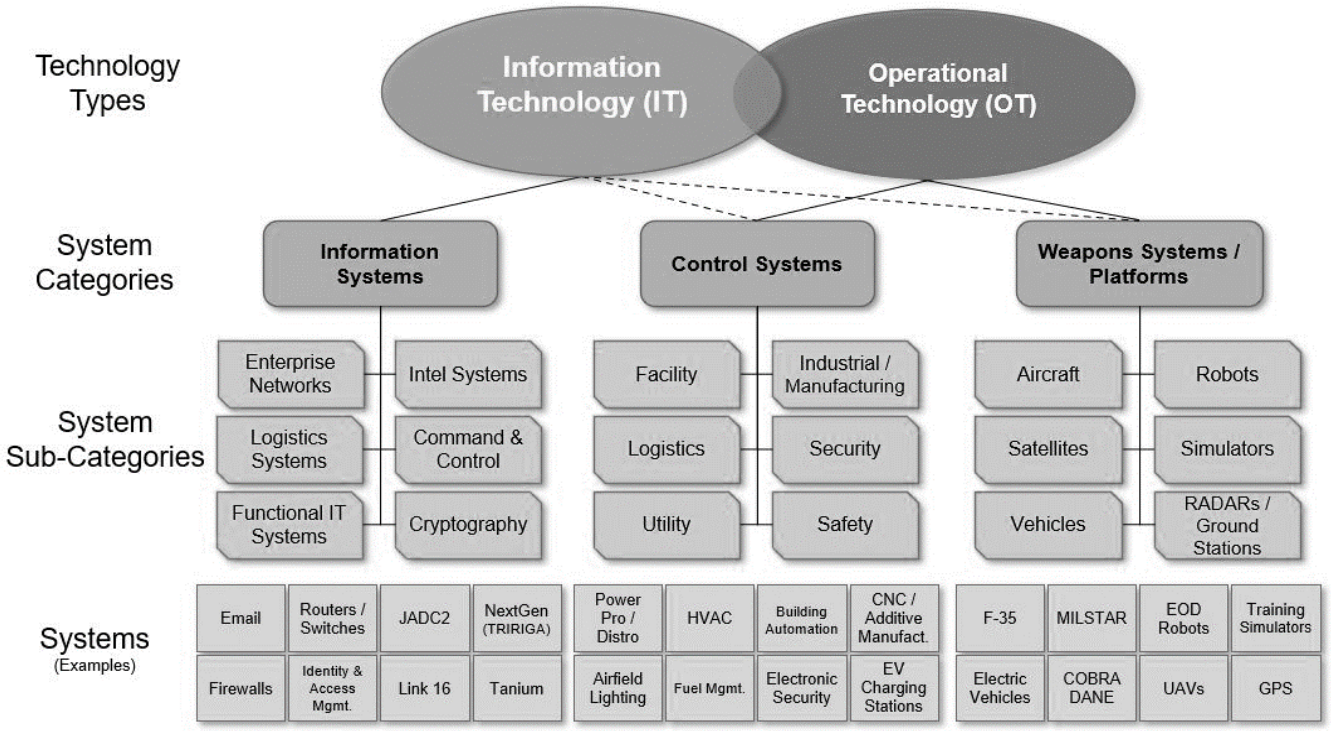

Figure 1 Terminology

[1] "Operational Technology is defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Dec. 2018 (pg. 101).

[2] Control systems are defined as, "a system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable." Control Systems include [supervisory control and data acquisition (SCADA) systems], [distributed control systems (DCS)], [programmable logic controllers (PLC)] and other types of OT measurement and control systems." [NIST SP 800-82r3, September 2023]

1.1.4. The difference between information technology (IT) and operational technology (OT) drives the approach of control system cybersecurity to prioritize and enable the continued availability, operational functionality, and integrity of these systems, slightly above the protection/confidentiality of their transmitted data and information. While security principles are well-defined for IT, these principles are not consistently tailored to or implemented across control systems. Security controls and solutions applied to control systems environments should be: (1) extensive without sacrificing control systems performance and reliability, (2) tailored to the specific control systems environment, (3) verified to ensure control systems continues to operate as intended in a cyber contested environment.

1.1.5. Because of the increased reliance on systems within cyberspace under the civil engineer portfolio, the civil engineer community is a stakeholder (along with mission owners and cyber defenders) in mitigating the rising threats to infrastructure and supporting control systems as part of Civil Engineers' mission to establish, operate, maintain, and protect installations. Cyber risk management has become a critical element of Civil Engineers' efforts to ensure infrastructure is always available to support the DAF mission.

1.2. Scope. This guidance memorandum supplements existing policies, such as Department of Defense Instruction (DoDI) 8500.01 *Cybersecurity*, DoD's RMF (outlined in DoDI 8510.01,) DoDI 8530 *Cybersecurity Activities Support to DoD Information Network Operations*, UFC 4-010-06 *Cybersecurity of Facility Related Control Systems*, and AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*), by providing more explanatory guidance on security measures and responsibility specifically for control systems.

Per the DAF Chief Information Security Officer's (CISO) (SAF/CN) Authorizing Official (AO) appointment letter (as required by AFI 17-101, the CE control system boundary includes DAF CE-owned control systems as well as IT that directly supports the operation, maintenance, and security of the logically-segmented, CE control systems network enclave (e.g., Community of Interest Network (COIN)). The authorization boundary includes, but is not limited to, the following types of systems (and their associated points, devices, components, equipment, control panels, means of connectivity, software, controllers, workstations, servers, etc.). Authorization packages will be created for information systems.

1.2.1. Utility Control Systems (UCS)
- 1.2.1.1. District Steam Control System
- 1.2.1.2. Cathodic protection systems
- 1.2.1.3. Natural gas distribution systems
- 1.2.1.4. Power generation systems, including renewable systems
- 1.2.1.5. Water/wastewater distribution systems
- 1.2.1.6. Water/wastewater treatment systems

1.2.2. Building Control Systems (BCS)
- 1.2.2.1. Energy Management Control Systems
- 1.2.2.2. Heating Ventilation & Air Conditioning
- 1.2.2.3. Advanced Meter Reading Systems
- 1.2.2.4. Building Lighting Control Systems

1.2.3. Fire & Life Safety (FLS) Systems[3]
- 1.2.3.1. Fire Alarm Reporting Systems
- 1.2.3.2. Fire Suppression Systems
- 1.2.3.3. Fire Detection and Alarm Control System

1.2.4. Utility monitoring and control systems (UMCS)
- 1.2.4.1. Electrical distribution systems
- 1.2.4.2. Generator monitoring systems
- 1.2.4.3. Uninterrupted Power Supply system
- 1.2.4.4. Electrical Vehicle Supply Equipment

1.2.5. Airfield control systems
- 1.2.5.1. Airfield Lighting Control Systems[4]
- 1.2.5.2. Aircraft Arresting Systems
- 1.2.5.3. Runway Ice Detection Systems
- 1.2.5.4. Bird Scare System
- 1.2.5.5. Ramp Lighting control systems

1.2.6. Electronic Security System (ESS)
- 1.2.6.1. Physical Access Control Systems (PACS)

1.2.7. Intrusion detection systems[5]
- 1.2.7.1. Closed-Circuit Television (CCTV) Systems
- 1.2.7.2. Digital Video Management Systems
- 1.2.7.3. Electronic Security Systems

1.2.8. CE control systems network enclave (e.g., COIN)

1.2.9. The civil engineer control systems boundary does <u>not</u> include:

1.2.9.1. Systems in the CE IT and CE OT systems boundaries (e.g., NexGen IT, BUILDER, survey equipment, explosive ordnance disposal (EOD) robots, weapons systems, Research, Development, Test & Evaluation (RDT&E) equipment, unmanned aerial systems (UAS)).

1.2.9.2. Control systems such as those contained in other organizations (e.g., force protection, depots, nuclear, medical) as well as control systems embedded in weapons systems.

---

[3] Life safety systems are control systems that must function reliably, safely, and meet applicable codes and standards. Life safety systems protect personnel against undue risk of fire, environmental, and/or other hazards that could potentially result in loss of life.

[4] Airfield lighting systems are control systems that must function reliably, safely, and meet applicable codes and standards. Airfield lighting systems protect personnel against undue risk of fire, environmental, and/or other hazards that could potentially result in loss of life.

[5] Most of these systems fall within security forces ownership; however, this memorandum applies to those that fall within civil engineer ownership

Chapter 2

ROLES AND RESPONSIBILITIES

Risk Management Framework:

2.1. Chief Information Security Officer (CISO), SAF/CNZ. Develops, implements, maintains, and enforces the DAF cybersecurity program and the RMF process, roles, and responsibilities. Is the approval authority for DAF control baselines (e.g., security / privacy, etc.) and overlays (e.g., Facility Related Control Systems, etc.). Serves as the DAF Risk Executive ensuring individual system risks reflects organizational risk tolerance and is considered along with other risks affecting mission/business success IAW AFI 17- 130, *Cybersecurity Program Management*, and NIST SP 800-39, *Managing Information Security Risk*.

2.2. The Director of Civil Engineers (AF/A4C). Responsible for organizing, training, and equipping the engineering force along with providing policy, strategy, oversight, and resource advocacy for Civil Engineer portfolio responsibilities (to include control systems cybersecurity).

2.3. Air Force Installation and Mission Support Center (AFIMSC). AFIMSC/RM (Resource Management Directorate) develops the funding line and distributes funding for execution. Coordinates with SAF/CN to ensure the cybersecurity risk posture, risk tolerance levels, and risk acceptance decisions for DAF systems meet mission and business needs.

2.4. Authorizing Official (AO). Appointed by SAF/CN and responsible for all roles listed in AFI 17-101, including managing the risk of control systems and tailoring controls to balance security and mission needs. **(T-1).**

2.5. Authorizing Official Designated Representative (AODR). Appointed by the AO and responsible for all roles listed in AFI 17-101, including CE control system asset portfolio oversight and management (including cybersecurity requirements) via the Facility Operations Enterprise Manager, reviewing, and validating annual requirements for Operating Agency Codes (OAC) -18 funding and distributes funding based on availability, and performing Program Objective Memorandum (POM) duties including interaction with AF/A4P. **(T-1).**

2.6. Security Controls Assessor (SCA). Appointed by the CISO and responsible for all roles listed in AFI 17-101, including supporting the AO in making assessment determinations and authorization recommendations. **(T-1).**

2.7. Security Controls Assessor Representative (SCAR). Appointed by SCA per AFI 17-101 and responsible for fulfilling duties under the SCA's direction.

2.8. Air Force Civil Engineer Center (AFCEC).

2.8.1. AFCEC will ensure incorporation of cybersecurity requirements and costs into all phases of each Directorate's activities and products (see para 3.3). This shall include, but is not limited to, a review process on the effectiveness of holding design agents accountable for AFCEC-managed requirements. **(T-1).**

2.8.2. AFCEC/COO (Operations Maintenance Division) will provide technical and execution guidance to CE units on control systems cybersecurity activities to supplement this DAFGM, to include, but not limited to, the subject-matter in this DAFGM (e.g., paras 2.9.3, 2.9.5, 2.11.3, 2.11.4, 3.1). **(T-1).**

2.8.3. Pertaining to RMF-related duties, AFCEC/COO is the execution organization directly supporting the AO to enable and facilitate the RMF process and assists CE units in that process for CE control systems. AFCEC/COO shall:

2.8.3.1. Support RMF authorization processes in the Civil Engineer enterprise for control systems aligned with RMF roles (para 2.4-2.7, 2.10-2.13), para 3.2.1, and para 3.5.1 in coordination with the AO. **(T-1).**

2.8.3.2. Perform RMF activities: establish security control baseline IAW with the DoD CIO standards while working toward compliance with the DAF-CISO requirements, validate Authorization to Operate (ATO) packages for SCA review and AO signature, process entries into Enterprise Mission Assurance Support Service (eMASS), and oversee and track CE unit's continuous monitoring program and mitigation of identified vulnerabilities in RMF Plans of Actions and Milestones (POA&Ms). **(T-1).**

2.8.3.3. Maintain "RMF continuous monitoring plan" template and determine "RMF continuous monitoring" checklist (both approved by the AODR) that installations can leverage for each control system's continuous monitoring plan (per para 3.5.1). **(T-1).**

2.8.3.4. Ensure rigorous review and monitoring of documentation and artifacts uploaded into eMASS. All systems with ATOs must ensure documentation is correct and complete. **(T-0).**

2.8.4. AFCEC/COO will assist installations in completing the following:

2.8.4.1. Perform local RMF activities: conduct system testing, review each system's RMF continuous monitoring plan, identify mitigations, and process entries into eMASS. **(T-2).**

2.8.4.2. In coordination with the installation's Comm/Cyber unit, install a control systems network enclave (see para 3.4.2) when requested at the installation level. Control systems are not managed as part of the IT portfolio and are not to be entered into the Information Technology Investments Portfolio Suite (ITIPS) **(T-1).**

2.8.4.3. In coordination with the installation's Civil Engineer unit, Information Security Officer, Comm/Cyber unit, and system vendor, migrate (when appropriate) AO-approved control systems into the installed control systems network enclave in a prioritized manner (see para 3.4.2). **(T- 1).**

2.8.4.4. Provide the COIN Memorandum of Understanding (MOU) template to the BCE to fill out with local Comm units, to assign roles and responsibilities with control system operations (e.g., in the event of disruptions of control systems due to configuration changes, updates, etc.) **(T-3)**.

2.8.5. AFCEC/COO is responsible for providing a standardized template and necessary guidance to installations to collect a CE-enterprise inventory of control systems (see para 3.1.1). **(T-1).**

2.9. Base Civil Engineer (BCE). Establish a control system program that is responsible for maintaining the operations, obtaining resources, and ensuring the cybersecurity posture of control systems at the installation **(T-1).** The Base Civil Engineer will ensure:

2.9.1. An Information System Owner (ISO) is appointed for installation-level control systems per AFI 17-101 since control systems are not centrally managed. **(T-2).**

2.9.1.1. Identify an ISO for control systems prior to the current ISO vacating the position. **(T-3).**

2.9.1.2. Provide AFCEC/COO with the names of the current control system ISO(s) (see para 2.10) and Information System Security Manager(s) (ISSM) (see para 2.11). **(T-3).**

2.9.2. The base commander will be briefed annually on POA&Ms to ensure a comprehensive understanding of the risks associated with CE control systems. Additionally, the base commander will be briefed bi-annually on all overdue POA&Ms. Documentations of both the annual and bi-annual briefings, including key discussion points and action items, will be captured in MFRs and uploaded into eMASS to maintain an auditable record of compliance and leadership awareness. **(T-1).**

2.9.3. Mitigation/remediation actions of identified cyber vulnerabilities for CE-owned control systems (e.g., through regular patching of systems and/or maintenance, sustainment, modernization, or replacement activities and projects) will be delivered in a timely manner. (reference 3.2.2, 3.3, 3.6-3.12, and 4.1-4.7). **(T-1).**

2.9.4. Coordination to provide physical and IT administrative access to the necessary facilities and systems required to support approved control systems cybersecurity activities (e.g., assessments, mitigation, data collection, inventory, etc.). **(T-3).**

2.9.5. Inventory of installation-level control systems is current, accurate, and collected no less than annually (see para 3.1). **(T-2).**

2.9.6. Incident Response and System Recovery/Contingency Plans are in place as outlined in para 4.7. **(T-3).**

2.9.7. Personnel have a depth of knowledge regarding control system(s) and associated forms of connectivity to avoid a single individual from being single point of failure. **(T-3).**

2.9.8. AO-approved control systems are migrated into the CE network enclave as appropriate. **(T-1).**

2.9.9. Work with local Comm units to determine roles and responsibilities via the COIN MOU between AFCEC, CE Squadron, and Comm Squadron. **(T-3)**.

2.10. Information System Owner (ISO).

2.10.1. Ensure execution of the ISO and Program Manager (PM) responsibilities are satisfied for CE-owned control systems per AFI 17-101[6] paras 3.9 and 3.10. **(T-2).**

2.10.2. Maintain cross-organizational awareness of acquisition, installation, maintenance, and security posture of CE-owned control systems. **(T-3).**

2.10.3. Follow the RMF authorization process identified by the AO (para 3.2) for control systems. **(T-2).**

---

[6] There is not currently nor is there intended to be a centralized program management office (PMO/PEO/PO) for control systems in the DAF; in turn, "those Program Manager duties specified in AFI 17-101 cannot be fulfilled.

2.10.4. Ensure establishment of the security control baseline for each system per AFCEC/COO guidance. **(T-2).**

2.10.5. Ensure policies in this Memorandum are satisfied. **(T-1).**

2.10.6. Ensure CE Project Support Agreement (PSA) requirements for deploying control systems network enclave (refer to para 3.4.2) are satisfied within 60 days of initiation, including physical, connectivity, and configuration requirements. **(T-3).**

2.10.7. Facilitate RMF, CE network enclave deployment, and system migration activities at the installation-level for control systems as outlined para 2.8.4.3. **(T-2).**

2.10.8. Appoint an ISSM at the installation for control systems to support and assist the ISO IAW DoDI 8510.01 **(T-0)** for the program office and ensure the ISSM is certified IAW DAFMAN 17-1305, *DAF Cyberspace Workforce Management Program*. **(T-1).**

2.10.9. Meet with the ISSM (and ISSO) at regular intervals to discuss RMF status and other related activities, as well as review vulnerabilities and suggested mitigations resulting from any assessments that have been conducted. **(T-1).**

2.11. Information System Security Manager (ISSM).

2.11.1. Appointed per para 2.10.8 and ensure the ISSM responsibilities are satisfied for CE-owned control systems per AFI 17-101. **(T-1).**

2.11.2. Support the ISO in ensuring the policies in this Memorandum are satisfied. **(T-1).**

2.11.3. Perform RMF activities, including verifying and overseeing the accuracy of entries into eMASS, reviewing, approving, or denying submitted RMF documentation; executing the CE unit's continuous monitoring program; and accomplishing and tracking the mitigation of identified vulnerabilities documented in RMF POA&Ms. **(T-1).**

2.11.4. Meet with the ISO (and ISSO) at regular intervals to discuss RMF status and other related activities as well as review vulnerabilities and suggested mitigations resulting from any assessments that have been conducted. **(T-1).**

2.12. Information System Security Officer (ISSO).

2.12.1. Ensure the ISSO responsibilities are satisfied for CE-owned control systems per AFI 17-101. **(T-3).**

2.12.2. Support the ISO and ISSM in ensuring the policies in this Memorandum are satisfied. **(T-3).**

2.13. User Representative (UR) / System Operator.

2.13.1. Will ensure the UR responsibilities are satisfied for CE-owned control systems per AFI 17-101.[7] **(T-3).**

2.13.2. Will support ISO, ISSM, and ISSO at the installation level in ensuring the policies in this Memorandum are satisfied. **(T-3).**

[7] By nature, the UR/System Operator may commonly exist through established positions within the Operations Flight (e.g., shop supervisor, technician, etc.).

External Partners:

2.14. Air National Guard and Air Force Reserve. HQ NGB/A4 and HQ AFRC/A4 will provide support and supplemental guidance as required for CE control systems under NGB and AFRC responsibility. **(T-1).**

2.15. Cyber Resiliency Office for Control Systems (CROCS). The DAF CROCS is an over-arching management body led by the Technical Director for OT systems. CROCS is empowered to direct, oversee and influence prioritization of mitigation resources, cyber defense training, personnel, planning, and programming across functional communities of DAF-wide control system activities through the DAF Corporate process and multiple resourcing panels (e.g., Cyber, Installation Support, and Logistics Panels). CROCS also oversees the execution of the *DAF Strategic Plan for Control Systems*.

2.16. Sixteenth Air force (16 AF). In support of the Defensive Cyberspace Operations mission, develops and implements appropriate activities to monitor and report on the occurrence of cyber-security events, cybersecurity implementation, and risk management. **(T-1).**

2.16.1. Guides cybersecurity and control systems experts to detect, mitigate, and recover from malicious cyber activity and carries out responsibilities described in Section 3.5.2 below. **(T-1).**

2.16.2. Collaborate with AF/A4CP to encourage the capture of CE hardware, software, and related control systems associated with task critical assets (TCA) are reflected in MRT-C mapping and reflected in Mission Assurance Decision Support Systems (MADSS). **(T-1).**

2.17. AF/A3 Mission Assurance (MA). Facilitate the coordination and collaboration with AF Mission Assurance, utilizing the MA Construct to identify, assess, and manage risks that endanger strategic mission execution. In addition, synchronize AF/A4CP, Technical & Data Integration Branch with appropriate level of AF MA forum.

2.18. AF/A2 Intelligence, Surveillance, and Reconnaissance (ISR). Identifies the capability and intent of specific threats to cause loss or damage to Defense Critical Infrastructure (DCI), assesses the likelihood that such threats will be carried out (T-1), and makes intelligence-based indications and warning information related to DCI available (T-1).

2.19. AF/A6 Warfighter communications and cyber systems. Identify security measures to mitigate risks and protect DCI. (T-1)

Chapter 3

CYBERSECURITY IMPLEMENTATION

3.1. Control Systems Inventory. With the support of AFCEC/COO, Civil Engineer units must annually and on an ad hoc basis conduct and continuously maintain accurate inventories of all the installation's CE-owned control systems and associated components and devices. **(T-0)**. All identified hardware and software shall be assigned a unique identifier and accounted for IAW DoD 5000.64.

3.1.1. Civil engineer units must utilize AFCEC/COO provided inventory template and process (located on CE Dash) and all applicable fields must be appropriately completed (see para 2.9.5). **(T-1).** The inventory shall contain each instance of a control system (per the types listed in para 1.2) at the installation down to topology *Level 2 - Field Control System (IP)* [8] in the Purdue Model (as defined in the control system architecture topology diagram and definitions in Unified Facilities Criteria (UFC) 4-010-06, Appendix E). Each instance shall include but is not limited to assigned IP addresses, MAC addresses, serial number, firmware and software versions, physical location, if applicable. **(T-1).**

3.1.2. The ISO, ISSM, and/or ISSO must document any new systems or system modifications and configuration changes (per para 3.9), including but not limited to: install date, version, location, applied patches and updates in the installation's control systems inventory per NIST SP 800-53r5 para 3.5 and this Guidance Memorandum's para 3.1. **(T- 1).**

3.1.3. CE units must maintain a baseline understanding of which control systems are mission critical. From the installation's inventory of CE-owned control systems, CE units shall, in coordination with local MA representative and/or mission owners, identify, perform risk assessment, prioritize, and document those control systems deemed critical for mission(s) execution[9] (e.g., directly, or indirectly enable Task Critical Assets (TCA), weapons systems, Mission Essential Functions (MEF), or locally identified critical missions on base).[10] Update the priority list as mission requirements evolve. For new and existing mission critical facilities that are dependent upon CE control systems, design or renovate systems to operate in manual override mode in compliance with UFC 4-010-06 Section 4.2.2. Degraded Operation. **(T-1).**

3.1.4. If a control system meets one or more of the statutorily defined National Security System (NSS) criteria, defined in 44 USC 3552, it is considered an NSS. This is documented in the Risk Management Framework Information Technology (IT) Categorization and Selection Checklist (ITCSC) and within the eMASS authorization package for each system. Further information can be found in Executive Order (EO) 14028, NATIONAL SECURITY MEMORANDUM 8, and the NATIONAL MANAGER ISSUANCE Identification and inventory of National Security Systems Guidance (NMM 2022 05 05.)

---

[8] References Figure E-1 (pg.45), UFC 4-010-06, Cybersecurity of Facility-Related Control Systems

[9] Further Guidance specific to CE control systems deemed "critical;" to mission is forthcoming

[10] Refer to Defense Critical Infrastructure (DCI) Line of Effort (LOE) Security Classification Guide (SCG) (27 Jul 2018) and Classification Guide for Control Systems (CS) for guidance on security classification of such information

[11] Note that some CE control systems (e.g. automatic door-locks) do not qualify as RPIE

Real Property Installed Equipment Designation (RPIE). CE control systems[11] and their associated components and devices may be considered Real Property Installed Equipment (RPIE). To determine if the control system is considered RPIE, use the components list associated to the category code of the facility found in the Air Force Category Codes SharePoint website located at (https://usaf.dps.mil/teams/10758/cit-catcode/module/home.aspx) For more information on RPIE refer to DAFI 32-9005.

3.1.4.1. The Real Property installed Equipment designation dictates the funding and management channel for a control system. IAW DAFI 32-9005 Real Property Management, RIPE- designated systems are sustained using Facilities, Sustainment, Restoration, and Modernization (FSRM) funds. This financial distinction does not change cyber requirements; all systems will be maintained to the same technical and cybersecurity standard based on mission requirements.

3.1.4.2. If a control system is not found in the Air Force Category Codes website or if unsure of RPIE designation, submit a request to AFCEC.CIT-.A@us.af.mil.

3.2. Mitigating Identified Vulnerabilities

3.2.1. **Risk Management Framework (RMF).**

3.2.1.1. Civil Engineer units must follow RMF and fulfill ATO requirements for authorization of control systems (outlined in para 2.9.3. and DAF RMF policy, AFI 17-101). **(T-0).**

3.2.1.2. Civil Engineer units must use eMASS for initiating, submitting, tracking, and updating all RMF artifacts. **(T-1).**

3.2.1.3. ISSM will ensure newly initiated authorization packages (e.g., ATO, IATT, DATO, ATC, etc.) for control systems shall be aligned with RMF, as outlined in para 2.9.3. (T-0). **(T-0).**

3.2.1.4. Civil Engineer units must adhere to the "*Civil engineer (CE) Facility Related Control System (FRCS) Baseline Security Controls*" memorandum stating CE units shall perform, at a minimum, the tailored security controls for CE FRCS that are based on functional security groups. **(T-2).** Expanding upon the minimum requirements, units will execute additional controls based on emerging adversarial threats and DAF mission requirements. **(T-3).** A4C and AFCEC are working on an implementation plan for compliance with the DAF-CISO AO memorandum of expectations and further guidance will be released outside this publication.

3.2.1.5. ISO will ensure that control systems determined to be NSS (refer to para 3.1.4) must have a default RMF categorization of M-M-M (Moderate-Moderate-Moderate) in the Information Technology Categorization Security Checklist (ITCSC) for Availability, Integrity, and Confidentiality. Any deviations up or down (e.g., L-M-M, M-H- H) from the default categorization require justification and authorization through the RMF Step 1 categorization process by the ISSM. **(T-2).**

3.2.1.6. CE units will comply with all requirements in AFI 17-101 **(T-1).**

3.2.1.7. For RMF continuous monitoring, perform verification of security controls, and RMF authorization packages, IAW para 3.5.1.

3.2.1.8. Refer to Chapter 2 for the RMF responsibilities translated for control systems.

3.2.2. **Identifying Vulnerabilities & Mitigations.**

3.2.2.1. AFCEC/COO through a standardized process will identify vulnerabilities from published sources (e.g., RMF assessments, CVE database, Notices to Airmen (NOTAM), joint mission assurance assessments (JMAA), self-assessments, CISA Stakeholder-Specific Vulnerability Categorization (SSVC), etc. *include all cybersecurity assessments sponsored by government agencies)*) and advise each base on the applicability of the vulnerability based on its hardware and software inventory**.** Civil Engineer units will develop a local plan to correct the vulnerabilities identified. **(T-3).**

3.2.2.1.1. CE Units may register at DHS CISA (Cybersecurity and Infrastructure Security Agency (govdelivery.com)) to receive security alerts, analysis reports, tips, and other updates. Additionally, CE Units may to view control systems Alerts and Advisories from CISA (Cybersecurity Alerts & Advisories | CISA).

3.2.2.2. CE units will ensure all identified vulnerabilities and their associated risks are captured in the control system's authorization package and associated POA&M (refer to para 3.2.1). **(T-2).**

3.2.2.3. CE units prioritize mitigations to critical vulnerabilities affecting mission critical systems (refer to para 3.1.3). **(T-2).**

3.2.2.4. Funding for cybersecurity mitigations is the responsibility of the local bases. Bases must use their local PEC for FRCS hardware / software replacement and cyber training activities to include facility servers, workstations, computers, laptops, tablets. **(T-1).**

3.3. Construction, Repair, or Energy Contract Requirements

3.3.1. The Civil Engineer unit and AFCEC must ensure design agents and vendors create and implement control systems IAW applicable UFC, UFGS guidance (including UFC 4-010-06 and UFGS 25 05 11) and this DAFGM. **(T-3).** The local CE control systems ISO will review and validate requirements from a control system's cybersecurity perspective prior to contract award reference para 3.3.2. **(T-3).**

3.3.1.1. For any new acquisition or replacement of control systems or their associated devices at level 2 or above of the Purdue model, CE units must consult AFCEC/COO for design reviews, proposals, quotes, statements of work, etc. **(T-3).**

3.3.2. All CE unit projects (e.g., Performance Contracts (ESPC), Utility Energy Service Contracts (UESC), microgrids, Environmental Security Technology Certification Programs (ESTCP), MILCON/SRM, etc.) will follow existing standards and policies to incorporate cybersecurity and associated costs into all phases of delivery. These phases include contract language[12], design, development, test and evaluation, integration, execution, construction, operation, maintenance, sustainment, upgrade, or replacement. **(T- 0).** These existing standards and policies include: Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, this Guidance Memorandum, *AF/A4CF Business Rules for MILCON Program Packages and Preparing the DD Form 1391 & 1390* para 9.1.1.3,

NIST SP 800-82r3, NIST SP 800-53r5, UFC 4-010-06, and the best practices from the Department of Homeland Security (DHS)'s Cyber Security Procurement Language for Control Systems (Cyber Security Procurement Language for Control Systems (cisa.gov).

3.3.3. ISO will ensure contract language requires newly acquired and/or substantially upgraded control systems to use open protocols and standards to maximize data interoperability IAW UFC 3-410-02, *Direct Digital Control for HVAC and Other Building Control Systems*, and in alignment with industry best practices. **(T-0).**

3.3.4. ISO will ensure contract language mandates machine-readable data structured formats (e.g., CSV, RDF, XML, JSON) to enable maximum data collection, centralization, and integration. **(T-1).**

3.3.5. ISO will ensure contract language requires any data interconnectivity protocols (e.g. HTTP) to utilize transport layer security (TLS) version 1.3, secure shell (SSH) protocol version 2.0 or greater (e.g., SSH, SFTP), or equivalent standard-based security protocol. **(T-1).**

3.3.6. ISO will ensure contract language accounts for the security of data in transit and at rest through use of industry best practices (e.g., encryption, firewalls, etc.). **(T-3).**

3.3.7. ISO will ensure contract language requires the use of government-owned assets (or government furnished equipment (GFE) (e.g., computer, tablet) for control systems maintenance. Connection of vendor laptops to the equipment and/or connection to the cloud is specifically prohibited for maintenance. **(T-0).**

3.3.8. ISO will ensure contract language requires on-site maintenance (see para 3.10). **(T-2).**

3.3.9. ISO will ensure contract language prohibits the connection of removable media (refer to para 3.12) to a control system or control systems network enclave other than as described in para 3.12.1. **(T-3).**

3.3.10. ISO will ensure contract language requires compliance with vulnerability scanning standards stated in UFGS-25 05 11, *Cybersecurity for Facility-Related Control Systems*, para 3.11. **(T-1).**

3.3.11. ISO will ensure contract language requires the vendor(s) to provide (1) copies of operator, administrator, and maintenance manuals, (2) copies of the system's topology, hardware/ software inventory, and configuration, (3) training and associated materials, as well as (4) any third-party validation/standardization (e.g., Common Criteria, ISO-9000, etc.) testing results. **(T-3).**

3.3.12. ISO will ensure contract language requires the vendor(s) to perform an initial security assessment, scan vulnerabilities, provide a copy of the scan results, and recommend and document mitigations for identified vulnerabilities prior to actions specified in para 3.3.15. **(T-3).**

3.3.13. ISO will ensure contract language requires vendors to remove and dispose of control systems and their components once no longer deemed necessary or decommissioned. **(T-3).**

[12] This includes, but is not limited to, clearly articulating the contractor's cybersecurity responsibilities in contract language requirements, including all required cybersecurity clauses in contracts, and considering cybersecurity specialty clauses.

3.3.14. ISO will adjust contract language to include labeling (i.e., unique nomenclature) of hardware and associated components (e.g., cables, ports, servers, etc.) and implement this requirement into new or renewal contracts. **(T-3).**

3.3.15. ISO must provide a system recovery plan for hardware/software maintenance on a system so in the event of patches and updates are installed that could result in future cybersecurity vulnerabilities. The recovery plan should include appropriate scanning capabilities to meet the RMF scanning requirements and government-mandated system scans risk impacting certification or warranty. **(T-3).**

3.3.16. Before a control system becomes operational (e.g., begins processing data, supporting mission, supporting facility operations), CE units, under the direction of the ISO, must receive an authorization decision document and will:

3.3.16.1. Ensure initial system authorization under RMF process is adequately resourced (e.g., staffing, funding, vendor artifacts, etc.). **(T-3).**

3.3.16.2. Mitigate all identified vulnerabilities that do not require additional funding. For the remaining vulnerabilities, create POA&M's that state the course of action for addressing remaining mitigation efforts that incur a cost. **(T-3).**

3.3.16.3. Prioritize, plan, budget, and execute all required mitigations. **(T-3).**

3.3.16.4. Provide sufficient documentation (refer to AFI 17-101) for the DAF to finalize the authorization of the control system (refer to para 3.2). **(T-3).** When appropriate, plan to utilize the existing CE control systems network enclave (refer to paras 3.4.2 and 3.4.4). **(T-1).**

3.3.17. CE units will add newly installed or acquired control systems to the installation's inventory (para 3.1). **(T-0).**

3.3.18. Additionally, civil engineer units will ensure utilities Privatization contracts include the DFARS 252.204- 7012 clause and follow standards specified in NIST SP 800-171r2, DoDI 4170.11, and additional cybersecurity direction stated in the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) memos: *Supplemental Guidance for the Utilities Privatization Program* (07 Feb 2019) and *Interim Defense Federal Acquisition Regulation Supplement Rule, 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements* (guidance for utilities privatization) (Nov 2020). **(T-0).**

3.3.19. For energy projects, CE units will follow cybersecurity guidance stated in the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (OASD (EI&E)) memo *Installation Energy Plans – Energy Resilience and Cybersecurity Update*, 30 May 2018. **(T-0).**

3.4. Connectivity.

Control systems rely on multiple forms of connectivity for uninterrupted operation. Two types of network connections are Control Systems hosted on a local communications unit VLAN connection on NIPRNet and the AFCEC CE Community of Interest Network (COIN). Design changes to any CE accredited system require approval of the system Configuration Control Board. Security relevant changes are processed IAW Risk Management Framework requirements for reassessment of the change in cybersecurity risk.

3.4.1. **Current State.**

3.4.1.1. In order to connect CE control systems to AFCEC CE COIN after deployment on the local Communications network enclave, the CE control systems must meet the Authorizing Officials (AO)'s Authority to Connect (ATC) requirements. **(T-3).**

3.4.1.2. Do not directly connect CE control systems to the SIPRNet or NIPRNet. **(T-3).**

3.4.2. **Additional Systems.** Additional CE control systems can be migrated to the CE network enclave at the discretion of the Base Civil Engineer and ISO Information systems security engineer per AFI 17-101. This will involve additional funding for the required network infrastructure. **(T-1).**

3.4.3. **Mission Critical Systems.** Mission critical CE systems may constitute a single point of failure for the associated mission. Providing mechanical redundancy to eliminate single points of failure that might adversely impact mission accomplishments**.** Mission critical systems should have the smallest cybersecurity attack surface possible, and consideration should be measured prior to connection to the CE network enclave or as stand-alone systems. In practice, the goal should be to reduce the cyber security risk to that of the physical security risk of the asset. Units should pay particular attention to the Task Critical Assets on their base and ensure that CE systems are not mission critical to the asset.

3.4.4. **Modems.** Modems are not allowed except:

3.4.4.1. They are on dedicated point-to-point circuits within the base, or

3.4.4.2. External modem connections are protected from outside access by relays or similar mechanical barriers.

3.4.5. **Wireless Communications/Radio Frequency (e.g., Wi-Fi, cellular, Bluetooth, satellite).**

3.4.5.1. The use of unlicensed frequencies under Federal Communications Title 47 Part 15 is generally prohibited, except where specific limitations and security requirements are met. Do not procure new control systems using a Part 15 radio frequency device. **(T-0).** OCONUS installations must also comply with applicable Host Nation rules, laws, policies, and agreements. **(T-0**). CE personnel must verify radio frequency spectrum certification compliance with the installation Spectrum Manager for any radio frequency devices currently in use. **(T-2).** Per DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, DoD requires non-licensed devices operating in the United States and their possessions to be registered with the local spectrum management office. **(T-0).** When purchasing new devices, also follow para 3.3. **(T-1).**

3.4.5.1.1. A wired infrastructure is more secure than one that uses wireless technologies; therefore, CE units will convert radio frequency networks to wired or fiber where practical. If (1) an existing control system needs to continue using radio frequency devices to transmit and/or receive data or (2) a control system not installation requires radio frequency (e.g., cellular tower leasing), ensure the system complies with DAFI 17-220, *Spectrum Management*, uses dedicated

frequencies per National Telecommunications Information Administration *Chapter 7 and Chapter 4*, and is approved by the installation's Spectrum Manager before seeking a waiver approval. **(T-1).**

3.4.5.1.2. CE units must check radio frequency devices to ensure data transmission is encrypted "end-to-end" over an assured channel; the device is aligned to the sensitivity of the data; and the device is validated under the "Cryptographic Module Validation Program" specified in FIPS PUB 140-3, *Security Requirements for Cryptographic Module*s, Overall Level 1 or Level 2, as dictated by the data's sensitivity. **(T-1).**

3.4.5.1.3. The use of unencrypted radio communication within the Fire Alarm Reporting System (FARS) will be reflected as a POA&M to the DAF CISO approved by the AO per the *Risk Acceptance for unencrypted wireless radios, Fire Alarm Reporting Systems (FARS) Memo Mar 2025*. Installations with unencrypted radio communication on FARS systems will adhere to the following risk management practices outlined in the Risk Management Framework (RMF): (1) Continuous Monitoring: The installation will regularly assess the effectiveness of existing security controls and implement enhancements as needed. (2) Annual Cyber Awareness Training (Cyber awareness challenge):

Personnel responsible for FARS will receive ongoing training on security best practices and potential vulnerabilities (https://lmsjets.cce.af.mil/moodle/course/view.php?id=14124). (3) Periodic Review: This risk acceptance decision will be re-evaluated periodically, or as new threats and vulnerabilities emerge, ensuring its continued alignment with the organization's risk appetite and evolving threat landscape.

3.4.5.1.4. Airborne wireless activation of Airfield Lighting Control Systems, when included as part of an authorized FAA system certification, is not required to be encrypted, as the purpose of this feature is to allow any aircraft to activate the lights in an emergency while the tower is not manned.

3.4.5.1.5. CE units must ensure that any data transmitted by Wi-Fi devices, services, and technologies follows IEEE Standard 802.11-2016 per DoD Directive (DoDD) 8100.02, DoDI 8420.01, DHS's *Guide to Securing Networks for Wi-Fi* (A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family) (cisa.gov)), and Wi-Fi best security practices where applicable. **(T-0).**

3.4.5.1.6. Authorization will not be granted by the AO for control systems utilizing Bluetooth. **(T-0).**

3.4.5.1.7. For all other uses of radio frequency, CE units must get approval before the purchase, testing, deployment, and usage of the system. **(T-3**).

3.4.5.2. **Commercial Internet & Services.** Control system devices must be configured to only utilize private IP addresses. All commercial Internet connections are prohibited unless approved by the AO and the DoD CIO has

granted a DoD Information Network (DoDIN) waiver. **(T-0).** Unauthorized connections will result in a Denial of Authorization to Operate (DATO).

3.4.5.2.1. **DoDIN Waiver Process.** Under DoDI 8010.01 and Air Force Manual (AFMAN) 17-101, the DoD Chief Information Officer (CIO) grants DoDIN waivers for procurement and use of non-Defense Information Systems Network (DISN) commercial services when in the best interest of the DoD and when Defense Information Systems Agency (DISA) services cannot support mission requirements. For further guidance on the waiver process, contact af.safcn.sro@us.af.mil.

3.4.6. **Unnecessary Connectivity.** CE units will ensure that any form of connectivity or communication protocol that is not used, not necessary for the function of the system, and not explicitly approved must be disabled in all components of the control system down to the end device. **(T-1).**

3.4.7. **Encryption.** CE units must use secured authentication and encryption protocols for data in transit and utilize encryption for data at rest and data in use (see para. 4.6.1) to the greatest extent possible without hindering functionality. **(T-3).**

3.5. Continuous Monitoring & Incident Response. There are two forms of continuous monitoring: RMF continuous monitoring & Defensive Cyber Operations (DCO) continuous monitoring for abnormal events/incidents.

3.5.1. **RMF Continuous Monitoring.** For RMF continuous monitoring, ISO, ISSM, and ISSO system-level responsibilities for continuous monitoring are outlined by the RMF process (refer to para 3.2.1 and the "*Civil Engineer Control Systems Baseline Security Controls"* memorandum). For instance, CE units must regularly evaluate the RMF security controls of their control systems (e.g., checking (and if needed, modifying) how the security controls are implemented, loading compelling artifacts into eMASS packages on recurring basis, etc.). **(T-3).**

3.5.1.1. CE units must continuously monitor their control systems' security controls according to their RMF continuous monitoring plan, regardless of the system's RMF authorization status.

3.5.1.2. CE control systems may be reauthorized or have the Authorization Termination Date (ATD) extended based on successful execution of the system's RMF continuous monitoring plan, with AO approval.

3.5.1.3. Perform security scans every 90 days on isolated CE control systems with Government Furnished Equipment (GFE) Continuous Monitoring (CONMON) laptop. Ensure proper sanitization of CONMON laptop prior and after plugging into control system to scan.

3.5.1.3.1. For systems CE cannot scan due to federal regulations (i.e., FAA), the base must contact the vendor or appropriate provider to perform the scan.

3.5.2. **DCO Continuous Monitoring**. Within the CE network enclave, Tier II Cybersecurity Service Provider (CSSP) services are provided by 16 AF through the 33 COS. For the remaining systems, further roles and responsibilities for DCO continuous monitoring are still being determined for coordination with 16 AF cyber defenders.

3.6. Hardware.

3.6.1. **Hubs.** The use of hubs will not be utilized by CE units. **(T-2).** Where used in legacy systems, plan and program for their replacement to managed switches (para 3.6.2) Please contact AFCEC/COO for further guidance. **(T-3).**

3.6.2. **Switches.** CE personnel will ensure that all control systems are utilizing managed switches. Use of switches within the control systems environment will be kept to a minimum. If used, configure switches to restrict port access to the control system. Switches will have physical (refer to para 4.5) and logical security measures. Ensure switches are stored in a locked, secure area/cabinet, and add necessary tamper-proof features to restrict access to these devices. Where used in legacy systems, plan and program for their replacement utilizing the *DISA Approved Products List* and AFCEC/COO for further guidance. **(T-3).**

3.6.3. **Servers.** CE personnel will ensure that rack mounted servers are preferred over towers or stand-alone cases. Use of specific software and hardware identified in current contract vehicles is required for servers and client workstations. **(T-1).**

3.6.4. The ISO will work with vendors to determine appropriate security settings for all control systems in accordance with NIST SP 800-82r3, NIST SP 800-53r5 and their associated components based on each system's C-I-A rating. For any device that has an applicable Security Technical Implementation Guide (STIG), follow the guide to apply the proper security controls and configurations where technically feasible. **(T-3).**

3.6.5. Implement additional routing paths, where possible, to provide redundancy.

3.6.6. ISO must ensure that control system networks that utilize virtual machines meet proper cybersecurity controls. Reference NIST SP 800-125B. **(T-3).**

3.6.7. ISSO will ensure that all unused hardware is disconnected and properly stored (see para 4.6.3). **(T-3).**

3.7. Software.

3.7.1. ISO/ISSM/ISSO will ensure that whitelisting software is used as a preferred mitigation approach per National Security Agency's (NSA) *Guidelines for Application Whitelisting Industrial Control Systems*. **(T-3).**

3.7.2. Upgrading and patching software is required for operating systems, embedded systems, and control system applications unless technologically unable. **(T-0).** Adhere to para 3.8 and the following:

3.7.2.1. The ISO/ISSM/ISSO will upgrade and maintain all operating systems (including control system components) to the most current versions applicable as approved by DISA and the DAF. **(T-3).**

3.7.2.2. Review the Long-Term Servicing Channel (LTSC): (https://usaf.dps.mil/sites/41288/SDC/Forms_Wiki/Home.aspx) for the most current operating system versions and builds.

3.7.2.3. Newly acquired control systems shall run on or be compatible with updates to the latest DoD approved operating system. **(T-1).**

3.7.3. When the control system operating system cannot be updated, a POA&M shall be documented and approved through the RMF process (refer to para 3.2) to appropriately manage the resulting security risk or to provide remediation that eliminates the risk. **(T-3).**

3.7.3.1. Once approved through the RMF process, submit waiver requests to SAF/CNZ at SAF.CNZR.Workflow@us.af.mil. **(T-1).**

3.7.4. **Ports, Protocols, and Services.** Because of the specific function of dedicated control systems devices, all ports and input/output devices shall be identified by the ISO/ISSM/ISSO as stated in UFGS-25 05 11 para 1.9.2. **(T-0).**

3.7.4.1. ISO/ISSM/ISSO must disable all unused and unnecessary ports, protocols, and services on control systems and their end devices after testing to ensure the system's operation is not affected. **(T-0).**

3.7.4.2. ISO/ISSM/ISSO will ensure that unused ports, protocols, and services remain disabled. **(T-0).**

3.7.4.3. ISO/ISSM/ISSO will configure control system network to utilize port security and MAC authentication where applicable. **(T-3).**

3.7.4.4. Implement secure protocols, where possible, to communicate with the control system(s). **(T-3).**

3.7.4.5. Develop and securely store data/network traffic-flow documentation listing the communication protocols in use by controllers and field devices connected to the control system and associated forms of connectivity. **(T-3).**

3.7.4.6. Label ports and cables with information on connection nodes to prevent misconfiguration and to aid in disaster recovery. **(T-3).**

3.7.4.7. Follow the standards and guidance listed on the DAF Ports, Protocols, and Services site (https://usaf.dps.mil/teams/IACE/Wiki/AF%20PPS.aspx). **(T-3).**

3.7.5. Only use software that is DAF-approved. **(T-1).** Uninstall software, programs, applications, and services that are unused and unnecessary for operation, maintenance, or cybersecurity of the control system (e.g., games, chat/messaging services, office productivity suites, etc.). **(T-1).** Eliminate these applications from backup or recovery software. **(T-1).**

3.8. Patch management.

3.8.1. The ISSM and ISSO, in coordination with the control system vendor, shall (1) determine a patch schedule for the control system and (2) ensure patches are validated and tested to verify safe operation of the control system after patching. **(T-2).** Installations are not expected to procure separate testbed environments. Refer to *Methods and Procedures Technical Order (MPTO) 00-33A-1109 Vulnerability Management* for guidance.

3.8.2. The ISSM and ISSO must ensure that systems are patched or updated only with digitally signed or hashed software from trusted sources that are approved by the DAF or DoD. **(T-2).**

3.8.3. See para 3.10 for on-site maintenance procedures.

3.9. Change & Configuration Management.

3.9.1. ISO/ISSM/ISSO must establish a configuration baseline for each control system and its associated components and devices. **(T-3).**

3.9.2 ISO/ISSM/ISSO will ensure that necessary changes to a control system are identified, authorized, and thoroughly documented. **(T-3).**

3.9.3. ISO/ISSM/ISSO must establish a Configuration and Change Management Plan that includes processes, procedures, and policies used to control modifications to hardware, firmware, and software, and documentation to ensure system is protected against improper modifications prior to, during, and after system implementation. **(T-3).**

3.9.3.1.Identify and acquire tools for implementing and monitoring configuration changes.

3.9.3.2.Update repository as changes are implemented.

3.9.3.3.Maintain a digital inventory for configuration management (CM) that contains configuration data of all deployed components to include install data, version and build numbers, patches, updates, physical location, etc.

3.9.4. ISO/ISSM/ISSO will ensure that change requests processes include evaluating change requests and approvals, testing configuration changes before deploying in production, having a rollback plan in place, and establishing a new baseline. **(T-3).**

3.10 On-site Maintenance.

3.10.1. ISO/ISSM/ISSO will ensure government personnel are qualified and/or vendors' credentials are verified before conducting on-site maintenance of control systems (to include patching or upgrading software). **(T-3).**

3.10.2. ISO/ISSM/ISSO will Escort and oversee on-site maintenance activities by vendors to ensure there is no operational impact or interruption to the control system. Verify vendors are connecting to control systems through proper procedures. **(T-3).**

3.10.3. ISO/ISSM/ISSO will ensure vendors performing on-site maintenance shall sign in/out with the owning organization using AF Form 1109, *Visitor Register Log*. Ensure control systems maintenance and repair is performed and logged in a timely manner. **(T-3).** The vendor shall leave a copy of their maintenance service record with the ISO detailing the work done on the control system and any repairs. **(T-3).**

3.10.4. ISO/ISSM/ISSO will provide and enforce the use of only government-owned assets (or GFE) (e.g., computer, tablet, handheld devices) to connect to control systems and control systems network enclaves for maintenance or other authorized uses. **(T-3).** The BCE may authorize temporary use of contractor-owned assets for emergency repairs through the duration of the emergency, where GFEs are not readily available or no other reasonable alternative exists. **(T-2).**

3.10.5. Government-owned maintenance assets will be maintained by the Civil Engineers and remain in government control. **(T-3).** These maintenance assets shall follow all cybersecurity practices and procedures and adhere to the following restrictions:

3.10.5.1. Uninstall any programs, applications, and services not strictly necessary (as further stated in para 3.7.5). **(T-3).**

3.10.5.2. Disable any Wi-Fi, cameras, or microphones, preferably at the hardware or physical level. **(T-3).**

3.10.6. ISO/ISSM/ISSO will ensure that on-site maintenance using a government-owned asset shall be conducted using the following procedures:

3.10.6.1. Download digitally signed or hashed software from trusted authoritative sources to a CD/DVD. **(T-3).**

3.10.6.2. Scan the CD/DVD/MMC on a computer that has scanning signatures to verify it is malware-free. **(T-3).**

3.10.6.3. Insert the CD/DVD into a government-owned asset (see para 3.10.5) to perform maintenance activity. **(T-3).**

3.10.6.4. After upgrading the system, sanitize the CD/DVD media to ensure it cannot be used in another device per AFMAN 17-1301, *Computer Security (COMPUSEC)* para 5.2. **(T-3).**

3.10.7. Further on-site maintenance requirements can be found in NIST SP 800-82r3.

3.11 Remote Maintenance. Remote maintenance increases cyber risk to CE-owned control systems because remote/off-site access is exploitable. When on-site maintenance and additional support requiring connectivity (see para 3.10) cannot be accommodated, remote maintenance access to control systems is only permitted as a last resort and must be with the permission of the BCE. Before utilizing remote connectivity, it shall be (1) justified and approved in writing by the Operations Flight Commander or Deputy and (2) recorded as part of the system's RMF package (refer to para 3.2.1). **(T-2).**

If remote maintenance is employed, the section chief shall ensure that:

3.11.1. Remote maintenance events shall be sanctioned by the CE unit to be logged, monitored, and reviewed to verify legitimacy and necessity of access. **(T-3).** Furthermore, the allotted time, initial time of access, and reason for access shall be coordinated with the vendor. **(T-3).**

3.11.2. ISSM/ ISSO will ensure that remote maintenance of the control system shall be of limited duration – allowed only for the time necessary to accomplish the established maintenance action. **(T-3).**

3.11.3. Any remote maintenance on the control system outside of the pre-arranged window shall be blocked by the ISSM/ISSO. **(T-3).**

3.11.4. ISSO/ISSM will ensure that any remote maintenance activities that involve patching or upgrading software shall follow additional guidelines outlined in paras 3.7 and 3.8. **(T-3).**

3.11.5. Follow security measures recommended in NIST SP 800-46r2, NIST SP 800-82r3, and DHS's *Configuring and Managing Remote Access for Industrial Control Systems* (Abstract: Configuring and Managing Remote Access for Industrial Control Systems | CISA, refer to the PDF at bottom of page) such as requiring encryption and token-based, multi-factor authentication. **(T- 3).**

3.11.6. The ISSM/ISSO will ensure any remote maintenance on the control system not meeting these specifications is prohibited. **(T-2).**

3.12 Solid State Devices and Removable Media. In accordance with NIST SP 800-82r3, CE personnel must not connect removable media to a control system or its network, other than as described in para 3.10.6. **(T-3).** Provisions shall be made to prohibit the connection of unauthorized items, including vendor-owned devices. **(T-3).** Modify any existing service contracts to comply as described in para 3.3.9. Follow guidance provided *in DAFMAN17-1301, 09 Dec 2024*. **(T-3).**

3.12.1. In the instance Hard Drives, Thumb Drives, Dongles, DVDs, CDs, and other removable media and storage devices are connected to a control system and associated forms of connectivity, the removable media will be scanned for viruses,

malware, etc. before connecting to a control system by the ISSM/ISSO. **(T-1).** Track and document vendor connection points, connection duration, and maintenance performed. Follow all established data loss prevention policies and protocols, ensuring alignment with incident response and disaster recovery plans to protect and restore sensitive information in the event of breach or disruption.

3.13 Privately-Owned Devices. The ISSM/ISSO will ensure that the use of privately-owned devices (i.e., not owned, provided, or approved by the government) to access, monitor, or operate control systems is prohibited. **(T-3).** The discovery of such a connection can result in issuance of a DATO and thus disconnection from the network.

3.14 Support to CE Units.

3.14.1. For specific control systems-related technical support and guidance, AFCEC/COO supports the RMF risk assessment and implements the network enclave for control systems at active-duty installations, contact the AFCEC Reach back Center at (850) 283-6995 or by e-mail at afcec.rbc@us.af.mil.

3.14.2. For technical support regarding control systems network enclave, control systems design reviews, inventory, RMF, or eMASS, contact 850-283-6898, or by e-mail at afcec.comi.icshelpdesk@us.af.mil.

3.14.3. For questions regarding CE's overall strategy and this DAFGM, contact AF.A4CP.Workflow@us.af.mil

3.14.4. HQ NGB/A4 and HQ AFRC/A4 will provide technical support and guidance as required.

Chapter 4

CONTROL SYSTEMS CYBER HYGIENE

Follow and review the modified list of foundational cyber hygiene requirements below. Additionally, the technical references listed in Attachment 1 provide comprehensive protection procedures.

4.1. Before selecting links or system prompts, check if it is expected, and validate it is from a trusted source. Be cautious of any messages received that contain a hyperlink, even if it seems to be from a friend or a trusted organization.

4.2. ISO will ensure system operators use and maintain control systems IAW manuals and technical specifications provided by the vendor. **(T-3).**

4.3. Education & Training Course

CE Air Force Institute of Technology (AFIT) School House offers three Cybersecurity Basic Training (CBT) courses for control systems that provide hands-on learning experiences and practical training for civil engineers. This training is available and recommended for all CE personnel.

4.3.1. WENG 170 – Cybersecurity for Control Systems

4.3.1.1 Ensure Air Force Specialty Codes (AFSCs) 3E0X1, 3E0X2, 3E1X1, and 3E4X1/A incorporate core training at the 3-skill, 5-skill, 7-skill levels for Active Duty and Air Reserve Component (ARC). Journeymen and Craftsmen level must incorporate core task cybersecurity training. Follow *Change to Upgrade Training Requirement for AFSCs 3E0X1, 3E0X2, 3E1X, and 3E4X1*. Refer questions to AFCEC/COF Chief of Force Development.

4.3.1.2 Federal Wage Service (FWS) who fall under the targeted series in Career field education and training plan (CFETP) are required to complete WENG170 across all grade levels.

4.3.1.3 The Base Civil Engineer, Deputy Base Civil Engineer, Operations Flight Chief, and Installation Management Flight Chief must complete WENG 170 *Control Systems Cybersecurity Training for Civil Engineer Personnel*. **(T-0)**

4.3.1.4 All remaining CE personnel performing duties that impact control systems are highly encouraged to complete WENG 170 per *Career field education and training plan (CFETP).*

4.3.1.5 For questions concerning this training, or to receive a copy of the enforcement training memorandum, reach out to AF.A4CCivilian.CareerFieldManager@us.af.mil.

4.3.2. WENG 270 – Advanced Control System Cybersecurity

4.3.2.1 This is an AFCEC funded 5-day hands on cybersecurity training course available to any CE personnel, with military being given priority. (AFSCs) 3E0X1, 3E0X2, 3E1X1, and 3E4X1/A incorporate in-resident 7-level training at Wright Patterson AFB, OH campus. 7-level skill (Craftsman) must complete the training. These important changes are effective 18 April 2025 for the active-duty community and optional for ARC. Reference *Change to Upgrade Training Requirement for AFSCs 3E0X1, 3E0X2, 3E1X1, and 3E4X1/A*. Refer questions to AFCEC/COF Chief of Force Development. **(T-0).**

4.3.3. WENG 370 – Control Systems Cybersecurity for CE Leaders

4.3.3.1 Individuals in leader (WL) or supervisory positions (WS) must complete WENG 370. Reference enforcement training memorandum *Control Systems Cybersecurity Training for Civil Engineer Personnel*. **(T-0).**

4.3.3.2 The Base Civil Engineer, Deputy Base Civil Engineer, Operations Flight Chief, and Installation Management Flight Chief must complete per enforcement training memorandum *Control Systems Cybersecurity Training for Civil Engineer Personnel*. **(T-0).**

4.3.3.3 For questions concerning this training, or to receive a copy of the enforcement training memorandum, reach out to AF.A4CCivilian.CareerFieldManager@us.af.mil

4.3.4. Training requirements expire after Career Field Education and Training Plans (CFETPs) are published to capture these new requirements.

4.3.5. Unit Training Managers (UTM) will be responsible for tracking and ensuring timely completion of these training requirements in section 4.3. **(T-0).**

4.3.6. Cyber Security for Control Systems Training is available via myLearning at https://lms-jets.cce.af.mil/moodle/.

4.4. Authentication/User Account Management.

4.4.1. ISSM/ISSO will ensure all personnel are educated on their responsibility for password/account protection. **(T-3).**

4.4.1.1 Shared, guest, and group accounts are not allowed and shall be disabled unless necessary for system functionality by the ISSM/ISSO. If deemed necessary, document and maintain all account information including reason for the account, who has access and how risks are mitigated. **(T-3).**

4.4.1.2 ISSO / ISSM will ensure that all personnel have a unique account configured based on required roles and responsibilities adhering to the principles of least privilege. **(T-3).**

4.4.2. ISSM/ISSO will eliminate the use of default usernames and passwords. **(T-3).** Additionally, all new passwords will follow requirements in DoDI 8520.03, *Identity Authentication for Information Systems*. **(T-0).**

4.4.3 ISSM/ISSO will review control system audit logs for unauthorized attempts or indicators of compromise. **(T-3).**

4.4.4 CE personnel will not share passwords. **(T-3).** In the event of a compromised password, change the password immediately. **(T-3).**

4.4.5. ISSM/ISSO will check all user accounts and policies periodically and delete accounts that are unused or no longer necessary (e.g., personnel permanently leave a role or location). **(T-3).**

4.4.6. ISSM/ISSO must apply the "principle of least privilege" to limit authorized users on an as-needed basis with permissions pertinent to the users' role. Enforce the "separation of duties" methodology when assigning personnel to roles. Additionally, personnel with multiple roles shall have different login credentials for each account. **(T-3).**

4.4.7. ISSM/ISSO will configure system settings (beyond default) where applicable, to improve cybersecurity posture. Ensure all control systems and components require a login/logout function. Do not bypass the system's authentication mechanisms and account "lock out" settings, including multi-factor authentication, automatic session time-out or termination (e.g., 30 minutes of inactivity), account lockout after multiple failed login attempts. **(T-3).** Account activity should be logged and audited regularly to catch potential malicious actions. **(T-3).**

4.4.8. Foreign Nationals may be provisioned with accounts per DAFMAN 17-1301, *Computer Security*, para 4.2.5 and must adhere to DAFMAN 17-1304, Sec. 5.3.5.

Per DAFMAN 17-1304, "Identity and Credential Access Management (ICAM)", section 3.2.2.3, the ISO must ensure systems on COIN shall adhere to DoD CIO memorandum, Interim Digital Authentication Guidelines for Unclassified and Secret-level DoD Networks and Information Systems, for specific use cases and exceptions. **(T-0).** The ISO/ISSM will ensure that privileged user management adhere to DAFMAN 17-1304, Section 5.4.3 Privileged. **(T-3).**

4.5. Physical Access Control.

4.5.1. ISSM/ISSO will store computers and interfaces that support control systems in a secure space equipped with operational locking mechanisms, such as on cabinets, doors, and enclosures. Physical access to this space must be monitored and restricted to authorized personnel only. **(T-3).**

4.5.2. ISSM/ISSO must abide by strict access control protocols to prevent unauthorized physical access to all components of control systems (particularly focusing on control nodes) and the unauthorized introduction of new hardware, infrastructure, and communications interfaces where feasible. Install intrusion detection on all enclosures that house critical infrastructure components (i.e., cabinets and panels) to alert personnel of unauthorized activity where feasible. If using electronic tokens, ensure two-factor authentication is used to guard against card duplication. **(T-3).**

4.5.3. CE Squadron leadership will designate in writing a key and lock custodian. Maintain positive, traceable key control by establishing policies and procedures. Ensure keys are not stored with currently used locks and panels are locked when not in use.

4.5.4. ISSM/ISSO will document who has control over control systems equipment locations (e.g., electrical, mechanical, communications rooms). **(T-3).**

4.5.5. ISSM/ISSO must document and confirm the physical security of control systems and components in the inventory on a quarterly basis (refer to para 3.1). **(T-3).**

4.6. Data Storage and Disposal.

4.6.1. ISSO will apply security techniques such as encryption and/or cryptographic hashes, to control systems, data storage, and communications where determined appropriate by ISO and local policy. **(T-3).**

4.6.2. ISSO will conduct backups of control systems quarterly and maintain, and properly store "gold copy" resources, such as firmware, software, ladder logic, service contracts, product licenses, product keys, and configuration information. Ensure that all "gold copy" resources are stored off-network and store at least one copy in a locked tamper-proof environment (e.g., locked safe) for business continuity and disaster recovery. **(T-3).**

4.6.3. When a control system is no longer required, the ISO will take appropriate action to ensure the system and its data is properly disposed per established procedures detailed in NIST SP 800-53r5, MP-6, NIST SP 800-82r3 para 6.2.7, and AFMAN 17-1301 chapter 5. **(T-3).**

4.7. Response, Recovery, and Contingency Plans.

4.7.1. ISO/ISSM/ISSO will evaluate, design, and implement contingencies based on mission requirements to ensure continuity of operations in the event of system degradation by kinetic or non-kinetic means (e.g., redundancies, manual operations, fail-over to back-up systems). **(T-1)**

4.7.2.ISO/ISSM/ISSO will ensure response plans (Incident Response/Business Continuity), recovery plans (Incident Recovery/Disaster Recovery), and contingency plans are in place

and managed per NIST SP 800-82r3 para 6.2.6 and 6.2.8. **(T-1).** Develop Response, Recovery, and Contingency Plans if they do not currently exist. Reference the *DoD AFCEC RMF Assessment and Authorization Process Incident Response Plan* template for guidance on getting started. **(T-1).**

4.7.3. Plans will contain a list of POCs by the ISO, clear roles and responsibilities, specific tactics, techniques, and procedures for when abnormal system operation is detected. **(T-1).** Document the systems critical to mission and prioritize resiliency requirements for system reactivation and restoration in case of a cyber-incident. Such a plan may include disabling affected user accounts, isolating suspect systems, an immediate 100 percent password reset (refer to para 4.3), etc. The plan may also define escalation triggers and actions, including incident response, investigation, and public affairs activities.

See DoD's *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)* (https://apps.dtic.mil/sti/pdfs/AD1056116.pdf) for examples of applicable procedures to be considered to use for tailoring to installation-specific conditions. Reference AFI 17-130 *Cybersecurity Program Management* and AFI 17-203 *Cyber Incident Handling* for additional guidance.

4.7.4. ISO/ISSM/ISSO will ensure plans are tested, reviewed annually at a minimum and updated as necessary and documented in the system accreditation package. **(T-2).**

4.7.5. ISO/ISSM/ISSO must have system recovery and contingency plans in place, including having recovery disk(s) and source configuration backups ready to restore systems to known good states. **(T-1).**

4.7.5.1. Additionally, ISSM/ISSO must ensure the ability to revert to manual operations in the instance connection is lost or if a system is "blacklisted." **(T-1)**.

4.7.6. Coordinate with Comm units to ensure Mission Critical CE control systems are included in installation operational and contingency plans for disconnected base operations and AF network protection and collapse.

4.7.7. For additional information on developing incident response actions for systems based on their risk levels and making risk-informed decisions for resiliency, reference the USCCI 5200-13 *Cyberspace Protection Conditions*.

4.8. Ransomware. Ransomware poses a growing threat to DAF infrastructure. Follow the guidance in this policy and review and implement Cybersecurity & Infrastructure Security Agency (CISA) best practices for protecting against ransomware threats (https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf). The ISSM/ISSO must ensure COIN connected systems are scanned for ransomware on a regular basis, and stand-alone systems are scanned on the quarterly continuous monitoring scan. **(T-3).**

Chapter 5

ZERO TRUST

5.1. The DAF is reshaping its cybersecurity framework and strategy to prioritize the protection of individual data as a strategic asset. By leveraging advanced Zero Trust (ZT) methodologies, the DAF emphasizes treating every connection as untrusted. Components must achieve the intended Target level outcomes for components by the end of FY2027 as stated in *DoD Zero Trust Strategy (2022)* for IT systems. However, while the strategy acknowledges the importance of applying Zero Trust to Operational Technology (OT) systems, it does not set a target date for OT implementation.

5.2. The Zero Trust (ZT) security model, characterized by continuous authentication and fine-grained policy enforcement, is being adapted for Operational Technology (OT) environments within the DoD, guided by the DoD ZT Roadmap and related documents. While the core ZT principles of data protection, strong authentication, network segmentation, and threat monitoring could be applicable to OT, their implementation necessitates careful consideration of OT-specific constraints, such as legacy equipment, diverse industrial protocols, process criticality, and distinct acquisition and authorization processes. Standard IT security approaches can be ineffective for OT, making ZT adoption more challenging and requiring thorough risk mitigation, often through testing.

5.3. The ZT Functional Management Office (FMO) applied inputs from multiple DAF working groups, industry, academia, ZT subject matter experts (SMEs), and stakeholders. A specific working group was established to focus on Non-Enterprise IT [Non-EIT] (includes control systems), enabling collaboration among Airmen, Guardians, application owners, system owners, and mission partners ensuring relevant section and application of the ZT Target (91) and Advanced (51) activities supporting the holistic DAF enterprise architecture.

5.4. Evaluating Zero Trust (ZT) activities in an Operational Technology (OT) environment requires collaboration between authorized personnel, OT system owners, and security professionals. This evaluation must consider specific operational constraints and risk profiles. While the ZT activities and outcomes are designed to be broadly applicable, system owners may determine that certain activities are inapplicable to their specific OT environment (e.g., standalone systems lacking threat stream ingestion).

Civil Engineer units are encouraged to familiarize themselves with zero trust content in anticipation of official guidance. This awareness will facilitate a smoother implementation process once the policy is formally adopted.

5.5. Zero Trust Pilot

5.5.1. Zero Trust (ZT) pilot programs are underway to evaluate the feasibility and implementation of ZT technology in Operational Technology (OT) systems.

5.5.2. Prior to a ZT Pilot inception, AFCEC/COO and AF/A4C must be involved in the process for CE control systems.

5.5.3. No Zero Trust pilot equipment will be installed on authorized CE Control System unless approved by the Authorizing Official. Zero Trust pilot approval must meet the interim authority to test (IATT) policy as defined by the AO.

5.5.4. Required Zero Trust Features for Pilots. Pilots planning to utilize commercial cellular or satellite internet connectivity to test communication between cloud and CS devices must, at minimum, implement the following cryptographic features for all client devices behind the Internet gateway.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order on Improving the Nation's Cybersecurity, 12 May 2021

Title 40 U.S.C. § 11101, *Public Buildings, Property, and Works,* 14 January 2019

Title 42 U.S.C. § 5195c(e), *Emergency Preparedness – Critical Infrastructure Protection*, 14 January 2019

Title 44 U.S.C. § 3552, *Coordination of Federal Information Policy*, 14 January 2019

DODD 3020.40*, Mission Assurance (MA)*, 11 September 2018

DODD 8100.02, *Use of Commercial Wireless Devices*, 23 April 2007

DODI 4165.14, *Real Property Inventory (RPI)*, 8 September 2023

DODI 4170.11, *Installation Energy Management*, 31 August 2018

DODI 5000.64, *Accountability of DoD Equipment*, 10 June 2019

DODI 5200.44, *Trusted Systems and Networks (TSN)*, 16 February 2024

DODI 8010, *DODIN Transport*, 10 September 2018

DoDI 8420.01, *Commercial WLAN Technologies*, 03 November 2017

DODI 8500.01, *Cybersecurity*, 07 October 2019

DODI 8510.01, *RMF for DoD Systems*, 09 July 2022

DODI 8520.03, *Identify Authentication*, 19 May 2023

DODI 8530. 01, *Cybersecurity Support to DODIN Ops*, 31 May 2023

CJCSI 6211.02D, *DISN Responsibilities*, 04 August 2015

DoD 8140.01, *Cyberspace Workforce Management*, 5 October 2020

DoD CIO Memo – *Control Systems Cybersecurity*, 18 December 2018

Deputy SecDef Memo – *Enhancing Cybersecurity Risk Management*, 19 July 2018

DFARS Clause 252.204.7012, *Cyber Incident Reporting*, 15 February 2024

OUSD(A&S) Memo – *Utilities Privatization Guidance,* 07 February 2019

OUSD(A&S) Memo – *DFARS Cybersecurity Rule*, November 2020

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

AFPD 32-10, *Installations and Facilities*, 20 July 2020

AFI 17-201, *C2 for Cyberspace Ops*, 05 March 2014

AFI 17-101, *RMF for AF IT*, 6 February 2020

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020

AFI 33-322, *Records Management,* 23 March 2020

AFMAN 17-1301, *COMPUSEC*, 09 Dec 2024

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

DAFI 17-220, *Spectrum Management,* 08 June 2021

DAFI 32-9005, *Real Property Accountability*, 14 September 2022

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

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

CNSSI No, 1253, *Security Categorization*, 29 July 2022

CNSSI No. 4009, *CNSS Glossary*, 02 March 2022

CISA Alerts and Advisories

CISA Guide to securing remote access software, June 2023

DHS Procurement Language for Control Systems, September 2009

DHS Wi-Fi Security Guide, 15 March 2017

NSA Guidelines for Application Whitelisting, 01 April 2016

NIST CSF 2.0

NIST SP 800-37r2, *RMF*, December 2018

NIST SP 800-40r4, *Patch Management*, 6 April 2022

NIST SP 800-46r2, *Telework & BYOD Security*, July 2016

NIST SP 800-53r5, *Security & Privacy Controls*, September 2020

NIST SP 800-82r3, *OT Security*, September 2023

NIST SP 800-125B, *Secure VM Configuration*, 07 March 2016

NIST SP 800-128, *Security-Focused Config Management*, 10 October 2019

NIST SP 800-137, *ISCM,* September 2011

NIST SP 800-171r2, *CUI Protection*, February 2020

FIPS PUB 140-3, *Cryptographic Modules*, 22 March 2019

IEEE 802.11-2016, 26 February 2021

NTIA Redbook, January 2021

OMB Circular A-130, 28 July 2016

OMB Memo M-02-01, 17 October 2001

JP 1-02, *DoD Dictionary*, January 2020

Control Systems Cyber Defense Reference Architecture, February 2022

Department of the Air Force Strategic Plan for Control Systems, March 2021

Department of the Air Force Implementation Plan for Control Systems, March 2021

DAF CE Control Systems Baseline Security Controls, 29 February 2024

DoD ACI TTP for ICS, March 2018

Enforcement Training Memo – Cybersecurity Training, 3 November 2021

Enforcement Training Memo – Upgrading Training, 21 September 2021

Enforcement Training Memo – Upgrade Training, 8 June 2023

HAF AF/A4CF Business Rules for MILCON, 30 December 2019

RAND Cybersecurity Risk to CE Infrastructure, January 2019

UFC 3-410-02, *HVAC Control Systems*, 12 April 2021

UFC 4-010-06, *Facility-Related Control Systems Cybersecurity*, 10 October 2023

UFGS-25 05 11, *Facility-Related Control Systems Cybersecurity*, 01 May 2021

USCCI 5200-13, *Cyberspace Protection Conditions*, 10 August 2023

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

Abbreviations and Acronyms

ACI TTP — Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures

AF/A4C — The Director of Civil Engineers

AF/A4CP – The Director of Civil Engineers Strategy and future concepts branch

AFCEC — Air Force Civil Engineer Center

AFCEC/COO — AFCEC Operations Maintenance Division

AFI — Air Force Instruction

AFIMSC — Air Force Installation and Mission Support Center

AFIMSC/RM — AFIMSC Resource Management Directorate

AFIN — Air Force Information Network

AFMAN — Air Force Manual

AMRS — Advanced Meter Reading System

AO — Authorizing Official

AODR — Authorizing Official Designated Representative

ATO — Authorization to Operate

CISA — Cybersecurity and Infrastructure Security Agency

CNSSI — Committee on National Security Systems Instruction

COIN — Community of Interest Network

CONMON – Continuous Monitoring

CROCS – Cyber Resiliency Office for Control Systems

CSSP — Cybersecurity Service Provider

CYBERCOM — United States Cyber Command

DAF — Department of the Air Force

DAFGM — Department of the Air Force Guidance Memorandum

DAFI — Department of the Air Force Instruction

DATO — Denial of Authorization to Operate

DCI – Defense Critical Infrastructure

DCO – Defensive Cyber Operations

DFARS — Defense Federal Acquisition Regulation Supplement

DHS — Department of Homeland Security

DISA — Defense Information Systems Agency

DISN — Defense Information Systems Network

DoDD — Department of Defense Directive

DoDI — Department of Defense Instruction

DoDIN — Department of Defense Information Network

eMASS — Enterprise Mission Assurance Support Service

EOD — Explosive Ordnance Disposal

ESPC — Energy Savings Performance Contract

ESTCP — Environmental Security Technology Certification Program

HQ AFRC/A4 — Headquarters Air Force Reserve Corp/A4

HQ NGB/A4 — Headquarters National Guard Bureau/A4

IATT – Interim Authorization to Test

ICS — Industrial Control System

ICS-CERT — Industrial Control Systems Cyber Emergency Readiness Team

IEEE — Institute of Electrical and Electronics Engineers

ISO — Information System Owner

ISSM — Information System Security Manager

ISSO — Information System Security Officer

IT — Information Technology

MMC — Multimedia Card

NexGen IT- NexGenIT is the official platform for the Air Force's accountable property system of record

NIST SP — National Institute of Standards and Technology Special Publication

NSA - National Security Agency

NSS – National Security System

OMB — Office of Management and Budget

OUSD (A&S) — Office of the Under Secretary of Defense for Acquisition and Sustainment

OT — Operational Technology

RMF — Risk Management Framework

SAF/DS — Office of the DAF Chief Information Officer

SAF/CNZ — DAF Chief Information Security Officer

SCA — Security Controls Assessor

SCAR — Security Controls Assessor Representative

SFTP — SSH File Transfer Protocol

UESC — Utility Energy Service Contract

UFC — Unified Facilities Criteria

UR — User Representative

U.S.C. — United States Code

ZT — Zero Trust

Terms

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, policymakers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems (ref. AFI 17-201).

Asset – A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or

operated by domestic, foreign, public, or private sector organizations (ref. DoDD 3020.40).

Authorization Boundary – All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected (ref. OMB Circular A-130 and NIST SP 800-37r2).

Approval to Connect (ATC) – The official management decision given by a senior organizational official to authorize connection of an information system to an enclave 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 (ref. AFI 17-101).

Authorization to Operate (ATO) – The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems (ref. OMB Circular A-130 and NIST SP 800-37r2)

Authorized User – Any appropriately cleared individual required to access a DoD IS to carry out or assist in a lawful and authorized governmental function. Authorized users include DoD employees, contractors, and guest researchers (ref. DoD 8570.01-M).

Authorizing Official (AO) – A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation (ref. OMB Circular A-130 and NIST SP 800-37r2).

Availability – Ensuring timely and reliable access to and use of information (ref. 44 U.S.C. § 3552).

Confidentiality – Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information (ref. 44 U.S.C. § 3552).

Configuration Management – A collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle (ref. NIST SP 800-128).

Continuous Monitoring – Maintaining ongoing awareness to support organizational risk decisions (ref. NIST SP 800-137 and DoDI 8500.01).

Control System – A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs, and other types of industrial measurement and control systems (ref. NIST SP 800-82r3).

Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (ref. 42 U.S.C. § 5195c(e)).

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 non-repudiation (ref. OMB Circular A-130 and DoDI 8500.01).

Cybersecurity Service Provider – An organization that provides one or more cybersecurity

services to implement and protect the DoDIN (ref. DoDI 8530.01 and further described at (https://www.disa.mil/Cybersecurity/Network-Defense/CSSP).

Denial of Authorization to Operate (DATO) – If risk is determined to be unacceptable when compared to the mission assurance requirement, then the AO, in collaboration with all program stakeholders, will issue the authorization decision in the form of a DATO. If the system is already operational, the responsible AO will issue a DATO and operation of the system will cease immediately. Network connections will be immediately terminated for any system that is issued a DATO (ref. AFI 17-101 para 4.8.1).

Department of Defense Information Network (DoDIN) – The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called DODIN (ref. JP 1-02).

DoD Advanced Zero Trust - Achievement of the full set of identified Zero Trust capability outcomes and activities that enable adaptive responses to cybersecurity risk and threats. Reaching an "advanced" state does not mean an end to maturing ZT; rather, protection of attack surfaces will continue to adapt and refine as the malicious attack approaches and vectors mutate (ref. DoD Zero Trust Strategy).

DoD Zero Trust Pillars - Seven capability pillars of Zero Trust that provide the foundational areas for the DoD Zero Trust Security Model and DoD ZT Architectures, including focus for the implementation of ZT controls as defined by the DoD Zero Trust Reference Architecture, v2 (ref. DoD Zero Trust Strategy).

DoD Zero Trust Capability Roadmap - Lays out how the DoD currently envisions achieving capability-based outcomes. The roadmap defines ZT capability outcomes to achieve DoD Zero Trust Target Level, identifies activities, outlines dependencies and interdependencies impacting sequence and parallel development, and provides a general timeline to achieve outcomes by fiscal year (ref. DoD Zero Trust Strategy).

DoD Zero Trust Ecosystem - Consists of the breadth of DoD leaders, mission owners, and partners (internal and external) who are stakeholders in the success of Zero Trust implemented across the Information Enterprise [IE] (ref. DoD Zero Trust Strategy).

DoD Zero Trust DOTMLPF-P Execution Enablers - Cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of DOTMLPF-P (e.g., ZT Training, etc.) that support the design, development, and deployment of the ZT Capabilities required to achieve the DoD Target and Advanced Levels (ref. DoD Zero Trust Strategy).

DoD Zero Trust Framework - An official cybersecurity blueprint, based on the seven DoD Zero Trust Capability Pillars, which describes how the DoD will achieve ZT by providing the foundation and the direction to help align on-going and future ZT-related efforts, investments, and initiatives (ref. DoD Zero Trust Strategy).

DoD Zero Trust Security Model - A more robust cybersecurity model that eliminates the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies based on the concept of least privileged access as defined by the DoD Zero Trust Reference Architecture, v2 (ref. DoD Zero Trust Strategy).

DoD Zero Trust Target Level - The required minimum set of Zero Trust capability outcomes and activities necessary to secure and protect the DoD's DAAS to manage risks from currently

known threats; includes basic and intermediate Zero Trust maturity as defined by the ZT RA (ref. DoD Zero Trust Strategy).

Enclave – Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location (ref. CNSSI No. 4009 and DoDI 8500.01).

Facility – A building, structure, or linear structure whose footprint extends to an imaginary line surrounding a facility at a distance of 5 feet from the foundation that, barring specific direction to the contrary such as a utility privatization agreement, denotes what is included in the basic record for the facility (e.g., landscaping, sidewalks, utility connections). This imaginary line is commonly referred to as the "5-foot line". A facility will have an RPUID received from the RPUIR and is entered into a Service RPI system as a unique RP record (ref. DoDI 4165.14 and DAFI 32-9005).

Hardware – The material physical components of a system (ref. CNSSI No. 4009).

Incident – An occurrence that- (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (ref. 44 U.S.C. § 3552).

Information – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (ref. OMB Circular A-130).

Information System Owner (ISO) – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system (ref. NIST SP 800- 37r1). *Note: For the purposes of the DoD, per DoDI 8510.01, the term is not synonymous with "Program Manager" or "PM." For the purposes of the Department of the Air Force, refer to AFI 17-101*

Information System Security Manager (ISSM) – Individual responsible for the information assurance of a program, organization, system, or enclave (ref. CNSSI No. 4009). *Note: For the purposes of the Department of the Air Force, refer to AFI 17-101*.

Information System Security Officer (ISSO) – Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program (ref. CNSSI No. 4009). *Note: For the purposes of the Department of the Air Force, refer to AFI 17-101*.

Information Technology (IT) – (A) With respect to an executive agency means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the 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 that requires the use— (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract (ref. 40 U.S.C. § 11101).

(D) **Installation** – A base, camp, post, station, yard, center, homeport facility for any ship or other

activity under the jurisdiction of the Department of Defense, including any leased facility, which is located within any of the States, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Virgin Islands, the Commonwealth of the Northern Mariana Islands or Guam. An installation is composed of a collection of sites under a single Installation Commander. The sites under the installation are the physical locations. One of these sites is referred to as the primary site. Such term does not include any facility used primarily for civil works, rivers and harbors projects or flood control projects. In a foreign country, an installation is any property under the operational control of the Secretary of a military department or the Secretary of Defense, without regard to the duration of operational control and by agreement with foreign governments or through other rights (ref. DoDI 4165.14 and DAFI 32-9005).

Integrity – Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity (ref. 44 U.S.C. § 3552).

IATT - Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization (CNSSI 4009-2015.)

Mission Assurance – A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission- essential functions in any operating environment or condition (ref. DoDD 3020.40).

Network – A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices (ref. NIST SP 800-53r5).

National Security System – any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; (5) is critical to the direct fulfillment of military or intelligence missions (not including systems used for routine administrative and business applications, e.g., payroll, finance, logistics, and personnel management applications. (ref. 44 U.S.C. 3552(b)(6); EO 14028)

Operational Technology – Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, building management systems, fire control systems, and physical access control mechanisms (ref. NIST SP 800-37r2).

Patch – A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component (ref. CNSSI No. 4009).

Plan of Action & Milestones – A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones (ref. OMB Memorandum M-02-01).

Real Property – Land and improvements to land (e.g., buildings, structures, and linear structures (see *facility*) (ref. DoDI 4165.14 and DAFI 32-9005).

Real Property Installed Equipment – An item of equipment that is affixed and built into a facility as an integral part of that facility. To qualify as real property installed equipment, the equipment

must be necessary to make the facility complete, and if removed, would destroy, or severely reduce the designed usefulness and operation of the facility.

The real property installed equipment costs are included as a funded initial construction or renovation cost. Real property installed equipment may be accounted for as a real property equipment asset record, but not as a separate facility record in the real property inventory. Real property installed equipment includes such items as control systems, heating, cooling, electrical, emergency lighting, etc. (ref. DAFI 32-9005).

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, and uninstalling a software application (ref. NIST SP 800-40r2).

Remote Maintenance – Maintenance activities conducted by individuals communicating through an external network (ref. CNSSI No. 4009).

Resilience – The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (ref. OMB Circular A-130).

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (ref. OMB Circular A-130).

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.

Part of risk management incorporates threat and vulnerability analyses and analyses of privacy- related problems arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with risk analysis (ref. NIST SP 800-39).

Risk Management – The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time (ref. OMB Circular A-130).

Risk Mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (ref. CNSSI No. 4009).

Sanitize – A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media (ref. AFMAN 17-1301).

Security Control – The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information (ref. OMB Circular A-130).

Security Control Baseline – The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system (ref. OMB Circular A-130).

Software – Computer programs and associated data that may be dynamically written or modified during execution (ref. CNSSI No. 4009).

Stand-Alone System – System that is not connected to any other network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary (ref. DoDI 8500.01).

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system (ref. NIST SP 800-53r5).

Tailoring – The process by which security control baselines are modified by identifying and designating common controls; applying scoping considerations; selecting compensating controls; assigning specific values to agency-defined control parameters; supplementing baselines with additional controls or control enhancements; and providing additional specification information for control implementation. The tailoring process may also be applied to privacy controls (ref. OMB Circular A-130).

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (ref. CNSSI No. 4009).

Zero Trust – Term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero-trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource (ref. NIST 800-207).