



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

DAFGM2023-32-01  
27 June 2023

MEMORANDUM FOR MAJCOMs/FLDCOMs/FOAs/DRUs  
DISTRIBUTION ON C

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](http://www.e-Publishing.af.mil) for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A4CS, Systems & Data Division

By Order of the Secretary of the Air Force, this Department of the Air Force Guidance Memorandum (DAFGM) re-issues the March 2022 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 Department of the Air Force publications, the information herein prevails, in accordance with 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 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 in accordance with 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.

TOM MILLER, Lieutenant General, USAF  
DCS/Logistics, Engineering & Force Protection

Chapters:

- |                               |                                  |
|-------------------------------|----------------------------------|
| 1. Overview                   | 3. Cybersecurity Implementation  |
| 2. Roles and Responsibilities | 4. Control Systems Cyber Hygiene |

Attachments:

1. Glossary of References and Supporting Information

## Chapter 1

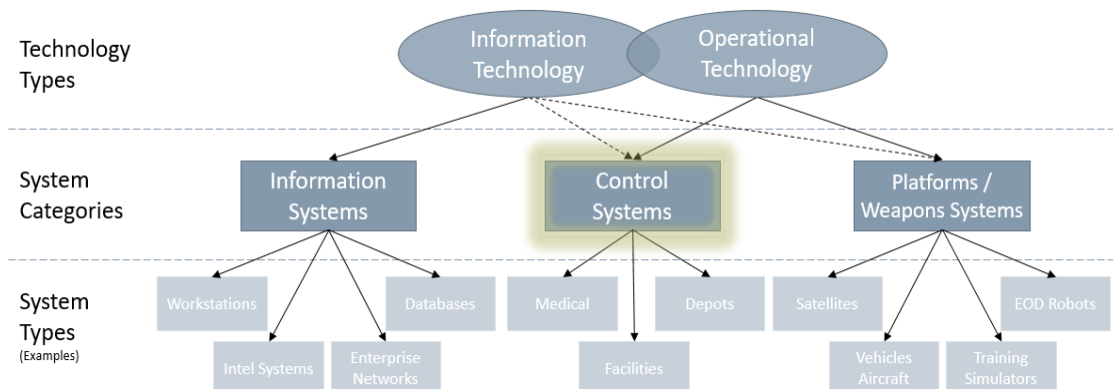
### OVERVIEW

#### 1.1. Control Systems Background.

1.1.1. Operational Technology<sup>1</sup> has become ubiquitous and integrated into every piece of modern life. Throughout the DAF, control systems<sup>2</sup> (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).

1.1.1.1. 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 as building automation systems, energy management control systems, or industrial control systems. Typically, they consist of components that can be categorized as inputs, controllers, actuators, sensors, and outputs.

1.1.2. 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 by adversaries, (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.



<sup>1</sup> “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).

<sup>2</sup> 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 industrial measurement and control systems.” [NIST SP 800-82r2, May 2015]

Figure 1: Terminology

1.1.3. The difference between information technology (IT) and operational technology 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 and (4) effective against today's threats.

1.1.4. 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 Department of the Air Force Chief Information Security Officer's (CISO) (SAF/CNZ) 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.):

- 1.2.1. Supervisory Control and Data Acquisition systems
  - 1.2.1.1. Protective relays (microprocessor-based)
  - 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 Automation Systems
  - 1.2.2.1. Energy Management Control Systems
  - 1.2.2.3 Heating Ventilation & Air Conditioning
  - 1.2.2.3. Advanced Meter Reading Systems
  - 1.2.2.4. Interior/exterior lighting controls

- 1.2.3. Life Safety systems<sup>3</sup>
  - 1.2.3.1. Fire Alarm Reporting Systems
  - 1.2.3.2. Fire Suppression Systems
  - 1.2.3.3. Facility Mass Notification Systems
- 1.2.4. Utility Monitoring and Control Systems
  - 1.2.4.1. Electrical distribution systems
  - 1.2.4.2. Generator monitoring systems
  - 1.2.4.3. Uninterrupted Power Supply system
  - 1.2.4.3. Electrical Vehicle Supply Equipment
- 1.2.5. Airfield Control Systems
  - 1.2.5.1. Airfield Lighting Control Systems<sup>4</sup>
  - 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. Traffic Control Systems
  - 1.2.6.1. Drop-arm barriers
  - 1.2.6.2. Pop-up barriers
  - 1.2.6.3. Traffic signal systems
- 1.2.7. Intrusion Detection Systems<sup>5</sup>
  - 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 not include:
  - 1.2.9.1. Systems in the CE IT and CE Platforms boundaries (e.g., NexGen IT, BUILDER, survey equipment, Explosive Ordnance Disposal (EOD) robots, 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/platforms.

---

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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

**2.1. Technical Director-Control Systems Cybersecurity Department of the Air Force.** Serves as the Department of the Air Force (DAF) Director of critical infrastructure and control systems' cybersecurity and cyber resilience, providing technical oversight for world-wide operations of USAF and USSF objectives, and provides direction and recommended actions on matters pertaining to formulation, review and execution of plans, policies, technical capabilities and programs related to the entire spectrum of control systems activities across the DAF. **(T-1).**

**2.2. Chief Information Security Officer (CISO), SAF/CNZ.** Develops, implements, maintains, and enforces the DAF Cybersecurity Program and the RMF process, roles, and responsibilities. Serves as the DAF Risk Executive ensuring individual system risk reflects organizational risk tolerance and is considered along with other risk affecting mission/business success IAW AFI 17-130, and NIST SP 800-39, Managing Information Security Risk.

**2.3. 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). **(T-1).**

**2.4. 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 **(T-1).**

**2.5. Authorizing Official (AO).** Appointed by SAF/CN and responsible for all roles listed in AFI 17-101 para 3.3, including managing the risk of control systems and tailoring controls to balance security and mission needs. **(T-1).**

**2.6. Authorizing Official Designated Representative (AODR).** Appointed by the AO and responsible for all roles listed in AFI 17-101 para 3.5 including CE Control System asset portfolio oversight and management (including cybersecurity requirements) via the Facility Operations Enterprise Manager, reviewing and validating annual requirements for OAC18 funding and distributes funding based on availability, and performing Program Objective Memorandum (POM) duties including interaction with AF/A4P. **(T-1).**

**2.7. Security Controls Assessor (SCA).** Appointed by the CISO and responsible for all roles listed in AFI 17-101 para 3.6, including supporting the AO in making assessment determinations and authorization recommendations. **(T-1).**

**2.8. Security Controls Assessor Representative (SCAR).** Appointed by SCA per AFI 17-101, Table 3.1, and responsible for fulfilling duties under the SCA's direction. **(T-1).**

**2.9. Air Force Civil Engineer Center (AFCEC).**

2.9.1. 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).**

2.9.2. 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 2.8.3, 2.8.5, 2.10.3, 2.10.4, 3.1). **(T-1).**

2.9.3. 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:

2.9.3.1. Support RMF authorization processes in the Civil Engineer enterprise for control systems aligned with RMF roles (para 2.3-2.6, 2.9-2.12), para 3.2.1, and para 3.5.1 in coordination with the AO. **(T-1).**

2.9.3.2. Perform RMF activities: establish Security Control Baseline, 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).**

2.9.3.3. Maintain “RMF continuous monitoring plan” template and determine “RMF continuous monitoring” control set (both approved by the AODR) that installations can leverage for each control system’s continuous monitoring plan (per para 3.5.1). **(T-1).**

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

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

2.9.4.2. In coordination with the installation’s Comm/Cyber unit, install a control systems network enclave (see para 3.4) when requested at the installation-level (only control systems to be entered into Information Technology Investment Portfolio Suite (ITIPS) are hybrid systems). **(T-1).**

2.9.4.3. In coordination with the installation’s Civil Engineer unit, ISO, 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). **(T-1).**

2.9.5. 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). **(T-1).**

**2.10. 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 shall ensure:

2.10.1. An Information System Owner (ISO) is appointed for installation-level control systems per AFI 17-101 para 1.2.5, since control systems are not centrally managed. **(T-2).**

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

2.10.1.2. Provide AFCEC/COO the names of current control system ISO(s) (see para 2.8.1) and Information Security System Manager(s) (ISSM) (see para 2.9.8). **(T-3).**

2.10.2. 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. (refer to paras 3.2.2, 3.3., 3.6-3.12, and 4.1-4.6). **(T-1)**.

2.10.3. 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)**.

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

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

2.10.6. 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)**.

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

## **2.11. Information System Owner (ISO).**

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

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

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

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

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

2.11.6. 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)**.

2.11.7. Facilitate RMF, CE network enclave deployment, and system migration activities at the installation-level for control systems as outlined in para 2.8.3. **(T-2)**.

2.10.8. Appoint an ISSM at the installation for control systems to support and assist the ISO per IAW DoDI 8510.01 **(T-0)** for the program office and ensure the ISSM is certified IAW AFMAN 17-1303. **(T-1)**.

2.11.9. Ensure the Control System Program Report (CPR) is reviewed monthly, and document corrective actions taken. **(T-1)**.

2.11.10. Meet with the ISSM (and ISSO) at regular interval 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 Manager (ISSM).**

2.12.1. Appointed per para 2.10.8, and ensure the ISSM responsibilities are satisfied for

---

<sup>6</sup> There is not currently nor is there intended to be a centralized program management office (PMO/PEO/PO) for control systems in the Department of the Air Force; in turn, "those Program Manager duties specified in AFI 17-101, Para 3.10.2 cannot be fulfilled."



CE-owned control systems per AFI 17-101 para 3.12. **(T-1).**

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

2.12.3. Perform RMF activities: process entries into Enterprise Mission Assurance Support Service (eMASS), perform the CE unit's continuous monitoring program, and accomplish and track mitigations of identified vulnerabilities in RMF Plans of Actions and Milestones (POA&Ms). **(T-1).**

2.12.4. Meet with the ISO (and ISSO) at regular interval 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).**

### **2.13. Information System Security Officer (ISSO).**

2.13.1. Ensure the ISSO responsibilities are satisfied for CE-owned control systems per AFI 17-101 para 3.13. **(T-3).**

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

### **2.14. User Representative (UR) / System Operator.**

2.14.1. Ensures the UR responsibilities are satisfied for CE-owned control systems per AFI 17-101 para 3.16.<sup>7</sup> **(T-3).**

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

**2.15. 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).**

**2.16. 16th Air force.** Develops and implements appropriate activities to monitor and report on the occurrence of cybersecurity 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).**

**2.17. A3 Mission Assurance.** Facilitate the coordination and collaboration of AF Mission Assurance (MA), utilizing the MA Construct to identify, assess, and manage cyber-related risks that endanger strategic mission execution.

2.17.1 Synchronize AF/A4CS, Systems & Data Division with appropriate level of AF MA forum.

2.17.2. Collaborate with AF/A4CS to ensure an inventory of all hardware, software, and related control systems task critical assets (TCA) are reflected in MRT-C mapping. **(T-1).**

**2.18. AF/A2/6.** Identifies the capability and intent of specific threats to cause loss or damage to Defense Critical Infrastructure (DCI) and assess the likelihood that such threats will be carried out. **(T-1).**

---

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

2.18.1. Makes intelligence-based indications and warning information related to DCI available. **(T-1).**

2.18.2. Identifies counterintelligence and security measures to mitigate risks and protect DCI. **(T-1).**

## Chapter 3

### CYBERSECURITY IMPLEMENTATION

**3.1. Control Systems Inventory.** Civil Engineer units shall annually 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.

3.1.1. Use of the AFCEC/COO provided inventory template and process (located on CE Dash) is required and all applicable fields must be appropriately completed (see para 2.8.5). **(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)*<sup>8</sup> 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 shall document any new systems or system modifications and configuration changes (per para 3.9), including but not limited to: 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 shall 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, prioritize, and document those control systems deemed critical for mission(s) execution<sup>9</sup> (e.g., directly, or indirectly enable Task Critical Assets (TCA), weapons systems, Mission Essential Functions (MEF), or locally identified critical missions on base).<sup>10</sup> 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 of defined National Security System (NSS) criteria it is considered an NSS. 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.)* DoD enclaves intended to support Facility Related Control Systems are considered NSS IAW EO 14028, DoDI 5200.44 and CJCSI 6211.02D. **(T-1)**.

**3.1.5. Real Property Designation.** CE control systems<sup>11</sup> 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 Real Property Category Code (CATCODE) Book (<https://usaf.dps.mil/teams/10758/citcatcode/module/home.aspx>). For more information on

---

<sup>8</sup> Reference Figure E-1 (pg. 45), UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*.

<sup>9</sup> Further guidance specific to CE control systems deemed "critical" to mission is forthcoming.

<sup>10</sup> Refer to *Defense Critical Infrastructure (DCI) Line of Effort (LOE) Security Classification Guide (SCG)* (27 Jul 2018) and forthcoming *Classification Guide for Control Systems (CS)* for guidance on security classification of such information.

<sup>11</sup> Note that some CE control systems (e.g., automatic door-locks) do not qualify as RPIE.

RPIE, refer to DAFI 32-9005.

3.1.5.1. If a control system is not found in the CATCODE Book or if unsure of RPIE designation, submit a request to [AFCEC.CIT-.A@us.af.mil](mailto:AFCEC.CIT-.A@us.af.mil).

### **3.2. Mitigating Identified Vulnerabilities & Accepting Risk.**

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

3.2.1.1. Civil Engineer units are required to follow RMF and fulfill ATO requirements for authorization of control systems (outlined in para 2.8.3.1 and DAF RMF policy, AFI 17-101). **(T-0)**.

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

3.2.1.3. All newly initiated authorization packages (e.g., ATO, IATT, DATO, ATC, etc.) for control systems shall be aligned with RMF, as outlined in para 2.7.8.1. **(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 should execute additional controls based on emerging adversarial threats and DAF mission requirements. **(T-3)**.

3.2.1.5. Control systems determined to be NSS (refer to para 3.1.4) shall have a default RMF categorization of M-M-M (Moderate-Moderate-Moderate) for Availability, Integrity, and Confidentiality. **(T-2)**. 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. **(T-2)**.

3.2.1.6. Shall comply with all requirements in DoDI 8510.01 *Risk Management Framework for DoD Systems*. **(T-2)**.

3.2.1.7. For RMF continuous monitoring, verification of security controls, and RMF authorization packages, in accordance with 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. 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. *to include all cybersecurity assessments sponsored by government agencies*)) and determine the applicability to installation’s hardware and software inventories and discover associated risks to the control system. Develop a local plan to correct the vulnerabilities identified. Additionally, utilize the Vulnerability Exploitability Exchange (VEX) to communicate whether a product is affected by a vulnerability and enable prioritized vulnerability response **(T-3)**.

3.2.2.1.1. Reference vendor recommended mitigations, where feasible. **(T-3)**.

3.2.2.1.2. To self-assess cyber risks to CE-owned control systems, follow the process in RAND’s *Assessing Cybersecurity Risk to CE Infrastructure* (pgs. 11-22) (<https://www.milsuite.mil/book/docs/DOC-1024779>). **(T-3)**.

3.2.2.2. Capture all identified vulnerabilities and their associated risks in the control

system's authorization package and associated POA&M (refer to para 3.2.1). **(T-2).**

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

3.2.2.4. Shall use PE 27478F for FRCS hardware / software replacement and cyber training activities to include facility servers, workstations, computers, laptops, tablets. Reference FY23 IMSC Execution Plan Guidance and CE IT Investment Matrix for details. **(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 in accordance with this DAFGM. **(T-3).** The local CE control systems ISO shall review and validate requirements from a control systems cybersecurity perspective prior to contract award. CE units should reference the requirements outlined in the *Control Systems Cyber Defense Reference Architecture (CSCRDA)* when designing control system and network environments, writing contracts, etc. **(T-3).**

3.3.1.1. For any new acquisition or replacement of control systems or their associated devices at a *Level 2 - Field Control System (IP)* of the Purdue Model or above (as defined by UFC 4-010-06), consult AFCEC/COO for design reviews, proposals, quotes, statements of work, etc. **(T-3).**

3.3.2. Performance Contracts (ESPC), Utility Energy Service Contracts (UESC), microgrids, Environmental Security Technology Certification Programs (ESTCP), Advanced Meter Reading Systems (AMRS), etc.) shall follow existing standards and policies to incorporate cybersecurity and associated costs into all phases of delivery. These phases include contract language<sup>12</sup>, 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, UFC 4-010-06, *AF/A4CF Business Rules for MILCON Program Packages and Preparing the DD Form 1391 & 1390* para 9.1.1.3, NIST SP 800-82r2, NIST SP 800-53r5, and the best practices from the Department of Homeland Security (DHS)'s Cyber Security Procurement Language for Control Systems ([https://www.us-cert.gov/sites/default/files/documents/Procurement\\_Language\\_Rev4\\_100809\\_S508C.pdf](https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf)).

3.3.3. Ensure contract language requires newly acquired and/or substantially upgraded control systems to use open protocols and standards to maximize data interoperability in accordance with UFC 3-410-02, *Direct Digital Control for HVAC and Other Building Control Systems*, and in alignment with industry best practices. **(T-0).** In order to prevent the government from being locked into a single vendor solution, the acquisition of proprietary systems, protocols, and standards is prohibited. **(T-2).**

3.3.4 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. Ensure contract language requires data interconnectivity capability for secure

---

<sup>12</sup> 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.

communication protocols (e.g., SSH, File Transfer Protocol (SFTP,) etc.). **(T-1).**

3.3.6. 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. Ensure contract language requires the use of government-owned assets (or government furnished equipment (GFE)) (e.g., computer, tablet) for control systems maintenance. **(T-0).**

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

3.3.9. 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 3.10.6. **(T-3).**

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

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

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

3.3.15.2. 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).**

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

3.3.15.4. Provide sufficient documentation (refer to AFI 17-101 para 4.3.8) for the DAF to finalize the authorization of the control system (refer to para 3.2). **(T-3).**

3.3.15.5. When appropriate, plan to utilize the existing CE control systems network enclave (refer to paras 3.4.2 and 3.4.4). **(T-1).**

3.3.16. Add newly installed or acquired control systems to the installation's inventory (para 3.1). **(T-0).**

3.3.17. Additionally, Utilities Privatization contracts shall include the DFARS 252.204-7012 clause and follow standards specified in NIST SP 800-171r1, 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)**.

3.3.18. For energy projects, 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)**.

3.3.19. Reference the Control Systems Cyber Defense Reference Architecture (CSCDRA) section 5 “Requirements” for more information.

**3.4. Connectivity.** Control systems rely on multiple forms of connectivity for uninterrupted operation of the system. For instance, many control systems rely on the Air Force Information Network, its inherited enterprise services, and a variety of other forms of connectivity for uninterrupted operation of the system. CE units shall aim to consolidate all control systems into a single connectivity architecture. **(T-1)**. Recognizing the disparate system requirements and connectivity landscape, adhere to the tiered approach outlined in this paragraph. All control systems not in the current state (para 3.4.1), protected by a control systems network enclave (para 3.4.2), or approved through exemption (para 3.4.3) are subject to disconnection from the network.

#### **3.4.1. Current State.**

3.4.1.1. Until AFCEC/COO installs a control systems network enclave (para 3.4.2) at the installation, the Civil Engineer unit will monitor their systems’ security controls. **(T-3)**. To prepare for the network enclave deployment and the migration of control systems into the enclave, all control systems shall go through the “assess only” or “assess and authorize” process (see para 3.2). **(T-3)**.

3.4.1.2. Once the network enclave is deployed at the installation, follow the policy stated in paras 3.4.2 and 3.4.4. **(T-1)**.

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

**3.4.2. Network Enclave.** In a prioritized manner (based on mission(s) criticality and dependencies of control systems), and in coordination with the local Comm/Cyber unit, AFCEC/COO shall deploy installation-level control systems network enclaves. Through the SAF/CN-appointed authorization boundary, the Civil Engineers have designed type-authorized, AO-sanctioned control systems network enclaves. These enclaves logically segregate control systems on the Air Force Information Network to provide secure access to enterprise services and a defensible and monitored network environment for control systems to operate. **(T-1)**.

3.4.2.1. Leverage existing base Comm infrastructure for the deployment of the network enclave (see para 3.4.3 for exceptions). **(T-1)**.

3.4.2.2. If a control systems network enclave has been deployed to an installation:

3.4.2.2.1. AO-approved control systems (see para 3.2) shall (1) be segmented from all other connectivity and (2) be migrated into the control system network enclave under direction of the ISO (see para 2.9.7) in coordination with the

installation's Comm/Cyber unit, AFCEC/COO, and system vendor. (T-2).

3.4.2.2.2. The Civil Engineer unit, specifically the ISO, ISSM, and ISSO (paras 2.9 - 2.11), shall continue to monitor their systems' security controls. (T-3).

3.4.2.3. If a control systems network enclave has not been deployed to an installation, adhere to the policy outlined in para 3.4.1. (T-1).

**3.4.3. Exceptions.** If there is a need to have a different form of connectivity other than the control systems network enclave (para 3.4.2) due to the function of the system or mission criticality concerns, the owner shall submit a justification to AFCEC/COO for AO approval. (T-2). An exception may also be directed at the AO's discretion. Additionally, follow the criteria listed below:

**3.4.3.1. Stand-alone systems.** Stand-alone systems (refer to "stand-alone" definition in Attachment 1) are those that do not interface with nor connect to other systems/networks. A system could remain stand-alone due to (1) mission criticality concerns, (2) existing vulnerabilities that cannot be mitigated, or (3) if the control system is a Life Safety system (para 1.2.3) or a system that is determined not technically feasible to migrate into the CE control systems network enclave.

3.4.3.1.1. Provide security, system administration, and authorization for stand-alone systems per DoDI 8510.01 and AFI 17-101. (T-3).

3.4.3.1.2. Implement a RMF continuous monitoring strategy for the system's security controls, as outlined in para 3.5.1, as part of the authorization requirement. (T-3).

**3.4.3.2. Stand-alone networks.** Where stand-alone network architecture is approved for control systems, DAF CIO requirements for network security, security protections, and Defensive Cyber Operations (DCO) continuous monitoring (refer to para 3.5.2) shall still be provided by the installation's stand-alone network design and the network administrator. (T-1).

**3.4.3.3. Modems.** Remove uncontrolled public access to dial-up modems. Modem connections to the AFIN require DAF Enterprise AO (ACC/A6) approval and an Approval to Connect (ATC) per AFI 17-101. Modem connections to any other network or network enclave require approval by the owning AO. (T-1).

**3.4.3.4. Wireless Communications/Radio Frequency (e.g., Wi-Fi, cellular, Bluetooth, satellite).** Using unlicensed frequencies under Federal Communications Commission Title 47 Part 15 is not allowed. (T-0). Do not procure new control systems using a Part 15 radio frequency device. (T-0). OCONUS installations shall also comply with applicable Host Nation rules, laws, policies, and agreements. (T-0). Verify radio frequency spectrum certification compliance with the installation's 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).

3.4.3.4.1. A wired infrastructure is more secure than one that uses wireless technologies, therefore convert radio frequency networks to wired or fiber where possible. 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 owned by the



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).**

3.4.3.4.2. 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 Modules*, Overall Level 1 or Level 2, as dictated by the data's sensitivity. **(T-1).**

3.4.3.4.3. Any data transmitted by Wi-Fi devices, services, and technologies shall follow IEEE Standard 802.11-2016 per DoD Directive (DoDD) 8100.02, DoDI 8420.01 and DHS's *Guide to Securing Networks for Wi-Fi* ([https://www.us-cert.gov/sites/default/files/publications/A\\_Guide\\_to\\_Securing\\_Networks\\_for\\_Wi-Fi.pdf](https://www.us-cert.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf)). **(T-0).**

3.4.3.4.4. Authorization will not be granted for control systems using Bluetooth. **(T-2).**

3.4.3.4.5. For all other use of radio frequency, approval is required before the purchase, testing, deployment, and usage of the system. **(T-3).**

**3.4.3.5. Commercial Internet & Services.** Control system devices should be configured to only utilize private IP addresses. All commercial Internet connections are prohibited unless approved by the AO and the DoD Chief Information Officer has granted a DoD Information Network (DoDIN) waiver. **(T-0).** Unauthorized connections will result in a Denial of Authorization to Operate (DATO).

**3.4.3.5.1. DoDIN Waiver Process.** Under DoDI 8010.01 para 4.4 and Air Force Manual (AFMAN) 17-2101 para 3.1.1, the DoD Chief Information Officer 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 [osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil](mailto:osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil).

**3.4.4. Unnecessary Connectivity.** Any form of connectivity or communication protocol that is not used, not necessary for the function of the system, and not explicitly approved shall be disabled in all components of the control system down to the end device. **(T-1).**

**3.4.5. Encryption.** Apply secure authentication and encryption protocols for data in transit and utilize encryption for data at rest and data in use (see para. 4.5.1) 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 “*CE FRCS Baseline Security Controls*” memorandum). For instance, CE units shall 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 package 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.

**3.5.2. DCO Continuous Monitoring.** 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 cyber defenders (e.g., 16 AF/AFCYBER or for incident detection and response of control systems, as well as for a Cybersecurity Service Provider (CSSP)), as well as an operations watch floor for automated continuous monitoring of control systems at the base and enterprise-level.

3.5.2.1. In lieu of established command and control (C2), DCO continuous monitoring, and/or CSSP entity, if an incident occurs (that could have been caused by a malicious cyber event, but needs investigation to determine), request assistance through the local Comm/Cyber unit to coordinate "9-Line" submission or other appropriate escalation/response. (T-1).

### 3.6. Hardware.

**3.6.1. Hubs.** The use of hubs is prohibited. (T-2). Where used in legacy systems, plan and program for their replacement to managed switches (para 3.6.2) utilizing the *DISA Approved Products List* (<https://aplits.disa.mil/apl/>) and AFCEC/COO for further guidance. (T-3).

**3.6.2. Switches.** All control systems are mandated to use managed switches. Use of switches within the control systems environment shall be kept to a minimum. (T-3). If used, configure switches to restrict port access to the control system. (T-3). Switches shall have physical (refer to para 4.4) and logical security measures. (T-3). Ensure switches are stored in a locked, secure area/cabinet, and add necessary tamper-proof features to restrict access to these devices. (T-3). 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.** Rack mounted servers are preferred over towers or stand-alone cases. Use of specific software and hardware identified in current contract vehicle, is required for servers and client workstations. (T-1).

3.6.4. Work with vendors to determine appropriate security settings for all control systems 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. Control system networks that utilize virtual machines must meet proper cybersecurity controls. Reference NIST SP 800-125B. (T-3).

3.6.7. All unused hardware shall be disconnected and properly stored (see para 4.5.3). (T-

3).

### 3.7. Software.

3.7.1. Use whitelisting software 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. **(T-0)**. Adhere to para 3.8 and the following:

3.7.2.1. 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 Standard Desktop Configuration SharePoint site (<https://usaf.dps.mil/sites/41288/SDC/SitePages/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.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 as stated in UFGS-25 05 11 para 1.9.2. **(T-0)**.

3.7.4.1. 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. Ensure that unused ports, protocols, and services remain disabled. **(T-0)**.

3.7.4.3 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. Use tamper-evident seals to cover disabled ports. **(T-3)**.

3.7.4.6. 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)**.

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

3.7.4.8. 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) 33A-1109* for guidance.

3.8.2. Systems shall be 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. Establish a configuration baseline for each control system and its associated components and devices. (T-3).

3.9.2 Ensure necessary changes to a control system are identified, authorized, and thoroughly documented. (T-3).

3.9.3. 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. A change request process shall 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. 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. 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. 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. 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 shall 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. 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 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. For existing contracts that do not allow maintenance using government-owned assets (or GFE) and until contract language is updated (see para 3.3.7), ensure assets used by vendors and service personnel are thoroughly scanned for viruses and malware in coordination with local Comm/Cyber unit procedures and contracting officer before the asset is allowed to connect to a control system or related infrastructure, as stated in NIST SP 800-46r2 (paras 2.1 and 5.4), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. **(T-3)**.

3.10.8. Further on-site maintenance requirements can be found in NIST SP 800-82r2.

**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. 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. 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. (T-3).

3.11.4. 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 800-82r2, 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. Other remote maintenance on the control system not meeting these specifications is prohibited. (T-2).

**3.12. Solid State Devices and Removable Media.** As recommended by NIST SP 800-82r2, removable media is not to be connected to a control system and associated forms of connectivity or control systems 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 AFMAN 17-130. (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 shall be scanned for viruses, malware, etc. before connecting to a control system. (T-1). Track and document vendor connection points, connection duration, and maintenance performed.

**3.13. Privately-Owned Devices.** The use of privately-owned devices (i.e., not owned, provided, or approved by the government) to access, monitor, or operate control systems is not authorized. (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. Contact the AFCEC Reach back Center at (850) 283-6995 or by e-mail at [afcec.rbc@us.af.mil](mailto:afcec.rbc@us.af.mil).

3.14.2. 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.

3.14.2.1. For technical support regarding control systems network enclave, control systems design reviews, inventory, RMF, or eMASS, contact 850-775-3200, or by e-mail at [afcec.comi.icshelpdesk@us.af.mil](mailto:afcec.comi.icshelpdesk@us.af.mil).

3.14.3. For questions regarding CE's overall strategy and this DAFGM, contact [AF.A4CSOWorkflow@us.af.mil](mailto:AF.A4CSOWorkflow@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. Ensure system operators use and maintain control systems in accordance with manuals and technical specifications provided by the vendor. **(T-3)**.

#### **4.3. Authentication/User Account Management.**

4.3.1. Ensure all personnel are educated on their responsibility for password/account protection. **(T-3)**.

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

4.3.1.2 All personnel shall have a unique account configured based on required roles and responsibilities adhering to the principles of least privilege. **(T-3)**.

4.3.2. 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)**.

4.3.3 Review control system audit logs for unauthorized attempts or indicators of compromise. **(T-3)**.

4.3.4. Do not share passwords. **(T-3)**. In the event of a compromised password, change the password immediately. **(T-3)**.

4.3.5. Review 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)**.

4.3.6. 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)**.

4.3.7. 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)**.

4.3.8. 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.

4.3.9. Per DAFMAN 17-1304, “Identity and Credential Access Management (ICAM)”,

section 3.2.2.3, Systems 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)**.

4.3.9.1 Any system or organization that is unable to use an approved DoD authenticator (e.g., CAC) shall contact ACC HQ CCC/CYX ICAM (acc.cyss.cyz.pki@us.af.mil) and AF PKI SPO (AFPKI.Helpdesk@us.af.mil) for further guidance. **(T-3)**.

4.3.9.2 Privileged user management shall adhere to DAFMAN 17-1304, Section 5.4. **(T-3)**.

#### **4.4. Physical Access Control.**

4.4.1. Store computers and interfaces that support control systems in a secure space, where physical access can be monitored and restricted to only those who require it. **(T-3)**.

4.4.2. 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. **(T-3)**.

4.4.3 Maintain positive key control by establishing policies and procedures. Ensure keys are not stored with currently used locks and panels are locked when not in use.

4.4.4. Document who has control over control systems equipment locations (e.g., electrical, mechanical, communications rooms). **(T-3)**.

4.4.5. 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)**.

#### **4.5. Data Storage and Disposal.**

4.5.1. 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)**.

4.5.2. 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)**.

4.5.3. When a control system is no longer required, the ISO shall take appropriate action to ensure the system and its data is properly disposed per established procedures detailed in NIST SP 800-53r5 para 3.11 MP-6, NIST SP 800-82r2 para 6.2.10, and AFMAN 17-1301 chapter 5. **(T-3)**.

#### **4.6. Response, Recovery, and Contingency Plans.**

4.6.1. 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)**.

4.6.2. Ensure response plans (Incident Response/Business Continuity), recovery plans (Incident Recovery/Disaster Recovery), and contingency plans are in place and managed per NIST SP 800-82r2 para 6.2.6 and 6.2.8. **(T-1)**. Develop Response, Recovery, and



Contingency plans if they do not currently exist. **(T-1).**

4.6.3. Plans shall contain POCs lists, clear roles and responsibilities, specific tactics, techniques, and procedures for when adversarial activity 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 disconnecting all Internet connections, running a properly scoped search for malware, disabling affected user accounts, isolating suspect systems, and an immediate 100 percent password reset (refer to para 4.3). 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://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS\\_Rev\\_2\\_\(Final\).pdf](https://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS_Rev_2_(Final).pdf)) for examples of applicable procedures to be considered to use for tailoring to installation-specific conditions.

4.6.4. Ensure plans are tested, reviewed annually at a minimum and updated as necessary. **(T-2).**

4.6.5. Have a 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).**

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

**4.7. 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](https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf)). **(T-3).**

4.8. Register at DHS CISA (<https://us-cert.cisa.gov/ mailing-lists-and-feeds>) to receive security alerts, analysis reports, tips, and other updates. **(T-3).**

4.9. View control systems Alerts and Advisories from CISA (<https://us-cert.cisa.gov/ics>).

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

*HAF AF/A4CF Business Rules for MILCON Program Packages and Preparing the DD Form 1391 & 1390*, 30 December 2019

AFI 17-201, *Command and Control (C2) for Cyberspace Operations*, 05 March 2014 (or referenced as AFI 10-1701)

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 10 June 2022

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

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 12 February 2020

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

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

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

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

*Civil Engineer (CE) Facility Related Control Systems (FRCS) Baseline Security Controls*, 10 September 2018

CISA Registration for security alerts, tips, and notices, <https://us-cert.cisa.gov/mailing-lists-and-feeds>

CISA Alerts and Advisories for Control Systems, <https://us-cert.cisa.gov/ics>

CJCS Instruction 6211.02D *Defense Information Systems Network (DISN) Responsibilities*, 04 August 2015

CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*, 29 July 2022

CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*, 02 March 2022

*Control Systems Cyber Defense Reference Architecture (CSCDRA)*, February 2022

DAF Ports, Protocols, and Services Site, <https://usaf.dps.mil/teams/IACE/Wiki/AF%20PPS.aspx>

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

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

DAFI 90-160, *Publications and Forms Management*, 1 April 2022

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

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

*DAF Civil Engineer (CE) Facility Related Control Systems (FRCS) Baseline Security Controls*, September 2018

Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204.7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, December 2019

Deputy Secretary of Defense memorandum *Enhancing Cybersecurity Risk Management for Control Systems Supporting DoD-Owned Defense Critical Infrastructure*, 19 July 2018

DHS's *Configuring and Managing Remote Access for Industrial Control Systems*, [https://www.us-cert.gov/sites/default/files/recommended\\_practices/RP\\_Managing\\_Remote\\_Access\\_S508NC.pdf](https://www.us-cert.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf), November 2010

DHS's *Cyber Security Procurement Language for Control Systems*, [https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement\\_Language\\_Rev4\\_100809\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf), September 2009

DHS's *Guide to Securing Networks for Wi-Fi* (IEEE 802.11 Family), [https://us-cert.cisa.gov/sites/default/files/publications/A\\_Guide\\_to\\_Securing\\_Networks\\_for\\_Wi-Fi.pdf](https://us-cert.cisa.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf), 15 March 2017

DISA's DoD Information Network Approved Products List, <https://aplits.disa.mil/apl/>  
DoD's *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)* (Revision 2), [https://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS\\_Rev\\_2\\_\(Final\).pdf](https://www.acq.osd.mil/eie/Downloads/IE/ACI%20TTP%20for%20DoD%20ICS_Rev_2_(Final).pdf), March 2018

DoD CIO Memo – *Controls Systems Cybersecurity* 18 December 2018

DoD 8140.01 *Cyberspace Workforce Management* 5 October 2020

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

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Network (GIG)*, 23 April 2007

DoDI 4165.14, *Real Property Inventory (RPI) and Forecasting*, 31 August 2018

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

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, 15 October 2018

DoDI 8010, *Department of Defense Information Network (DODIN) Transport*, 10 September 2018

DoDI 8420.01, *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*, 03 November 2017

DoDI 8500.01, *Cybersecurity*, 07 October 2019

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Systems*, 09 July 2022

DoDI 8520.03, *Identity Authentication for Information Systems*, 27 July 2017

DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*, 25 July 2017

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

Federal Communications Commission Title 47 Part 15, *Radio Frequency Devices*, <https://www.ecfr.gov/cgi-bin/text-idx?SID=c53bfc176746794ec4b0086b86350d54&mc=true&node=pt47.1.15&rgn=div5>, updated 26 Aug 2022

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

IEEE Standard 802.11-2016, <https://standards.ieee.org/findstds/standard/802.11-2016.html>, 26 February 2021

JP 1-02, *DoD Dictionary of Military and Associated Terms*, January 2020

National Telecommunications and Information Administration *Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)*, <https://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook>, January 2021

NIST SP 800-37r2, *Risk Management Framework for Information Systems and Organizations*, December 2018

NIST SP 800-39, *Managing Information Security Risk*, March 2011

NIST SP 800-40r4, *Guide to Enterprise Patch Management Technologies*, 6 April 2022

NIST SP 800-46r2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 2016

NIST SP 800-53r5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (updated December 2020)

NIST SP 800-82r2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

NIST SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*, 07 March 2016

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, 10 October 2019

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

NIST SP 800-171r1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, 02 February 2018

NSA's *Guidelines for Application Whitelisting Industrial Control Systems*, [Guidelines for Application Whitelisting in Industrial Control Systems \(cisa.gov\)](#) 01 April 2016

National Security Memorandum 8, Task 5: *Identification and Inventorying of National Security Systems Guidance* (NMM-2022-05)

OMB Circular A-130, *Managing Information as a Strategic Resource*, 28 July 2016

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, 17 October 2001

OUSD (A&S) memorandum, *Supplemental Guidance for the Utilities Privatization Program*, 07 February 2019

OUSD (A&S) memorandum, *Interim Defense Federal Acquisition Regulation Supplement Rule, 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements*, Nov 2020.

RAND's *Assessing Cybersecurity Risk to CE Infrastructure*, <https://www.milsuite.mil/book/docs/DOC-1024779>, January 2019

RMF Knowledge Service Portal, <https://rmfks.osd.mil/rmf/Pages/default.aspx>

Standard Desktop Configuration SharePoint site, <https://usaf.dps.mil/sites/41288/SDC/SitePages/Home.aspx>

Title 40 U.S.C. § 11101, *Public Buildings, Property, and Works (Information Technology Management – General – Definitions)*, 14 January 2019

Title 42 U.S.C. § 5195c(e), *The Public Health and Welfare (Disaster Relief – Emergency*

*Preparedness – Critical Infrastructure Protection*), 14 January 2019

Title 44 U.S.C. § 3552, *Public Printing and Documents (Coordination of Federal Information Policy, Information Security, Definitions)*, 14 January 2019

UFC 3-410-02, *Direct Digital Control for HVAC and Other Building Control Systems*, 12 April 2021

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*, 18 January 2017

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

### ***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

**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

**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

**NIST SP** — National Institute of Standards and Technology Special Publication

**NSA** — National Security Agency

**NSS** – National Security System

**OMB** — Office of Management and Budget

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

**OT** — Operational Technology

**RMF** — Risk Management Framework

**SAF/CN** — 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

### *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 800-82r2).

**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).

**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).

**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 to 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 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).