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

AFGM2017-32-01

2 February 2017

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: AF/A4C
1800 Air Force Pentagon
Washington DC 20330-1800

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

ACCESSIBILITY: Publication is available for downloading on the e-Publishing web site at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum (AFGM) immediately establishes cybersecurity policy for civil engineer (CE)-owned or operated control systems (CS). This Memorandum details the unique operational characteristics of Air Force (AF) CS, outlines roles and responsibilities for managing risk under the Risk Management Framework, and implements guidance and policy for securing and mitigating risk to AF CE CS.

This Guidance Memorandum supersedes *Engineering Technical Letter 11-1* and applies to all military and civilian Air Force personnel, the Air Force Reserve and the Air National Guard. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force (AF) publications, the information herein prevails, IAW AFI 33-360, *Publications and Forms Management*.

Ensure all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). This Memorandum becomes void after one year from the date of this Memorandum, or upon the publication of a new Instruction permanently establishing this guidance, whichever is earlier.

JOHN B. COOPER, Lieutenant General, USAF
DCS/Logistics, Engineering & Force Protection

2 Attachments:
1. Control Systems Background
2. Cybersecurity Policy for Civil Engineer Control Systems

Attachment 1

CONTROL SYSTEMS BACKGROUND

A1.1. Control Systems Overview.

A1.1.1. Control systems are integrated hardware and software designed to monitor, or monitor and control, the operation of equipment, infrastructure, or associated devices. Control systems consist of a combination of technology (computers, human-machine interfaces (HMI)) and control components (electrical switches, mechanical actuators, environmental sensors) that act together upon underlying mechanical or electrical equipment to achieve a physical objective (the transport of matter or energy, control of a dynamic process, or maintenance of a secure and comfortable work environment, etc.) Generally, these special-purpose systems regulate the flow of electricity, fluids, gases, air, traffic, and even people.

CS are comprised of several sub-groups of systems including building automation systems and industrial control systems (ICS). Various categories of ICS include supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLC), intelligent HMI modules, and other dedicated CS configurations often found in the industrial sector and support critical infrastructure.

A1.1.1.1. SCADA systems are highly distributed systems used to monitor and control geographically-dispersed assets where centralized data acquisition, control, and status reporting are critical to system operation. SCADA systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

A1.1.1.2. DCS are used to control industrial processes such as electrical power generation, oil refineries, water/wastewater treatment, manufacturing production, and materiel distribution. DCS are integrated control architectures that provide supervisory-level control and integration over subsystems responsible for local process control.

A1.1.1.3. PLC are proprietary processor-based, solid-state devices found in almost all industrial equipment and processes to provide logic algorithms for connected input and output devices. They can vary in sophistication from simple, stand-alone microcontrollers to sophisticated, multi-processor controllers that provide advanced motion control, network capability, error detection, diagnostics, process recovery, and fail-safe redundancy. While PLC are components of DCS and SCADA systems, they are often the solitary control device for smaller CS configurations used to provide operational control of separate processes.

A1.1.1.4. A list of AF CE-owned CS can be referred to in section A1.2.

A1.1.2. Throughout the Air Force, CS are typically used to monitor and/or control electricity; facility heating, ventilation, and air conditioning (HVAC); interior and exterior lighting; water and wastewater; natural gas distribution; certain intrusion detection systems and fire/life safety systems (such as fire alarm reporting systems and fire suppression systems). CS are a critical part of automation and are used extensively to optimize resources supporting nearly all aspects of Air Force core mission areas.

A1.1.3. Historically, CE CS were neither automated nor networked. Devices used for monitoring or control had no computing resources, and those that were digitized typically used proprietary protocols and PLCs rather than full computer control. As controllers became interconnected, they were not designed with traditional IT system and security considerations, as they were expected to operate as isolated systems running on their own dedicated network with proprietary communication protocols and specialized hardware and software. This intentional separation from AF-wide traditional IT (e.g., e-mail, web access, networked printing, or remote access) allowed CS to be easily connected, open and accessible, highly stable, and readily serviced.

Today, however, CS are designed using standard platforms, operating systems, network protocols, and access controls commonly found in traditional IT systems. The ever-increasing connectedness of CS allows for greater operational capabilities, efficiencies, and automation. However, this integration also introduces new vulnerabilities that expose both the CS and the underlying network to threats.

A1.1.4. Special precautions must be taken when introducing IT security controls and solutions to CS environments because of the unique ways CS communicate and operate. Interconnections between CS and organizational networks/business systems are a particular point of focus for security and should be carefully considered. In all cases, security solutions must be tailored to the specific CS environment and verified to ensure their impact to the CS is not detrimental to a CS’s operation.

A1.1.5. CS can have long life spans (often exceeding 20 years) and can be comprised of technology that suffers rapid obsolescence. This longevity introduces several issues. Most importantly, older hardware and software may no longer be supported by the manufacturer. Companies can go out of business or terminate their support for an installed product. Because of this, patches and forward support for compatibility with new operating systems may no longer be available as new vulnerabilities are discovered.

A1.1.6. In the traditional IT domain, where data is the preeminent priority, cyber defenders often focus on preventing the disclosure of information to unauthorized individuals or processes. Consequently, confidentiality tends to be the most important attribute among the three properties of the confidentiality – integrity – availability (CIA) triad. However, with CS, it is paramount to actively manage or monitor physical processes and maintain high availability and positive control of the system. Therefore, availability and integrity of the CS take precedent over confidentiality. It is this difference in cybersecurity priorities that impacts what security controls and procedures are appropriate to implement for CS compared with those of traditional IT.

A1.1.7. The goal of securing CS components is to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the CS as much as possible. Therefore, security controls such as intrusion detection software, antivirus software and file integrity checking software should be utilized to the fullest extent technically feasible. However, it is also recognized that CS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT processes. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

A1.1.8. CS and their real-time operating systems are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have desired features including encryption capabilities, error logging, and password protection. Indiscriminate use of IT security practices in CS may cause availability and timing disruptions. There may not be computing resources available on CS components to retrofit these systems with current security capabilities. Adding resources or features may not be possible.

A1.2. Scope. AF CE-owned CS include, but are not limited to, the following types of systems (including all points, devices, control panels, means of connectivity, software, controllers, computer workstations, servers, etc.):

A1.2.1. SCADA Systems
A1.2.1.1. Protective relays (microprocessor-based)
A1.2.1.2. Cathodic protection systems
A1.2.1.3. Natural gas distribution systems
A1.2.1.4. Power generation systems, including renewable systems
A1.2.1.5. Water/wastewater distribution systems
A1.2.1.6. Water/waste treatment systems

A1.2.2. Building Automation Systems (BAS)
A1.2.2.1. Energy Management Control Systems (EMCS)
A1.2.2.2. Advanced Meter Reading Systems (AMRS)
A1.2.2.3. Interior/exterior lighting controls

A1.2.3. Fire/Life Safety systems
A1.2.3.1. Fire Alarm Reporting Systems (FARS)
A1.2.3.2. Fire Suppression Systems (FSS)
A1.2.3.3. Facility Mass Notifications Systems

A1.2.4. Utility Monitoring and Control Systems (UMCS)
A1.2.4.1. Electrical distribution systems
A1.2.4.2. Generator monitoring systems

A1.2.5. Airfield Control Systems
A1.2.5.1. Airfield Lighting Control Systems (ALCS)
A1.2.5.2. Aircraft Arresting Systems (AAS)
A1.2.5.3. Runway Ice Detection Systems (RIDS)
A1.2.5.4. Bird abatement systems
A1.2.5.5. Ramp lighting control systems

A1.2.6. Vehicle Traffic controls
A1.2.6.1. Drop-arm barriers
A1.2.6.2. Pop-up barriers
A1.2.6.3. Traffic signal systems

A1.2.7. CE-maintained Intrusion Detection Systems

Attachment 2

CYBERSECURITY POLICY FOR CIVIL ENGINEER CONTROL SYSTEMS

A2.1. Applicability. Due to the unique nature of CS, there is a need for specific control system guidance and policies to help secure, maintain, and provide mission assurance of the critical infrastructure and missions these systems support.

A CS is considered operational technology (OT), which is IT adapted to directly monitor and/or control physical devices, processes and events where availability is the primary operational concern. Accordingly, OT is more sensitive to the application of cybersecurity measures and controls that can affect its availability. The Authorizing Official (AO) assigned to the CS boundary is responsible for managing the risk for OT and may tailor controls to balance security and availability.

Air Force CE CS consist of OT classified as either Real Property Installed Equipment (RPIE) or Non-RPIE Equipment. Figure 1 represents the elements that comprise CS in addition to OT's affiliation with the Platform IT (PIT) category of Air Force IT, defined further in AFI 17-101. Referencing AFI 17-101, Platforms and Non-RPIE Equipment would generally be classified as types of "PIT Systems" or "PIT Subsystems."

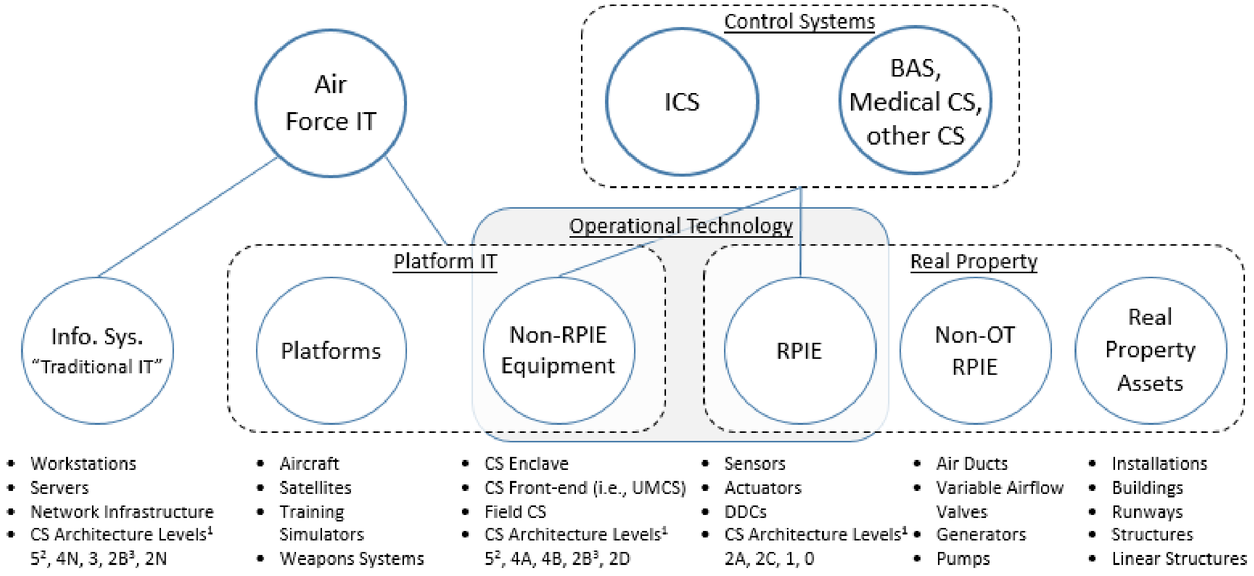

Figure 1: Categorization of AF IT and CS

Attachment 2 outlines some of the defensive cybersecurity policies to be adhered to throughout the life cycle of CS operating on AF installations. These policies are not meant to supersede any established Federal, Department of Defense (DoD) or AF policy, but instead are intended to

[1] From Unified Facilities Criteria 4-010-06, *Cybersecurity of Facility-Related Control Systems*, Appendix E
[2] Equipment in CS Architecture Level 5 is considered Non-RPIE Equipment when installed as part of a CS enclave.
[3] CS Architecture Level 2B is considered an Information System as a Base Area Network (BAN) access switch and Non-RPIE Equipment when part of a CS in Levels 0-2.

supplement existing policy (such as DoDI 8500.01) and DoD's Risk Management Framework (RMF) (outlined in DoDI 8510.01) by providing guidance on security measures.

A2.2. Standard Level of Cybersecurity Service. At a minimum, the standard cybersecurity level of service for base CE organizations is to be compliant with this AFGM for the CE-owned, operated, or managed on-base assets supporting identified Defense Critical Infrastructure (DCI) missions and capabilities. These procedures and guidelines should also be followed in a prioritized manner for the remaining infrastructure under CE's ICS PIT AO boundary (introduced in section A2.4.1).

A2.3. Installations' CS Inventory. Installations will conduct and maintain accurate inventories of all CS under the purview of CE. The installations' CS inventory should provide thorough awareness of existing systems, their interconnections, and their link to the mission or function they serve. For more information on the recommended content and CS inventory specificity, see NIST SP 800-82.

A2.3.1. The CS inventory at installations shall include both hardware (physical devices and systems) and software (communications platforms and applications) down to Topology Tier Level 2 at a minimum. A diagram of CS topology, its associated levels and components are defined and exemplified in Unified Facilities Criteria 4-010-06, *Cybersecurity of Facility-Related Control Systems*, Appendix E.

A2.3.2. The inventory shall include descriptions of CS-supported assets and infrastructure, and whether the CS supports DCI as determined by A3OA or locally-derived mission critical capabilities. Actual names of critical infrastructure, Task Critical Assets (TCA), or Defense Critical Assets (DCA) should not be listed in an unclassified environment. TCA and DCA are defined as part of the Defense Critical Infrastructure Program (DCIP) detailed in DoD Manual 3020.45, Volume 1.

A2.4. Risk Management Framework. The AF CE community shall adhere to the NIST ICS guidelines (NIST SP 800-82), DoD RMF guidance outlined in DoDI 8510.01, and subsequent AF RMF policy (AFI 17-101) to the greatest extent possible in order to sufficiently manage the life cycle cybersecurity risk of CS.

A2.4.1. RMF Roles and Responsibilities. The transition from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to RMF warrants changes in workflow, roles and responsibilities to accompany the shift from compliance-based accreditation to a risk-based approach to securing assets. To comply with RMF, the AF Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) has appointed the Deputy Director of Civil Engineers (A4C-2) as the AO for CE ICS PIT. Upon appointment by the AF Chief Information Security Officer, the Air Force Civil Engineer Center (AFCEC) Operations Directorate Director will be the Security Control Assessor (SCA) for CE ICS PIT.

During the phase-in period to RMF, the role of Information System Security Manger (ISSM) will be temporarily assumed by AFCEC. The roles of the Information System Owner (ISO) and the Program Manager (PM) for CE CS will be performed, in the short-term, by the owning base's Deputy Base Civil Engineer (BCE). Funding for contract support to assume these roles and responsibilities is currently in the process of being approved through the FY18 budgeting process. The specific roles and responsibilities for performing continuous monitoring, as required by RMF, are forthcoming.

See section A2.17 for further details regarding FY18 funding and the transition plan to meet CS cybersecurity protocol expectations.

A2.4.2. Preliminary Baseline Classification. For assistance with determining the Potential Impact Values for the RMF "Step 1 - Categorize System" process, please reference the *EI&E PIT Control System Master List* located on the RMF Knowledge Service portal. The list provides a baseline confidentiality – integrity – availability impact rating for various AF control systems. This baseline rating is considered the minimum impact value for a given system based on its mission criticality.

A2.5. Acquisitions. Because a CS is related to the facility being constructed and tailored to the mission it supports, acquisition and procurement of CS is currently a decentralized process in the AF. Until there is a centralized CS Program Management Office (PMO) able to adequately conduct CS lifecycle management, the CE community needs to collaborate with the Acquisitions community to accurately define security requirements and prioritize CS acquisitions with cybersecurity measures already incorporated into the design of the asset. Additionally, it is recommended to incorporate the best practices from the Department of Homeland Security (DHS)'s *Cyber Security Procurement Language for Control Systems* document into all future procurement and maintenance contracts.

A2.6. Segregated CS Network Environment. The AFCEC Operations Directorate's Civil Engineer Maintenance Inspection Repair Team (CEMIRT) Division will assist Base CE squadrons to establish an accredited CS enclave in order to segregate CS and CS traffic from the base area network (BAN). The enclave configuration will provide a defendable and monitored space protecting both the CS from network vulnerabilities and the network from CS vulnerabilities. CS should be operated either as stand-alone systems (no network connectivity), on an air-gapped network, or on a CS enclave. CS should not be directly connected to the Internet through either static or dial-up connections except as described in sections A2.9 and A2.16.

A2.7. Information Protection and Mission Assurance. A modified list of cybersecurity best practices to follow and frequently review is listed below. Additionally, the technical references listed in section A2.19 provide comprehensive procedures to follow for information protection and mission assurance.

A2.7.1. Apply security techniques such as encryption and/or cryptographic hashes to CS data storage and communications where determined appropriate.

A2.7.2. Frequent backups of CS data should be conducted, maintained, and properly stored. It is recommended to store copies of data and "golden image" configuration backups in a secure location for business continuity and disaster recovery.

A2.7.3. When a CS is no longer required, the ISO should take appropriate action to ensure the system and its data is properly disposed IAW established procedures detailed in NIST SP 800-53r4 and NIST SP 800-82r2.

A2.7.4. Ensure response plans (Incident Response/Business Continuity) and recovery plans (Incident Recovery/Disaster Recovery) are in place and managed IAW NIST SP 800-82.

A2.7.4.1. Response and recovery plans should contain specific tactics, techniques, and procedures (TTP) for when adversarial activity is detected. 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. The plan may also define escalation triggers and actions, including incident response, investigation, and public affairs activities.

See *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures for Department of Defense Industrial Control Systems* for examples of applicable TTPs to be considered for use or tailoring to base-specific conditions.

A2.7.4.2. Response and recovery plans should frequently be tested and reviewed. Personnel should be aware of their roles and responsibilities in case of an incident.

A2.7.4.3. Have a restoration plan in place, including having "gold disks" ready to restore systems to known good states.

A2.8. Access Control.

A2.8.1. Abide by strict access control protocols to prevent unauthorized physical access to all components of the CS (focusing on control nodes) and the unauthorized introduction of new hardware, infrastructure, and communications interfaces where feasible.

A2.8.2. Adhere to strict access control protocols for logical access to systems – limit to authorized users on an as-needed basis with permissions pertinent to the users' role.

A2.8.3. Enforce separate authentication mechanisms and credentials for users of the CS network and the BAN (i.e., CS network accounts do not use BAN user accounts).

A2.9. Connectivity. All non-BAN connectivity to CS (including, but not limited to, dial-up, Internet, Bluetooth, wireless, and cellular) are considered external connections. These connections bring substantial vulnerabilities warranting additional scrutiny and cybersecurity safeguards.

A2.9.1. Any data transmitted by commercial wireless devices, services, and technologies will implement end-to-end data encryption over an assured channel (AC). The security level of data encryption shall be dictated by the sensitivity of the data and validated under the "Cryptographic Module Validation Program," specified in FIPS PUB 140-2. Per DoDD 8100.02, individual exceptions to unclassified wireless encryption may be granted on a case-by-case basis after an operational risk assessment is conducted and approval is granted by the AO.

A2.9.2. CS with dial-up modem connections to the Defense Switched Network (DSN), such as direct subscriber lines (DSL), require AF Enterprise AO approval and ATC prior to use. The DSN is a primary information transfer network for the Defense Information Systems Network (DISN) and provides the worldwide non-secure voice, secure voice, data, facsimile, and video teleconferencing services for the DoD and other Federal agencies. All dial-up modem requests shall be submitted through *eMASS* for CE's ICS PIT AO and the AF Enterprise AO approval. Until approved, all dial-up modem connections are immediately prohibited.

A2.9.3. A DoD Chief Information Officer (CIO) waiver is required before procuring any of the following commercial services: Internet Service Provider (ISP), networking, system hosting, satellite and cloud computing. The DoD CIO grants DoD Information Network (DODIN) (formally Global Information Grid (GIG)) waivers to use non-DISN commercial IT services when in the best interest of DoD and when Defense Information Systems Agency (DISA) services cannot support mission requirements. Requests are evaluated from a Joint Information Enterprise (JIE) perspective for efforts such as cybersecurity, information sharing, budgeting, interoperability and mission scope.

A2.9.4. Use of a commercial ISP is not authorized unless a DODIN waiver has been approved for this service. Immediately cease all unapproved commercial ISP connections. Seek a DODIN waiver from the DoD CIO. Neither the Installation Commander, Mission Support Group Commander, nor CE's ICS PIT AO have the authority to approve commercial ISP connections. Unauthorized Commercial ISP connections result in a Denial of Authorization to Operate (DATO).

A2.9.4.1. Visit the DISA website for the DODIN Waiver Process.

A2.10. Solid State Devices and Removable Media. As recommended by NIST SP 800-82, no removable media is to be connected to a CS or CS enclave other than as described in section A2.15.4. Provisions should be made to prohibit the connection of unauthorized items, including vendor-owned devices. Make any necessary adjustments to the Service Level Support Agreement or service contract with the system maintainer or vendor.

A2.10.1. In the instance Solid State Hard Drives, Thumb Drives, Dongles, DVDs, CDs, and other removable media and storage devices are connected to a CS or CS enclave, ensure compliance with requirements outlined in USCYBERCOM CTO 10-084 and AF Network Operations Center NETOPS Tasking Order 2008-323-001.

A2.11. Switches. The use of switches within the CS should be kept to a minimum and should use managed switches to restrict port access to the CS. These devices have Security Technical Implementation Guides applicable to them, and their configurations will be assessed during the RMF lifecycle. The use of hubs is not permitted. In instances where replacing unmanaged switches becomes an enormous cost and labor burden, the best practice is to replace unmanaged switches with managed switches at the end of the asset's life cycle, however operating unmanaged switches will be taken into account by the SCA and AO.

All switches should have physical security measures. Ensure switches are stored in a locked, secure area/cabinet, and add necessary tamper-proof features to restrict access to these devices.

A2.12. Handheld Personal Devices. The use of a Personal Data Assistant (PDA) to access, monitor or control CE-owned CS is not authorized. The discovery of such a connection can result in issuance of a DATO and thus disconnection from the AF Information Network (AFIN).

A2.13. Device Security.

A2.13.1. Operating Systems. NIST SP 800-82 notes that CS operating systems and control networks are often quite different from their IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel. Assumptions that differences are not significant can have disastrous consequences on system operations.

A2.13.1.1. To the greatest extent practicable given acceptable levels of risk and final approval by the Lifecycle System Owners, AF CS' operating systems should be upgraded and maintained to the most current operating system and patch levels approved by the Air Force for the workstation baseline.

A2.13.1.2. In instances when the CS operating system cannot be upgraded for technical or operational reasons, the risk, mitigating actions, and a Plan of Actions and Milestones must be documented and approved through the RMF process by the appropriate approval roles.

A2.13.2. Anti-Virus. Use security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware on CS.

A2.13.2.1. Antivirus tools only function effectively when installed, configured, run full-time, and are maintained properly against the state of known attack methods and payloads. However, while antivirus tools are common security practice in IT computer systems, their use with CS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics. These special practices should be utilized whenever new signatures or new versions of anti-virus software are installed.

A2.13.2.2. Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general purpose SCADA and backup servers generally can be secured just like enterprise IT equipment: install push- or auto-updated antivirus and patch management software with updates distributed via an antivirus server and patch management server located inside the CS network and auto-updated from the BAN.

A2.13.2.3. Follow vendor recommendations on all other servers and computers (DCS, PLC, instruments) that have time-dependent code, modified or extended operating systems or any other change that makes it different from a standard device. Expect the vendor to make periodic maintenance releases that include security patches.

A2.13.3. Ports / Services. Because the specific function of dedicated CS devices should be determined and documented, it is relatively easy to identify those ports and input/output devices that are unnecessary.

A2.13.3.1. Disable all unused ports and services on CS devices after testing to ensure this will not impact the CS operation.

A2.13.3.2. Ensure that unused ports and services remain disabled.

A2.13.3.3. Uninstall any programs, applications and services not strictly necessary for operation of the control system.

A2.14. Configuration / Patch Management. An essential aspect of life cycle cybersecurity management is patch management to mitigate known vulnerabilities of CE-owned CS.

A2.14.1. Appropriate configuration change processes and procedures should be instituted and followed to ensure any changes to the baseline configuration are approved and coordinated with the ISO and Mission Owner (MO). The ISO should track any system modifications and document them in the installation’s CS inventory IAW NIST SP 800-53.

A2.14.2. Ideally, in order to evaluate the operational impact of installation new software prior to being applied to an operational environment, system patches and upgrades should first be assessed in a testing environment, on a backup/redundant system, or on an offline system. Then, the operational risk to the availability of the system should be weighed against the unpatched security risk to the system by the appropriate approval authority for the system or subsystem.

A2.14.3. While recognizing that an enterprise-wide CS cyber test range does not exist yet, it is recommended to work with the system vendor or manufacturer through hardware and software maintenance agreements to provide operational testing and evaluation. Bases are not expected to procure separate testbed environments for every CS.

A2.14.4. Systems should be patched or updated only with digitally-signed or hashed software from trusted authoritative sources.

A2.14.5. Procedures for on-site maintenance and patches for CS are outlined in sections A2.15.4 and A2.15.5.

A2.14.6. For further guidance on patch management, refer to *NSA Guidelines for Configuration / Patch Management in Industrial Control Systems*.

A2.15. On-site Maintenance. System maintenance practices to be followed are listed below. Further details of these practices can be found in NIST SP 800-82.

A2.15.1. To the greatest extent possible, maintenance and support should be performed on-site only (not remotely).

A2.15.2. Plan for or enforce having (if a plan exists) only government-owned computers connect to CS and CS enclaves (for maintenance or other authorized uses).

A2.15.3. Government-owned maintenance assets will be maintained by CE and must remain in government control. These maintenance assets must adhere to the following restrictions:

A2.15.3.1. Maintain the cybersecurity practices and procedures also required for NIPRNet machines.

A2.15.3.2. Uninstall any programs, applications, and services not strictly necessary.

A2.15.3.3. Disable any Wi-Fi, cameras, or microphones, preferably at the hardware or physical level.

A2.15.3.4. As stated in NIST SP 800-46 procedures, when existing contracts do not allow for maintenance using government-owned assets, ensure assets used by vendors and service personnel are thoroughly scanned for viruses and malware and have anti-virus software enabled before the asset is allowed to connect to a CS enclave or related infrastructure.

A2.15.3.5. For future CS maintenance-related contracts, incorporate contracting language ensuring the use of government-owned assets for CS maintenance. Suggested CS contracting language is detailed in DHS's *Cyber Security Procurement Language for Control Systems*.

A2.15.4. CS that support Tier 1 TCAs should be on air-gapped networks and not directly connected to either a CS enclave, the NIPRNet, or the Internet. On-site maintenance and patches for DCI-supporting CS will be accomplished using the following procedures:

A2.15.4.1. Download digitally-signed or hashed software from trusted authoritative sources to a CD/DVD.

A2.15.4.2. Scan the CD/DVD on a computer having classified scanning signatures to ensure it is malware-free.

A2.15.4.3. Insert the CD/DVD into a government-owned maintenance computer (per section A2.15.3) to connect to the stand-alone system or air-gapped CS network.

A2.15.4.4. After patching or upgrading the system, destroy the CD/DVD media to ensure it cannot be used in another device.

A2.15.5. CS that do not support DCI, whether stand-alone or connected to a CS enclave, can be maintained according to defined base maintenance, configuration, and patch management processes.

A2.15.6. Ensure CS maintenance and repair is performed and logged in a timely manner with approved tools IAW this AFGM and existing policy.

A2.16. Remote Maintenance. When on-site maintenance and support (per section A2.15) absolutely cannot be accommodated for existing contractual or cost-effective reasons, remote maintenance access to CS is allowed as an option of last resort only for CS not supporting DCI. If remote access is employed, bases must adhere to the following recommendations and restrictions:

A2.16.1. Follow security measures recommended in NIST SP 800-46, NIST SP 800-82, and DHS/CPNI's *Configuring and Managing Remote Access for Industrial Control Systems* such as requiring encryption and token-based, multi-factor authentication.

A2.16.2. Remote access to the CS or CS enclave should be of limited duration – allowed only for the time necessary to accomplish the established maintenance task. The allotted time, initial time of access, and reason for access should be coordinated between the base and vendor in order for remote access to be enabled and monitored.

A2.16.3. Any remote access to the CS or CS enclave outside of the pre-arranged window should be blocked by disabling the modem or by other technical means.

A2.16.4. All remote access events should be logged and monitored. Access and events should be reviewed on a regular schedule. Additionally, the legitimacy and necessity of access should be verified.

A2.16.5. Remote access to CS is to be phased out. On-site maintenance requirements, cybersecurity procedures and Service Level Support Agreements are to be written into new, renewed or updated maintenance and support contracts.

A2.16.6. Other remote access to the CS or CS enclave not meeting these specifications is prohibited.

A2.16.7. Remote access to CS supporting DCI is prohibited.

A2.17. Transition Plan. Funding for contract support to assume these roles and responsibilities is currently in the process of being approved through the FY18 budgeting process.

A2.17.1. To alleviate the burden and to support compliance with these RMF and cybersecurity requirements, funding for contract support is in the approval process for FY18 to provide CE CS cybersecurity expertise at the base level in a prioritized manner. These full-time cybersecurity professionals will be dedicated to managing the CS cybersecurity efforts for the CE functional community, including conducting and maintaining accurate inventories, conducting mission support analysis, managing and configuring the type-accredited CS enclaves, conducting self-assessments of security controls and performing cybersecurity maintenance and lifecycle management of CE-owned CS.

A2.17.2. Inventories and the full implementation of cybersecurity controls on critical infrastructure-related CS need to be completed and in place by the end of FY19. Until bases receive dedicated manpower, bases are expected to plan for and comply with the remainder of guidance contained in this AFGM to the greatest extent possible given availability of resources and expertise.

A2.17.3. At this time, the exact roles and responsibilities for a Cybersecurity Defense Service Provider (CDSP) to provide defensive cyber operations and continuous monitoring for CE-owned CS and CS enclaves have not yet been determined.

A2.17.4. Further training material and templates are forthcoming to assist in base execution of this AFGM's requirements.

A2.18. Technical Support. For specific CS-related technical support and guidance, AFCEC's CEMIRT Division supports the accreditation of CE CS and guidance for implementing the enclave for CE-owned CS. CEMIRT can be reached by phone at DSN 523-6989/6929 or by e-mail at afcec.comi.icshelpdesk@us.af.mil, afcec.comi.ics@us.af.mil.

A2.19. Technical References. For specific technical guidance on the policies outlined above and on additional CE CS security controls, consult the following references which detail procedures on cybersecurity best practices and on system classification for tailoring security controls.

A2.19.1. NIST SP 800-82

A2.19.2. NIST SP 800-53

A2.19.3. NIST Framework for Industrial Control System Cybersecurity

A2.19.4. NSA Information Assurance Directorate Guidance for Industrial Control Systems

A2.19.5. *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures for Department of Defense Industrial Control Systems*

A2.19.6. Federal Information Processing Standards Publications (FIPS PUBS)

A2.19.7. CNSSI No. 1253, *Security Control Overlays for Industrial Control Systems*

A2.19.8. DHS ICS-CERT Standards and References

A2.19.9. Air Force Control Systems Community