****

USACE / NAVFAC / AFCEC **UFGS-25 05 11 (August 2024)**

Preparing Activity: USACE **Superseding**
UFGS-25 05 11 (May 2021)

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated July 2024
****

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
08/24

****

NOTE: This guide specification covers the requirements for cybersecurity for LOW and MODERATE impact facility-related control systems to meet the requirements of the Department of Defense Risk Management Framework (RMF).

Adhere to UFC 1-300-02 Unified Facilities Guide Specifications (UFGS) Format Standard when editing this guide specification or preparing new project specification sections. Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable item(s) or insert appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be as a Criteria Change Request (CCR).
****
****

Note: Facility-related control systems are a subset of control systems that are used to monitor and control equipment and systems related to DoD real property facilities (e.g., building control systems, utility control systems, electronic security systems, and fire and life safety systems). This section includes Cybersecurity requirements to be included on every DoD project which includes a facility-related control system. This Section does not provide general requirements for a control system, nor are the requirements in this section sufficient to procure a control system. This section must be used in conjunction with another controls system specification. For example, for a

HVAC controls project, this section should be used in conjunction with Section 23 09 00 and related sections.

Requirements and activities in this section must be coordinated with the other relevant control specification sections. Requirements specific to Cybersecurity should be incorporated into this section, and requirements not specific to Cybersecurity should be included in the appropriate controls section.

This section includes requirements in support of the DoD Risk Management Framework (RMF) for implementing cybersecurity. Refer to UFC 4-010-06, Cybersecurity for Facility-Related Control Systems for requirements on incorporating cybersecurity into control system design and for general information on the RMF process as it applies to control systems.

Assistance for control system cybersecurity is available from the following Service organizations:

Army (other than USACE Civil Works):
Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX), Huntsville Engineering and Support Center (CSC-MCX@usace.army.mil).

Navy (and Marine Corps):
Naval Facilities Engineering Systems Command, Command Information Office (CIO)

Air Force (and Space Force):
Air Force Civil Engineering Center (AFCEC) Operations Directorate, Tyndall Air Force Base

USACE Civil Works:
USACE Critical Infrastructure Cybersecurity Mandatory Center of Expertise (UCIC-MCX) (uciccybersecurity@usace.army.mil)

Note that all projects where USACE is the design-construction agent require coordination with the relevant cybersecurity MCX as well as all other relevant control system MCXs.

Since this Section covers a wide range of control systems, and those systems often have different capabilities and requirements, there are requirements identified in this Section which need extensive designer input or decisions.

Many designer selections in this Section will require coordination with the project site, System Owner, Authorizing Official or a subject matter expert in the specific control systems being installed.

****
****

NOTE: This Guide Specification is for use on control systems having no impact rating higher than MODERATE. If the project includes systems with impact ratings of HIGH, this specification must be modified to include those additional requirements.

Systems of different types at the same impact level may have different requirements based on the specific needs and capabilities of the control system. This is addressed in this Guide Specification by indicating when requirements apply to a specific system type.
Systems of the same type may have different requirements. This may be due to those systems having different impact levels or due to system-specific requirements for systems at the same impact level.

If a project includes multiple systems, it's critical that it be clear which requirements apply to which systems. This can be done by a) using a single Section and specifying the applicability of requirements (indicating for each system what impact level and system type it is) or b) using multiple Sections. Which approach to employ depends on the needs of the project and the preferences of the specifier and project manager. If using multiple sections use the fourth level specification numbering to differentiate the Sections and indicate in each which systems the Section applies to, for example, one project may have:
1) Section 25 05 11.01 CYBERSECURITY FOR LOW IMPACT HVAC CONTROL SYSTEMS

2) Section 25 05 11.02 CYBERSECURITY FOR LOW IMPACT LIGHTING SYSTEMS

3) Section 25 05 11.03 CYBERSECURITY FOR MODERATE IMPACT ELECTRONIC SECURITY SYSTEMS

4) Section 25 05 11.04 CYBERSECURITY FOR LOW IMPACT CIVIL WORKS CONTROL SYSTEMS

(The fourth level numbering is not required to be sequential, as long as the mapping between the cybersecurity specification and the control system is clear. Some projects may wish to use fourth level numbering that matches the division they support (25 05 11.23 for HVAC (mechanical) for example).)

In accordance with UFC 4-010-06, for projects designed by or under contract to USACE use multiple specifications as described in this note, where each system has a corresponding cybersecurity section which is included with the section(s) specifying the control system.

****
****
NOTE: This specification makes use of SpecsIntact Tailoring Options.

Services tailoring options:
Army
Air Force

Impact Level tailoring options:
LOW Impact
MODERATE Impact

Control system type tailoring options:
HVAC Control Systems
Lighting Control Systems
Electronic Security Systems (ESS)
Fire Protection Systems
USACE CW (for USACE Civil Works systems)
Designer Specified Requirements
Default Requirements

Currently, all text in Fire Protection tags is also within MODERATE Impact tags, and LOW Impact Fire Protection systems are addressed by the default requirements.

These tailoring options affect the subparts that are included throughout the specification to "break out" specific requirements. The "Default Requirements" tailoring option includes "generic" requirements that are intended to apply to a wide range of control systems. The "Designer Specified Requirements" tailoring option will include blank subparts for the specification of requirements, and is intended to be used when customizing requirements to a control system type for which there is no specific tailoring option and for which the "Default Requirements" are not applicable.

Include only tailoring options for the specifications to be addressed. Only include "Default Requirements" if the section is to cover a system not covered by one of the specific system type options AND the "Default Requirements" are adequate. Only include "Designer Specified Requirements" if the section is to cover a system not covered by one of the specific system type options, AND the "Default Requirements" are NOT adequate. When selecting "Designer Specified Requirements", requirements must be added throughout the specification.
****

PART 1 GENERAL
****
NOTE: As described in the paragraph below, this Section includes text in curly braces ("{" and "}")

indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. When editing this specification to incorporate requirements for other controls or CCIs or to remove requirements related to specific controls or CCIs, revise the list of controls and CCIs accordingly. DO NOT REMOVE THE TEXT IN CURLY BRACES in the final specification; this information is needed for reference during construction, commissioning and cybersecurity assessments.

****

****

NOTE: This subpart points the contractor to the locations of STIGs and SRGs, as this Section requires the contractor to meet available STIGs or SRGs. It's not necessary for the designer/specifier to review the STIGs or SRGs for applicability. The contractor is responsible for determining which STIGs or SRGs are applicable and for meeting the relevant requirements.

While most STIGs/SRGs do not require a CAC to access, FOUO STIGs/SRGs do. See the SRG-STIG Compilation Read-Me for more information - https://dl.dod.cyber.mil/wp-content/uploads/stigs/pdf/U_STIG_Library-zip_Read-ME_v1-07.pdf

****

Many subparts in this Section contain text in curly braces ("{" and "}") indicating which cybersecurity control and control correlation identifier (CCI) the requirements of the subpart relate to. The text inside these curly braces is for Government reference only and enables coordination of the requirements of this Section with the RMF process throughout the design and construction process. Text in curly braces are not contractor requirements.

This Section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at https://public.cyber.mil/stigs/downloads/ and an SRG/STIG Applicability Guide and Collection Tool is available at https://public.cyber.mil/stigs/SCAP/. Not all control system components have applicable STIGs or SRGs. The "Control Systems SRG" does not apply to work performed under this Section; all requirements within this section to apply applicable SRGs DO NOT include the "Control Systems SRG".

[1.1 CONTROL SYSTEM APPLICABILITY

****

NOTE: If multiple versions of this Section are used on a single project, keep this subpart and list all the systems to which this specific version of the Section applies.

****

There are multiple versions of this Section associated with this project. Different versions have requirements applicable to different control systems. This specific Section applies only to the following control systems: [_____].

]1.2 RELATED REQUIREMENTS

This section does not contain sufficient requirements to procure a control system and must be used in conjunction with other Sections which specify control systems. This Section adds cybersecurity requirements to the control systems specified in other Sections, and as these requirements are conditioned on the control system being provided, there may be requirements in this Section that will not apply to this project. All Sections containing facility-related control systems or control system components are related to the requirements of this Section. Review all specification sections to determine related requirements.

In cases where a requirement is specified in both this Section and in another Section, the more stringent requirement must be met. In cases where a requirement in this Section conflicts with the requirements of another Section such that both requirements cannot be met at the same time, request direction from the [Contracting Officer][_____] to determine which requirement applies to the project.

1.3 REFERENCES

****

NOTE: This paragraph is used to list the publications cited in the text of the guide specification. The publications are referred to in the text by basic designation only and listed in this paragraph by organization, designation, date, and title.

Use the Reference Wizard's Check Reference feature when you add a RID outside of the Section's Reference Article to automatically place the reference in the Reference Article. Also use the Reference Wizard's Check Reference feature to update the issue dates.

References not used in the text will automatically be deleted from this section of the project specification when you choose to reconcile references in the publish print process.

****

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE)

ASHRAE 135 (2020; Interpretation 1-8 2021; Errata 1-2 2021; Addenda CD 2021; Addenda BV-CE 2022; Interpretation 9-12 2022; Interpretation 13-24 2023; Addenda BV-CF 2023; Errata 3 2023) BACnet—A Data Communication Protocol for Building Automation and Control Networks

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE 802.1x	(2010) Local and Metropolitan Area Networks - Port Based Network Access Control

INTERNET ENGINEERING TASK FORCE (IETF)

IETF RFC 2819	(2000) Remote Network Monitoring (RMON) Management Information Base (MIB)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 140-2	(2001) Security Requirements for Cryptographic Modules
NIST FIPS 201-2	(2013) Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

DODI 8551.01	(2014) Ports, Protocols, and Services Management (PPSM)
DTM 08-060	(2008) Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement

1.4 DEFINITIONS

1.4.1 Administrator Account

An administrator account is an account with full permissions to a device, application, or operating system, including the ability to create and modify other user accounts.

Note that the operating system Administrator Account may be different than Administrator Accounts for applications hosted on that operating system. Also, most controllers will not have any support for accounts and will therefore not have an 'Administrator Account'.

1.4.2 Computer

A computer is one of the following:

a. a device running a non-embedded desktop or server version of Microsoft Windows

b. a device running a non-embedded version of MacOS

c. a device running a non-embedded version of Linux

d. a device running a version or derivative of the Android Operating System, where Android is considered separate from Linux

e. a device running a version of Apple iOS

Unless otherwise indicated or clear from context use of the word "device" in this Section includes computers.

1.4.3 Controller

****
NOTE: This subpart uses the USACE CW tailoring option to add IP Router.
****

A device other than a computer, IP Router, or Ethernet switch. For Fire Protection systems this includes fire alarm control panels, remote operating consoles, and remote annunciators.

1.4.4 Mission Space

****
NOTE: Define "Mission space" such that the contractor is able to determine when a network or device is outside of the mission area. Coordinate the definition of Mission Space with the physical security design and the security organization at the project site.

Select whether to leave the definition or to define mission space on a drawing.
****

[A device or media is in mission space if physical access to the device or media is controlled by the organization served by the device. For example, a variable air volume (VAV) box controller in a suspended ceiling is in mission space if the VAV box serves that room; an electrical switchgear in an electrical room or an air handling unit (AHU) in a mechanical room or on a rooftop may still be considered to be in mission space if the organization (mission) served by that switchgear or AHU controls access to the electrical room, mechanical room or rooftop.][Mission space is shown on the drawings.]

1.4.5 Network

A network is a group of two or more devices that can communicate using a network protocol. Network protocols must provide a method for addressing devices on the network; a communication method that does not provide an addressing scheme is not a networked form of communication. Devices that communicate using a method of communication that does not support device addressing are not using a network. Addresses may be other than IP addresses, and addressing may be at either Open Systems Interconnection (OSI) layer 2 or layer 3.

1.4.6 Network Connected

A component is network connected (or "connected to a network") only when the device has a network transceiver which is directly connected to the network and implements the network protocol. A device lacking a network transceiver (and accompanying protocol implementation) can never be considered network connected. Note that (unlike many IT definitions of "Network Connected") a device connected to a non-IP network is still considered network connected (an IP connection or IP address is not required for a device to be network connected).

1.4.6.1 Wireless Network Connected

Any device that supports wireless network communication is network connected to a wireless network, regardless of whether the device is communicating using wireless. Unless physically disabled, devices with wireless transceivers support wireless, it is not sufficient to disable the wireless in software.

1.4.7 Network Media

The thing that provides the communication channel between the devices on a network. Typically wire, but might include wireless, fiber optic, or even power line (some network protocols allow sending network signals over power wiring).

1.4.8 Network Segmentation

****
NOTE: This subpart is only included when the USACE CW tailoring option is selected.
****

Segmenting or segregating networks either by logical or physical methods. Examples of logical methods include firewall zones, virtual local area networks (VLANs), or virtual private networks (VPNs). Physical separation is done by deploying additional hardware. Network segmentation is used for isolation of discrete functions or processes. Each network segment will have its own IP address space or subnet.

1.4.9 Operational Technology (OT)

****
NOTE: This subpart is only included when the USACE CW tailoring option is selected.
****

The hardware and software dedicated to detecting and/or causing changes in physical processes through direct monitoring and control of physical devices to accomplish a specific mission in real time.

1.4.10 User Account Support Levels

The support for user accounts is categorized in this Section as one of three levels:

1.4.10.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts. These devices support user-based (as opposed to role-based) authentication.

1.4.10.2 MINIMALLY Supported

Device supports a small, fixed number of accounts (perhaps only one). Accounts cannot be modified. A device with only a "User" and an "Administrator" account would fit this category. Similarly, a device with two PINs for logon - one for restricted and one for unrestricted rights would fit here (in other words, the accounts do not have to be the traditional "username and password" structure). These devices typically

only support role-based authentication.

Examples of devices which MINIMALLY support accounts are a) a variable frequency drive with a single account which requires a PIN for access to configuration; and b) a room lighting control touchpad interface that has a single account.

1.4.10.3 NOT Supported

Device does not support any Access Enforcement therefore the whole concept of "account" is meaningless.

1.4.11 Manual Local Input

Manual Local Inputs are system analog or binary inputs that are adjustable by a person but are, by intrinsic hardware design, very limited in potential capabilities. Manual Local Inputs do not have touch screens or full keyboards, but may have a few buttons or dials to allow input. Manual Local Inputs do not have full graphic screens or dot-matrix displays, but may have simple lights (LEDs) or 7-segment displays. Manual Local Inputs do not have any sort of menu structure, each button has a single well-defined function.

Examples of Manual Local Inputs are H-O-A switches, simple thermostats, and disconnect switches.

1.4.12 Card Reader

A card reader is an input/output device whose primary function is to assist in two-factor authentication. A card reader must have an interface to read data from a card and may be able to write data to a card. A card reader may have a means (such as buttons, keypad, touchscreen, etc.) for a user to input a PIN or password, as well as a limited display.

1.4.13 User Interface

A User Interface (UI) is something other than a Manual Local Input or Card Reader that allows a person to interact with the system or device. Note that while a Card Reader is not by itself a User Interface, a User Interface may contain a Card Reader in order for it to authenticate its user. Within control systems, there are a wide range of User Interfaces.

Two important distinctions are 1) whether the user interface is Local or Remote, and 2) the effective capabilities of the User Interface to alter data, which is the "privilege" of the user interface (where effective privilege available to a specific user at a specific user interface is the combination of the greatest privilege offered by the user interface and the specific account the user is logged into).

1.4.13.1 Local User Interface

A Local User Interface is a user interface where the physical hardware the user interacts with (keyboard, buttons, display, etc.) is physically part of the device being affected. All of the relevant characteristics of the user interface are embodied within a single device.

Note that a Local UI may be able to access data in a different device, Local versus Remote in this context refers to the user interface itself; the capability to access data in a different device is covered under "Full

User Interface".

1.4.13.2 Remote User Interface

A Remote User Interface implements a Client/Server model where the physical hardware the user interacts with (Client) is physically distinct from the device being affected (Server). Most or all of the security and functionality characteristics of the user interface are defined by the Server, not the Client. The Client and Server communicate via a network connection. A common example of a remote user interface is a web-based interface where the browser (client) is generally on different hardware than the web server (server). A Remote UI remains a Remote UI even if the user happens to be at a Client on the same hardware as the Server. What is important is that a) the Client may be on different hardware than the Server and b) the majority of the security and functional characteristics of the interface are defined at the Server.

Note that this definition of "remote" is consistent with that generally used in the control industry but is not aligned with the NIST 800-53 definition of "Remote", which refers to "outside the system". The term "Remote" here better aligns with the NIST 800-53 definition of "Network" (remote from within the system) Access.

1.4.13.3 Types of User Interface (by capability)

User interfaces are also categorized by their capabilities as being Read Only, Limited, or Full.

1.4.13.3.1 Read-Only User Interface

A Read Only User Interface (also referred to as a View-Only User Interface) is a user interface that only allows for reading data, it does not allow (have the capability to) modify data. A Read Only User Interface may be either Local or Remote. A User Interface that is configured to be Read Only (by some other means than the interface itself, such as using configuration software on a laptop) is a Read-Only Interface. Note a Read Only User Interface may have buttons (or touch screen, etc.) allowing the user to navigate through the presentation of data.

Examples of a Read Only User Interfaces are a) a publicly viewable "energy dashboard" showing weather data and energy usage within a building and b) digital wayfinding signage.

1.4.13.3.2 Limited User Interface

A Limited User Interface is a user interface that - by design - can only alter information local to the user interface. Note that the determination of "alter" includes only direct interactions, it explicitly excludes interactions that might occur as secondary effects. For example, an interface changing the flow setpoint in a pump controller is a direct interaction, the subsequent change in flow (as well as any subsequent downstream changes in valve position) are not direct interactions.

Two examples of LIMITED UIs are: a) a variable speed drive has a Limited Local User Interface which allows the user to change properties within the drive, but does not allow affecting things outside the drive; and b) a typical home WiFi Router has a Limited Remote User Interface which allows configuration of the Router, but does not allow direct interaction with

other devices.

1.4.13.3.3 Full User Interface

A Full User Interface can alter information in devices outside the device with the user interface. For example, a typical Local Display Panel is a Full Local User Interface while a browser-based front end is a Full Remote User Interface.

1.4.13.3.4 View-Only User Interface

See Read-Only User Interface

1.4.13.4 Other User Interface Terminology

In addition to defining whether a user interface is a Hardware Limited, Read-Only, Limited or Full, and whether it is Local or Remote, user interfaces are classified by whether they are writable or privileged.

1.4.13.4.1 Writable User Interface

Any User Interface that is not Read-Only is Writable. (Limited User Interfaces and Full User Interfaces are both writable user interfaces (as they are capable of changing a value)).

1.4.13.4.2 Privileged User Interface

****

NOTE: This subpart uses tailoring options for the lettered requirements. After selecting tailoring options edit the letters in this subpart accordingly.

****

A Privileged UI is a UI that has sufficient capabilities or functionality that it requires specific cybersecurity measures to be put in place to limit its unauthorized use. Ultimately, whether a specific user interface is considered a Privileged User Interface must be determined by usage. Unless otherwise specified, user interfaces can be determined to be privileged or not using the following:

a. Read-Only User Interfaces are not privileged user interfaces.

b. User Interfaces that can inhibit or force the activation of a fire suppression system (e.g. such as for a pre-action or deluge system) are always privileged user interfaces. Other Full User interfaces for Fire Alarm Systems are privileged user interfaces as indicated and shown, or when another requirement of this Section establishes they are privileged. For all other systems, Full User Interfaces are privileged user interfaces.

c. User interfaces that allow for configuration of auditing or allows for modification or deletion of audit logs are privileged user interface.

d. User interfaces that allow for reprogramming a network connected device is a privileged user interface.

e. Writeable User Interfaces in Electronic Security Systems (ESS) are privileged user interfaces.

e. Except as specified above, a Limited User Interface must be determined to be privileged or not based on the specific capabilities and use case of the user interface. In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged.

1.4.14 Wireless Network

Any network that communicates without using wires or fiber optics as the communication media. Wireless networks include: WiFi, Bluetooth, ZigBee, cellular, satellite, long and short wave radio, 2.4 GHz, free space optical, point-to-point laser, microwave, and IR.

1.4.15 Wired Broadcast Network

Wired Broadcast Networks are any network, such as powerline carrier networks and modem (wired telephony), that use wire-based technologies where there is not a clearly defined boundary for signal propagation.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Points of Contact

****

NOTE: Indicate the appropriate point of contact (POC) for each POC.

Previous versions of this specification identified the Contracting Officer Representative (COR) as the POC. UFC 1-300-02, 2-3.7 states, "Use the term "Contracting Officer" \1\; do not use terms such as /1/ “Officer in Charge of Construction,” “Contracting Officer Representative ,” or “Government Representative.” The Contracting Officer (KO) will likely designate a representative, but this is an internal decision and not something the Contractors need to be apprised of.

Government Computer Access Point of Contact: To provide contractor user access to Government computers. Specifically, this POC may be required to arrange for elevated permissions to computers to create a backup disk image or install malware protection software.

HTTPS Certificate Point of Contact: To provide the contractor with web certificates.

Email Address Point of Contact: The POC who will provide the contractor with email addresses for the ISSM and application administrator for auditing.

Password Point of Contact: The POC who will either coordinate the selection of passwords with the contractor or who will indicate individuals to change the passwords in coordination with the contractor.

Mobile Code Point of Contact: The POC who will provide access to the mobile code repository. (This will generally be someone from the installation IT organization (for the Army, the NEC).)

PKI Infrastructure Point of Contact: The POC who will provide access to the PKI Infrastructure. If PKI is not required by PART 3 of this Section, remove this bracketed text. (This will generally be someone from the installation IT organization (for the Army, the NEC).)

These points of contact are used by name in the specification, and can be found by searching the document for the POC (using underlined text).

Not all projects will require all POCs. If unsure of the POC keep "The Contracting Office Representative (COR)" and the contractor will request as needed.

****

Coordinate with the following Points of Contact as indicated in this Section and as required. Not all projects will require coordination with all Points of Contact. When coordination is required and no Point of Contact is indicated, coordinate with the [Contracting Officer (KO)][_____].

a. Government Computer Access Point of Contact: [Contracting Office (KO)][_____]

b. HTTPS Certificate Point of Contact: [Contracting Officer (KO)][_____]

c. Email Address Point of Contact: [Contracting Officer (KO)][_____]

d. Password Point of Contact: [Contracting Officer (KO)][_____]

e. Mobile Code Point of Contact: [Contracting Officer (KO)][_____][

f. PKI Infrastructure Point of Contact: [Contracting Officer (KO)][_____]
]

1.5.2 Coordination

****

NOTE: This subpart deals with cybersecurity related coordination requirements for the contractor, and does not indicate coordination that must be done by the designer/specifier. In addition to the normal project coordination, authorization for wireless use, alternate account lock permissions and devices with multiple IP connections may be impacted by site (or Service) policies and need to be coordinated with the appropriate Government representatives before authorization is provided.

****

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS. Items that must be considered when coordinating project efforts include but are not limited to:

a. If requesting permission for wireless or wired broadcast communication, the Wireless and Wired Broadcast Communication Request submittal must be approved prior to control system device selection and installation.

b. If requesting permission for alternate account lock permissions, the Device Account Lock Exception Request must be approved prior to control system device selection and installation.

c. If requesting permission for the use of a device with multiple physical connections to IP networks, the Multiple IP Connection Device Request must be approved prior to control system device selection and installation.

d. Wireless testing may be required as part of the control system testing. See requirements for the Wireless Communication Test Report submittal.

e. If the Device Audit Record Upload Software is to be installed on a computer not being provided as part of the control system, coordination is required to identify the computer on which to install the software.

f. The Cybersecurity Interconnection Schedule must be coordinated with other work that will be interconnected to, and interconnections must be approved by the Government before relying on them for system functionality.

g. Cybersecurity testing support must be coordinated across control systems and with the Government cybersecurity testing schedule.

h. Passwords must be coordinated with the indicated contact for the project site.

i. If applicable, HTTPS web server certificates must be obtained from the indicated HTTPS Certificate Point of Contact.

j. Contractor Computer Cybersecurity Compliance Statements must be provided for each contractor using contractor owned computers.

1.6 SUBMITTALS

****

NOTE: Review Submittal Description (SD) definitions in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list, and corresponding submittal items in the text, to reflect only the submittals required for the project. The Guide Specification technical editors have classified those items that require Government approval, due to their complexity or criticality, with a "G." Generally, other submittal items can be reviewed by the Contractor's Quality Control System. Only add a "G" to an item, if the submittal is sufficiently important or

complex in context of the project.

For Army projects, fill in the empty brackets following the "G" classification, with a code of up to three characters to indicate the approving authority. Codes for Army projects using the Resident Management System (RMS) are: "AE" for Architect-Engineer; "DO" for District Office (Engineering Division or other organization in the District Office); "AO" for Area Office; "RO" for Resident Office; and "PO" for Project Office. Codes following the "G" typically are not used for Navy, and Air Force.

The "S" classification indicates submittals required as proof of compliance for sustainability Guiding Principles Validation or Third Party Certification and as described in Section 01 33 00 SUBMITTAL PROCEDURES.

****

****

NOTE: All submittals in this Guide Specification require Government approval and must have a "G" designation.

Government review of submittals in this Section impact Cybersecurity, and must be coordinated with the appropriate Cybersecurity experts to ensure appropriate review and the identification of issues or concerns that may affect the cybersecurity posture of the system or the ability of the system to receive an RMF authorization.

****

****

NOTE: Throughout this subpart, the USACE CW Tailoring Option is used to add "(Encrypted)" after some submittal names.

****

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are for Contractor Quality Control approval. Submittals not having a "G" or "S" classification are for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government. Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

****

NOTE: When the FIRE PROTECTION tailoring option is selected, the Wireless and Wired Broadcast Communication Request will be in brackets. If this specification is used ONLY for Fire Protection Systems remove the bracketed text. Otherwise keep it.

****

****

NOTE: When the USACE CW tailoring option is selected, the USACE OT/Control Systems Acceptable Use Policy (AUP) and Account Level Permissions List submittals are included.

[Wireless and Wired Broadcast Communication Request; G, [_____]

] Device Account Lock Exception Request; G, [_____]

Multiple Ethernet Connection Device Request; G, [_____]

Contractor Computer Cybersecurity Compliance Statements; G, [_____]

Contractor Temporary Network Cybersecurity Compliance Statements; G, [_____]

Cybersecurity Interconnection Schedule (Encrypted); G, [_____]

Protection of Information At Rest Proposal; G, [_____]

Proposed STIG and SRG Applicability Report; G, [_____]

Pre-Construction Control System Inventory Report (Encrypted); G, [_____]

Contractor Personnel Certifications; G, [_____]

USACE OT/Control Systems Acceptable Use Policy (AUP); G, [_____]

Account Level Permissions List (Encrypted); G, [_____]

SD-02 Shop Drawings

NOTE: When the USACE CW tailoring option is selected, the System Data Flow Diagram submittal is included.

Network Communication, Ports, Protocols and Services Report; G[, [_____]]

Cybersecurity Network (Riser) Diagram (Encrypted); G, [_____]

System Data Flow Diagram (Encrypted); G, [_____]

SD-03 Product Data

NOTE: When the USACE CW tailoring option is selected, the Certificate Protection Status submittal is included.

Control System Cybersecurity Documentation; G, [_____]

Certificate Protection Status (Encrypted); G, [_____]

SD-06 Test Reports

****
NOTE: When the FIRE PROTECTION tailoring option is selected, the Wireless Communication Test Report will be in brackets. If this specification is used ONLY for Fire Protection Systems remove the bracketed text. Otherwise keep it.
****

[Wireless Communication Test Report; G, [_____]
]

Control System Cybersecurity Testing Procedures; G, [_____]

Control System Cybersecurity Testing Report; G, [_____]

Antivirus/Antimalware Scan Results; G, [_____]

SD-07 Certificates

Software Licenses; G, [_____]

SD-11 Closeout Submittals

****
NOTE: In PART 3 of this Section there is a designer selection to indicate whether the contractor changes passwords or accompanies site personnel while they change passwords.

If requiring contractor to change passwords, keep "Confidential Password Report" and remove "Password Change Summary Report"

If requiring contractor to accompany site personnel to change passwords, keep "Password Change Summary Report" and remove "Confidential Password Report"
****

[Confidential Password Report; G, [_____]

][Password Change Summary Report; G, [_____]

] Enclosure Keys; G, [_____]

Software and Configuration Backups (Encrypted); G, [_____]

Auditing Front End Software; G, [_____]

Device Audit Record Upload Software; G, [_____]

System Maintenance Tool Software; G, [_____]

Control System Scanning Tools; G, [_____]

STIG, SRG and Vendor Guide Compliance Result Report (Encrypted); G, [_____]

Final Control System Inventory Report (Encrypted); G, [_____]

Integrity Verification Software; G, [_____]

Vulnerability Resolution Report; G, [_____]

BIOS/UEFI Protection Password/Passphrase List (Encrypted); G, [_____]

1.7 ENCRYPTED SUBMITTAL REQUIREMENTS

****
NOTE: This subpart is only included when the USACE CW tailoring option is selected
****

Submittals with sensitive data are marked with "(encrypted)" and must be encrypted with NIST FIPS 140-2 compliant encryption methods with a password that meets the requirements under paragraph PASSWORDS. Encrypted submittals must be sent via DoD SAFE (https://safe.apps.mil/) and only sent to those who need to know. If DoD SAFE is not available, the government will provide an alternative secure file transfer that must be used. Do not store encrypted submittals on shared storage systems. Store and send encrypted information separately than the password.

1.8 QUALITY CONTROL

****
NOTE: If using these subparts to add requirements, be sure to add submittal requirements as needed to support these requirements.
****

[1.8.1 Regulatory Requirements

****
NOTE: If there are regulatory requirements related to a control system, specify those in the control system specification. If there are regulatory requirements related to cybersecurity for a control system they can be specified here.
Regulatory requirements specified here must indicate which system or systems they apply to, DO NOT include requirements here that are not directly linked to a specific control system.

For typical UMCS or building control system projects there will not be requirements to include here.
****

For the [_____] control system: [_____].

][1.8.2 [Certifications][Qualifications]

****
NOTE: THIS SUBPART IS NOT USED FOR USACE CW SYSTEMS. When the USACE CW tailoring option is selected, a subpart with USACE CW requirements is included, and this subpart should be removed during bracket replacement.

For all other systems:
If there are contractor qualification or certification requirements related to the control system, specify those in the control system specification. If there are contractor qualifications or certifications specifically related to cybersecurity they can be specified here.

Use care when including requirements here, as many cybersecurity certifications are IT-centric and do not apply to control systems.

Requirements specified here must indicate which system or systems they apply to, DO NOT include requirements here that are not directly linked to a specific control system.

For typical UMCS or building control system projects there will not be requirements to include here.
****

For the [_____] control system: [_____].

]1.8.3 Certifications

****
NOTE: This subpart only applies to USACE Civil Works systems and is only included when the USACE CW Tailoring Option is selected.
****

Personnel performing cybersecurity functions must have current [IAT level 1][IAT level II][_____] certification according to approved DoD IA baseline certifications. Provide Contractor Personnel Certifications no later than [30][_____] days following Notice To Proceed. A cybersecurity function includes security-relevant functions that ordinary users are not authorized to perform. Examples of these activities include, but are not limited to, creating/modifying user accounts, configuring auditing levels, configuring functionality of a device that is restricted from general users, network architecture design, and applying secure configuration to an Operating System or device. See https://public.cyber.mil/cwmp/dod-approved-8570- baseline-certifications/.

Personnel who will have access to make changes to the OT system must read, agree to, and sign the USACE OT/Control Systems Acceptable Use Policy (AUP), provided by the government prior to accessing the OT system. Provide signed AUPs no later than [30][_____] days after notice to proceed.

[1.8.4 Pre-Construction Testing

****
NOTE: If there are cybersecurity Pre-Construction Testing requirements, include them here.

For a LOW-LOW-LOW Impact system pre-construction testing will generally not be required. For systems with a MODERATE or HIGH impact there may be some pre-construction testing requirements based on the

specific needs of the project site.

Requirements specified here must indicate which system or systems they apply to, DO NOT include requirements here that are not directly linked to a specific control system.

Note, these concern testing of the control system, requirements on testing of the contractor's network during construction are separately covered below.

****

For the [_____] control system: [_____].

][1.9 DELIVERY, STORAGE, AND HANDLING

****

NOTE: If there are general delivery, storage or handling requirements related to a control system, specify those in the control system specification If there are delivery, storage or handling requirements specific to cybersecurity, include them here.

For a LOW-LOW-LOW Impact system delivery, storage and handling requirements will generally not be needed. For systems with a MODERATE or HIGH impact there may be some requirements based on the specific needs of the project site.

****

[_____]

]1.10 CYBERSECURITY DOCUMENTATION

{For Government Reference Only: This subpart (and its subparts) relates to PL-7; CCI-003071}

1.10.1 Proposed STIG and SRG Applicability Report

For each model of network connected or network infrastructure device, use the DISA SRG/STIG Applicability Guide and Collection Tool (available at https://public.cyber.mil/stigs/SCAP/to identify applicable STIGs or SRGs and provide a report indicating applicable STIGs and SRGs for each model. Provide the Proposed STIG and SRG Applicability Report concurrently with the Pre-Construction Control System Inventory Report.

[1.10.2 Cybersecurity Interconnection Schedule (Encrypted)

****

NOTE: When the USACE CW Tailoring Option is selected, the text "(Encrypted)" is included following the submittal title in the title of this subpart.

****

****

NOTE: The Cybersecurity Interconnection Schedule is used in two situations:

1) The control system communicates with a separately authorized system or an unauthorized system. In this case, include a Cybersecurity Interconnection Schedule in the design showing the following interconnection details: Name/description of other system, POC for the other system, type of data/information.

2) The control system is a sub-part of a larger system and will communicate with and integrate to the larger system (and will be part of the same authorization as the larger system). In this case, the control system design must include requirements for the expected communication between the sub-system and the larger system. The Cybersecurity Interconnection Schedule will not be a design drawing, but will still be a contractor submittal.

If neither of these situations apply (if the system is stand-alone with no connection or integration to another system), remove the bracketed text requiring the Cybersecurity Interconnection Schedule, and remove the Cybersecurity Interconnection Schedule from the SUBMITTALS paragraph of this Section.

If Case 1 applies, keep the bracketed text referring to Foreign Destination and POC for Destination, otherwise remove this text.

In situations where both cases apply, a single submittal will serve both purposes.

Note that this submittal does not create a requirement for interconnections, but documents interconnection details in accordance with other requirements.

****

{For Government Reference Only: This subpart relates to CA-3(b), PL-8, SC-7(9), SC-7(11); CCI-000258, CCI-003072, CCI-003073, CCI-003075, CCI-002398, CCI-002399, CCI-002401, CCI-002402, CCI-002403. For MODERATE Impact systems, this subpart also relates to SC-7; CCI-001126, CCI-001109}

Provide a completed Cybersecurity Interconnection Schedule documenting network connections between the installed system and other systems. Provide the following information for each device directly communicating between systems: Device Identifier, Device Manufacturer, Device Description, Transport layer Protocol, Network Address, Port (if applicable), MAC (Layer 2) address (if applicable), Media, Application Protocol, Service (if applicable), Descriptive Purpose of communication. [For communication with other authorized systems also provide the Foreign Destination and POC for Destination.] For MODERATE Impact Systems: Also describe the impact of loss of the connection on the control system. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES,

provide the Cybersecurity Interconnection Schedule as an editable Microsoft Excel file (a template Cybersecurity Interconnection Schedule in Excel format is available at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11.)

]1.10.3 Network Communication, Ports, Protocols and Services Report

****

NOTE: Control system specifications should include requirements related to protocol and documentation. In the design cybersecurity documentation required by the UFC, document what, if any, protocol requirements are included in the control system specification (CCI-002103). Also document any requirements or submittals related to network communication, such as Points Schedules (CCI-002105).

****

{For Government Reference Only: This subpart (and its subparts) relates to CA-9, PL-8; CCI-002102, CCI-002103, CCI-002104, CCI-002105, CCI-003072, CCI-003073, CCI-003075 and also the submittal requirements associated with CM-6, CM-7, including CM-7(3), CCI-000388.}

Provide a Network Communication, Ports, Protocols and Services Report. For each networked device, document device identifier and the communication characteristics of the device including communication protocols, services used, encryption employed, and a general description of what information is communicated over the network. For each device using IP communication, document all TCP and UDP ports used. For each device using non-IP communication, document communication protocol and media used. If other control system Sections used on this project include submittals documenting this information, provide copies of those submittals to meet this requirement.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Network Communication, Ports, Protocols and Services Report as an editable Microsoft Excel file.

1.10.4 Control System Inventory Reports

****

NOTE: Select whether the inventory report must include non-networked devices.

Unless specifically required by the project, keep the first bracketed text to require inventory of only networked devices and remove the later bracketed text requiring inventory of non-networked devices, input devices and output devices.

This subpart contains text that is only included when the USACE CW tailoring option is selected.

When the CW tailoring option is selected, "Inventory Spreadsheet" and "Hardware-Software List Template" will be in brackets. KEEP "Hardware-Software List Template" and REMOVE "Inventory Spreadsheet".

****

{For Government Reference Only: This subpart (and its subparts) relates to CM-8(a), SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a Pre-Construction Control System Inventory Report (Encrypted) report and a Final Control System Inventory Report (Encrypted), using the [Inventory Spreadsheet][Hardware-Software List Template] listed under this Section at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11. In the Control System Inventory Reports, document all [networked devices, including network infrastructure devices][devices, including networked devices, network infrastructure devices, non-networked devices, input devices (e.g. sensors) and output devices (e.g. actuators)], and all software. For each device provide all applicable information for which there is a field on the spreadsheet in accordance with the instructions on the spreadsheet.

In addition to the requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide the Control System Inventory Reports as editable Microsoft Excel files. Provide the Pre-Construction Control System Inventory Report concurrently with the Proposed STIG and SRG Applicability Report

1.10.5 System Data Flow Diagram (Encrypted)

****

NOTE: This subpart is included only when the USACE CW tailoring option is selected

****

Submit a system data flow diagram (encrypted) a minimum of 60 days prior to installed operation of the equipment. Provide diagrams electronically in PDF as well as either Microsoft Visio (VSDX) or Microstation (DGN), formatted for 11" x 17" sheets. Include:

a. All devices that communicate via routable protocols.

b. The normal system communications among the devices on the network, including the ports and protocols utilized for communications

c. Arrows to indicate direction of data flow between components. Define the physical media and protocol for each link.

d. Logical boundary of the system marked with a red line clearly defining components inside the boundary as well as components outside the boundary. Label connections to external networks and indicate the boundary protection.

e. Indicate VLAN segmentation of the devices on the diagram.

1.10.6 Software and Configuration Backups (Encrypted)

****

NOTE: This requirement covers disk images to allow recovery and reconstitution of applications on computers, and also covers program and configuration backups for controllers. As described in UFC 4-010-06 Cybersecurity for Facility-Related Control

Systems, as-built documentation (including copies of custom programming and device settings) must be required in the Section specifying the control system itself, but is included here in case that has not been done.

For MODERATE Impact Systems: Support of Information System Recovery and Reconstitution requires that the information system have spare parts available on site and that staff are properly trained in repair, recovery, and reconstitution of the system. Make sure the underlying controls spec has requirements in support of this requirement.

When the USACE CW tailoring option is selected, the requirement for the submittal to be on an encrypted external hard drive and the requirement to test the backup are included (and otherwise they are not).

****

{For Government Reference Only: This subpart (and its subparts) relates to CP-10; CCI-000550, CCI-000551, CCI-000552}

For each computer on which software is installed under this project, provide a recovery image of the final as-built computer on an encrypted external hard drive. This image must allow for bare-metal restore such that restoration of the image is sufficient to restore system operation to the imaged state without the need for re-installation of software. If additional user permissions are required to meet this requirement, coordinate the creation of the image with the identified Government Computer Access Point of Contact.

For all Ethernet switches provide a backup of the switch configuration. For all controllers, provide a backup of the controller configuration and the source code for all loaded application programs (all software that is not common to every controller of the same manufacturer and model).

Test backups to verify as functional for restoring the system prior to submittal. Include verification of testing and functionality with submittal. If any or all of these are provided under another Section, provide documentation indicating this and referencing those submittals.

1.10.7 Cybersecurity Network (Riser) Diagram (Encrypted)

****

NOTE: Select or specify the format for the riser diagram.

This subpart contains additional text when using the USACE CW tailoring option

****

{For Government Reference Only: This subpart (and its subparts) relates to PL-2(a), PL-8; CCI-003051, CCI-003053, CCI-003072, CCI-003073, CCI-003075}

Provide a cybersecurity network (riser) diagram of the complete control system including all network and device hardware. For each device,

include the device identifier, device type, and manufacturer. If the control system specifications require a riser diagram submittal, provide a copy of that submittal as the cybersecurity riser diagram. Otherwise, provide a riser diagram in [one-line format][one-line format overlayed on a facility schematic][tabular format][_____].

Provide diagrams electronically in Portable Document Format (PDF) as well as either Microsoft Visio (VSDX) or Microstation (DGN), formatted for 11" x 17" sheets.

1.10.8 STIG, SRG and Vendor Guide Compliance Result Report (Encrypted)

****
NOTE: Select whether SCAP or Evaluate-STIG is required.
****

For every component (device or software) with an applicable STIG or SRG in the Proposed STIG and SRG Applicability Report, document compliance with the STIG or SRG requirements.

a. For components which are scannable by [the SCAP (security content automation protocol) tool (available online at https://public.cyber.mil/stigs/scap), include the SCAP][the Evaluate-STIG tool (available online at (CAC Required), include the Evaluate-STIG] report and raw scan results in addition to the final, manually reviewed and revised, documentation of compliance with STIG and SRG requirements. Checklist files should not contain any findings with a Not Reviewed (NR) status after manual reviews.

b. For components which do not support automated scanning, a manual review using the General Purpose STIG option should be done. A completed Checklist file should not contain any findings with a Not Reviewed (NR) status after manual reviews

For every component (device or software) with manufacturer provided cybersecurity documentation, procedure, or method for secure configuration or installation, provide a report documenting how the component was configured and any deviation from the manufacturer instructions.

1.10.8.1 STIG, SRG and Vendor Guide Compliance Result Report Deviations List

****
NOTE: This subpart is only included when the USACE CW Tailoring Option is selected.
****

Within the STIG, SRG and Vendor Guide Compliance Result Report, include a Deviations List documenting all deviations required for system operation, and reasons why a STIG, patch, firmware update, or other requirement cannot be met. Include for each deviation:

a. STIG, SRG, Patch, Firmware Update, or other requirement being deviated

b. Vulnerability Identification

c. Rule Identification

d. Control

e. Control Correlation Identifier (CCI)

f. Finding

g. Justification

h. Current Risk-Mitigation Actions

1.10.9 Control System Cybersecurity Documentation

****
NOTE: The following enumerates very detailed requirements for documentation; requirements that would be impossible to meet for some control devices. The requirements are broken out in the sub paragraphs such as:
1) Requirements to be met by all software running on computers
2) Requirements to be met by HVAC control devices
3) Requirements to be met by Lighting Control System Devices
4) Requirements to be met by [fill in the blank] control devices
5) Default requirements for control system devices (when not covered in 1-4 above)

If the project incorporates devices other than HVAC or Lighting devices, and the general requirements in sub-paragraph 5 are not satisfactory, add requirements to subparagraph 4. If multiple different requirements are needed (e.g. the project incorporates a micro-grid and an electronic security system, both with specific requirements) add additional paragraphs similar to paragraph 4. Leave the "devices not otherwise covered" at the end of the list and do not edit those requirements.

Note that within HVAC and Lighting devices, a further distinction is made between devices that FULLY support accounts and those that do not. This distinction is a surrogate to account for the range of capabilities and complexity among various HVAC or Lighting control devices.
****

{For Government Reference Only: This subpart (and its subparts) relates to SA-5(a),SA-5(b),SA-5(c), SA-22(b); CCIs: CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131, CCI-003374}

Provide a Control System Cybersecurity Documentation submittal containing the indicated information for each device and software application.

1.10.9.1 Software Applications

For all software applications running on computers provide:

a. administrator documentation that describes secure configuration of the software {For Government Reference Only: relates to CCI-003124}

b. administrator documentation that describes secure installation of the software and software updates. {For Government Reference Only: relates to CCI-003125}

c. administrator documentation that describes secure operation of the software {For Government Reference Only: relates to CCI-003124}

d. administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software {For Government Reference Only: relates to CCI-003127}

e. administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software {For Government Reference Only: relates to CCI-003128}

f. user documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to CCI-003129}

g. user documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner {For Government Reference Only: relates to CCI-003130}

h. user documentation that describes user responsibilities in maintaining the security of the software {For Government Reference Only: relates to CCI-003131}

1.10.9.2 For HVAC Control System Devices

1.10.9.2.1 HVAC Control System Devices FULLY Supporting User Accounts

For all HVAC Control System Devices which FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003129}

f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.10.9.2.2 All Other HVAC Control System Devices

For all HVAC Control System Devices which do not FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}

c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.10.9.3 For Lighting Control System Devices

1.10.9.3.1 Lighting Control System Devices FULLY Supporting User Accounts

For all Lighting Control System Devices which FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003129}

f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.10.9.3.2 All Other Lighting Control System Devices

For all Lighting Control System Devices which do not FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}

c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

[1.10.9.4 [_____] Control System Devices

****
NOTE: Use this bracketed subpart if needed to add requirements for a specific control system type (e.g. lighting, electrical distribution etc.), similar to how HVAC and Lighting control system devices are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.
****

[_____]

]1.10.9.5 For USACE Civil Works Control System Devices

1.10.9.5.1 USACE Civil Works Control System Devices FULLY Supporting User Accounts

For all USACE Civil Works Control System Devices which FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

e. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms; or a specific indication that there are no user-accessible security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003129}

f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.10.9.5.2 All Other USACE Civil Works Control System Devices

For all USACE Civil Works Control System Devices which do not FULLY support user accounts, provide:

a. Documentation that describes secure configuration of the device; or a specific indication that there are no secure configuration steps that apply {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes effective use and maintenance of security functions or mechanisms for the device; or a specific indication that there are no security functions or mechanisms in the device {For Government Reference Only: relates to CCI-003127}

c. For devices which include a user interface, documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

1.10.9.6 Default Requirements for Control System Devices

****

NOTE: Do not edit these requirements (beyond selection of bracketed text). These default requirements should only be used in lieu of technology-specific requirements in the preceding paragraphs. If these default requirements are inappropriate, ensure that the preceding paragraphs provide appropriate technology-specific requirements.

****

For control system devices where Control System Cybersecurity Documentation requirements are not otherwise indicated in this Section, provide:

a. Documentation that describes secure configuration of the device {For Government Reference Only: relates to CCI-003124}

b. Documentation that describes secure installation of the device {For Government Reference Only: relates to CCI-003125}

c. Documentation that describes secure operation of the device {For Government Reference Only: relates to CCI-003124}

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {For Government Reference Only: relates to CCI-003127}

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device {For Government Reference Only: relates to CCI-003128}

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms {For Government Reference Only: relates to

CCI-003129}

g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner {For Government Reference Only: relates to CCI-003130}

h. Documentation that describes user responsibilities in maintaining the security of the device {For Government Reference Only: relates to CCI-003131}

i. Documentation of the published last date of support by the manufacturer or indication that a published date is not available. {For Government Reference Only: relates to CCI-003374}

1.11 SOFTWARE LICENSING

****

NOTE: The installation may procure its own software update licensing or contract and thus needs less than 5 years. Alternatively, the installation may require longer than five years (although this will likely increase the costs significantly). Coordinate with the installation to determine if they have any specific requirement; if they don't then keep the 5 year requirement.

Note that this requirement may already exist in the control system specifications, in which case it can removed from this Section (or kept in this Section and removed from the control system specification).

****

{For Government Reference Only: This subpart (and its subparts) relates to SI-2(a), SI-2(c), SI-7(14); CCI-001227, CCI-002605, CCI-002737}

For all software provided that has not already been licensed to the government or project site, provide a license to the [Government][project site][_____] for a period [of no less than 5 years][___], and the license must also include the following software updates:

a. Security and bug-fix patches issued by the software manufacturer.

b. Security patches to address any vulnerability identified in the National Vulnerability Database at http://nvd.nist.gov with a Common Vulnerability Scoring System (CVSS) severity rating of MEDIUM or higher.

Provide a single Software Licenses submittal with documentation of the software licenses for all software provided

1.12 CYBERSECURITY DURING CONSTRUCTION

****

NOTE: The requirements in this subpart do not tie to cybersecurity specific cybersecurity controls or CCIs as tightly as most other requirements in this Section. They are included to provide a basic level of "cyber hygiene" during the construction process, and the controls that they are related to are still

noted for reference.

These requirements are not related to the networks contractors will often establish in their project offices/trailers. They are specific to temporary networks used by the control system during installation. For example, a wireless access point set up in a mechanical room to allow construction personnel laptops to access the control system during construction before the building IT infrastructure is operational..

****

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, CA-3; CCI-000258}

In addition to the control system cybersecurity requirements indicated in this section, meet following requirement throughout the construction process.

1.12.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. Contractor computers connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.12.1.1 Operating System

The operating system must be an operating system currently supported by the manufacturer of the operating system. The operating system must be current on security patches and operating system manufacturer required updates.

1.12.1.2 Anti-Malware Software

The computer must run anti-malware software from a reputable software manufacturer. Anti-malware software must be a version currently supported by the software manufacturer, must be current on all patches and updates, and must use the latest definitions file. Computers used on this project must perform a full antivirus scan at least once per day. Computers which have connected to any other network since the last full antivirus scan must perform a full antivirus scan prior to connection to the control system network or to the temporary contractor-installed IP network. Perform an antivirus scan on all removable media (e.g., external hard drives, CDs, DVDs, USB flash drives) prior to connecting to the control system environment.

1.12.1.3 Passwords and Passphrases

The passwords and passphrases for computers, applications, and web-based applications supporting passwords must be changed from their default values. Passwords must be a minimum of eight characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.12.1.4 User-Based Authentication

Each user must have a unique account; sharing of a single account between

multiple users is prohibited.

1.12.1.5 Firewall

****
NOTE: This subpart is only included when the USACE CW Tailoring Option is selected
****

Computers must have a firewall enabled and set to "public".

1.12.1.6 Encryption

****
NOTE: This subpart is included only when the USACE CW Tailoring Option is selected
****

Employ data-at-rest encryption to protect information stored on the device. The types of information that must be protected include site specific drawings, configuration files, project files, vulnerability data, and any other specific information that could potentially lead to a compromise. Immediately notify the Contracting Officer in the event that a Contractor-owned computer that stores this information is lost or stolen.

1.12.1.7 Demonstration of Compliance

The Government has the right to require demonstration of computer compliance with these requirements at any time during the project.

1.12.1.8 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers. Contractor Computer Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.12.2 Temporary IP Networks

****
NOTE: The allowance of connection to "Government furnished IP networks provided for this purpose" covers the case of there being a "guest" network the contractor can use. This is likely not available in many cases, but is covered here for the instances in which it is offered by the project site.
****

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks connected to the control system, control system network, or a control system component at any point during construction must meet the following requirements:

1.12.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect

to any IP network other than those specifically provided or furnished for this project. Any and all access to the network from outside the project site is prohibited.

1.12.3 Government Access to Network

Government personnel must be allowed to have complete and immediate access to the network at any time in order to verify compliance with this specification.

1.12.4 Temporary Wireless IP Networks

****
NOTE: For USACE Civil Works Projects, wireless networks are not permitted. When the USACE Civil Works Tailoring Option is selected, the text concerning the use of wireless networks will be in brackets, and the statement prohibiting them will be added.

For USACE Civil Works projects, remove the bracketed text.
****

[In addition to the other requirements on temporary IP networks, temporary wireless IP (WiFi) networks, when permitted, must not interfere with existing wireless networks, must use WPA2 security and must not broadcast the network name (SSID). Network names (SSID) for wireless networks must be changed from their default values.]

Temporary wireless networks are NOT PERMITTED.

1.12.5 Passwords and Passphrases

The passwords and passphrases for all network devices and network access must be changed from their default values. Passwords must be a minimum 8 characters with a minimum of one uppercase letter, one lowercase letter, one number and one special character.

1.12.6 Contractor Temporary Network Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Temporary Network Cybersecurity Compliance Statements for each company implementing a temporary IP network. Contractor Temporary Network Cybersecurity Compliance Statements must use the template published at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11. Each Statement must be signed by a cybersecurity representative for the relevant company. If no temporary IP networks will be used, provide a single copy of the Statement indicating this.

1.13 CYBERSECURITY DURING WARRANTY PERIOD

All work performed on the control system after acceptance must be performed using Government Furnished Equipment or equipment specifically and individually approved by the Government.

PART 2 PRODUCTS

****
NOTE: The product requirements of this Section are

the minimum requirements necessary to meet the cybersecurity requirements of this Section, and add to the product requirement specified in the control system specifications. Components (Network media, switches, routers, firewalls, controllers, computers, software etc.) must be specified in the control system specifications, and submittals for those components must be included in those Sections as this Section does not contain separate submittals for these products.

****

All products used on this project must meet the indicated requirements, but not all products specified here will be required by every project.

2.1 ETHERNET SWITCH

Provide Open Systems Interconnection (OSI) Layer 2 Ethernet switches with the following capabilities, and with an interface to support switch configuration for these capabilities:

2.1.1 Required Functionality

****

NOTE: Include bracketed options which correspond to required switch functionality, and change bullet letters accordingly. Determine functionality in coordination with the system owner organization and do not include any requirements that are not specifically needed.

Use particular caution in requiring IEEE 802.1x as most controllers will not support it.

****

Switches must:

a. Copper Ethernet ports must auto negotiate for 10, 100 and 1000 megabits-per-second links.

b. Be capable of implementing port level access control by MAC address and limit the number of MAC addresses to one MAC address per port.

c. For MODERATE Impact Systems, be capable of implementing per-port access control lists (ACLs) where the list can be filtered by source and destination IP addresses, and by source and destination UDP or TCP ports.[

c. For LOW Impact Systems, be capable of implementing per-port access control lists (ACLs) where the list can be filtered by source and destination IP addresses, and by source and destination UDP or TCP ports.][

d. Support Remote Network Monitoring (RMON) Port Analysis in accordance with IETF RFC 2819][

e. Configure target port and analysis port such that switch clones all target port traffic to analysis port.][

f. Support authentication via RADIUS server (for management and 802.1x)][

g. Support IEEE 802.1x network login.]

2.1.2 Configuration Requirements

****
NOTE: Coordinate with the system owner organization to determine if the capability to lock to a dedicated management port is required, and include or remove bracketed text requiring this as needed.
****

Switches must:

a. Support configuration save and restore.

b. Support both manual IP address assignment and acquisition of a dynamic IP address via Dynamic Host Configuration Protocol (DHCP).

c. Be capable of limiting access for configuration to one or more of: a web interface using HTTPS, a command line interface using SSH, or an SNMP connection using SNMP version 3 or later.[

d. Support the ability to lock configuration capability to a dedicated management port.]

2.2 DAISY CHAIN IP CONTROLLERS

Controllers used as Daisy Chain IP Controllers must be IP controllers with exactly two Ethernet network connections and basic built-in switch capabilities to allow implementation of an Ethernet network in a daisy chain architecture. Switches incorporated by Daisy Chain IP Controllers are not required to meet the requirements for Ethernet Switches as defined in this Section.

2.3 DATABASE AND WEB SERVER SOFTWARE FOR MODERATE IMPACT SYSTEMS

****
NOTE: Indicate the permitted database and web servers.
****

{For Government Reference Only: This subpart (and its subparts) relate to RA-5(1), RA-5(5); CCI-001062, CCI-001067, CCI-001645, CCI-002906}

All computer-based databases must use [Microsoft SQL Server][or][Oracle][or][MySQL]. All computer-based web interfaces must use [Internet Information Services (IIS)][or][Apache] as the web server.

2.4 Lockable Enclosures with Padlock

****
NOTE: This subpart is only included when the USACE CW tailoring option is selected.
****

Provide lockable enclosures with lockable handles, doors, or accessories allowing the cabinet to be secured using a padlock. Provide a stainless

steel padlock with a minimum of a 3/8-inch diameter hardened shackle for each enclosure.

PART 3 EXECUTION

3.1 CYBERSECURITY HARDENING AND CONFIGURATION GUIDES

Install, configure, and harden all hardware and software furnished on this project in accordance with manufacturer provided documentation, procedures, or methods for secure configuration or installation. Configure hardware and software in accordance with the applicable STIGs and SRGs per the STIG and SRG applicability report. Install the most current versions of operating systems, software updates, firmware updates, security patches, service packs, and BIOS/UEFI, unless otherwise specified or approved. Do not implement specific hardening actions if that action would conflict with required functionality or another requirement of this Section.

3.2 NETWORK REQUIREMENTS

3.2.1 Information Flow Enforcement In MODERATE Impact Systems

****

NOTE: For non-IP networks (In MODERATE Impact Systems), ensure that the control specifications require that those networks limit traffic to that required for the control system.

****

{For Government Reference Only: This subpart (and its subparts) relate to AC-4; CCI-001368, CCI-001414, CCI-001548, CCI-001549, CCI-001550, CCI-001551}

Install and configure Ethernet switches to block all traffic on all ports not required by the control protocol.

3.2.2 Wireless and Wired Broadcast Communication for Fire Protection Systems

****

NOTE: Indicate whether the communication from a facility fire protection system to the central monitoring station must meet FIPS 140-2. Coordinate this requirement with the project site, and if the existing system does not use FIPS certified radios and it is not certain the existing system is able to employ FIPS certified radios DO NOT include this requirement.

Note that mitigation measures for non-FIPS 140-2 radios are covered in "Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems"

****

The use of wireless and wired broadcast communication for fire protection systems within a facility is prohibited. Wireless communication may be used to provide communication from the fire protection system in a facility to the central monitoring station. [Communication between the fire protection system and the central monitoring station must be via FIPS 140-2 certified devices.]

[3.2.3 Wireless and Wired Broadcast Communication for Systems Other than Fire Protection Systems

****
NOTE: When the FIRE PROTECTION tailoring options is selected, this subpart is in brackets. If this specification is only for fire protection systems remove this subpart. If this specification includes requirements for other systems, keep this subpart.
****

****
NOTE: Avoid wireless and wired broadcast networks to the greatest extent possible. Wireless may be considered for retrofits where running wires would be prohibitive. While powerline carrier should be avoided where possible, it (and other wired broadcast networks) are likely more secure than wireless and should be considered as a potential alternative to cases where wireless seems unavoidable. If the site has a clear preference for non-wireless broadcast (e.g. powerline or similar) over wireless, include the bracketed text.

In general, contractors should never install a wireless network which carries the IP protocol. The Air Force may allow wireless IP networks to be installed in some instances, when it is installed in accordance with existing site requirements - coordinate with the project site to determine if this is required and remove the bracketed text if not required.

Note that contractors may (where permitted and supported) USE a government provided wireless IP network.
****

{For Government Reference Only: This subpart (and its subparts) relates to AC-18, AC-18(3); CCI-001438, CCI-001439, CCI-002323, CCI-001441, CCI-001449}

Unless explicitly authorized by the Government, do not use any wireless or wired broadcast communication. [If requesting authorization for wireless or wired broadcast communication, wired broadcast media such as powerline carrier is preferred to wireless.]

3.2.3.1 Wireless and Wired Broadcast IP Communications

[Unless specifically approved and installed in accordance with the project site requirements,]Do not install wireless or wired broadcast IP networks, including: do not install a wireless access point; do not install or configure an ad-hoc wireless network; do not install or configure a WiFi Direct communication.

When explicitly authorized by the Government, wireless IP communication may be used to communicate with an existing wireless network.

3.2.3.2 Non-IP Wireless Communication

****
NOTE: Note that the MODERATE requirement for FIPS 140-2 may effectively prohibit the use of non-IP wireless. This is intentional, for MODERATE Impact systems wireless encryption is required.
****

For LOW Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, use the maximum level of encryption supported by the specific protocol employed and select signal strength and radiated power to the minimum necessary for reliable communication.

For MODERATE Impact Systems: When non-IP wireless communication is explicitly authorized by the Government, the radios must meet NIST FIPS 140-2 Level 2.

3.2.3.3 Wireless and Wired Broadcast Communication Request

****
NOTE: The Wireless and Wired Broadcast Communication Request submittal will be used to authorize specific use of wireless communication, and to indicate whether or not testing of the signal strength is required. In general, testing is not required for a LOW impact system.

There may be project site or Service policies that govern the use of wireless. Before authorizing wireless use coordinate with the relevant Service and project site representatives.
****

Provide a report documenting the proposed use of wireless or wired broadcast communication prior to device selection using the Wireless and Wired Broadcast Communication Request Schedule at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11. If there is no proposed use of wireless or wired broadcast communication, provide a document indicating this instead of the Request Schedule.

For each device proposed to use wireless or wired broadcast communication show: the device identifier, a description of the device, the location of the device, the device identifiers of other devices communicating with the device, the protocol used for communication, encryption type and strength. For wireless communication, also show: RF Frequency, Radiated Power in dBm (decibel with a milliwatt reference), free-space range, and the expected as-installed range.

3.2.3.4 Wireless Communication Testing

****
NOTE: Select or enter appropriate name for the system-level test of the control system.

Select or indicate the wireless network test boundary.
****

As part of [Performance Verification Testing (PVT)][Functional Performance Testing {FPT}][_____], conduct testing of wireless communication for all devices indicated on the approved Wireless and Wired Broadcast Communication Request as requiring testing.

To test wireless communication, test for wireless network reception at multiple points along the wireless test boundary in the vicinity of the wireless device, and record whether a network connection can be established at each point. The wireless test boundary is [the building exterior walls][the facility fence line][_____]. If wireless testing is required, provide a Wireless Communication Test Report documenting the testing points and results at each point for each wireless device.

]3.2.4 Non-IP Control Networks

When control system specifications require particular communication protocols, use only those communication protocols and only as specified. Do not implement any other communication protocol.

When control system specifications do not indicate requirements for communication protocols, use only those protocols required for operation of the system as specified.

3.2.5 IP Control Networks

{For Government Reference Only: This subpart relates to CM-6(a), CM-7(a), CM-7(b), CM-7(1)(b), SC-41; CCI-001588, CCI-000381, CCI-000380, CCI-000381, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For Moderate Impact Systems, this subpart (and its subparts) also relates to SC-5(1), SC-5(2); CCI-001094 CCI-001095}

IP Networks must be Ethernet networks and must use switches which are Ethernet Switches or Daisy Chain IP Controllers as defined in this Section. Do not use nonsecure functions, ports, protocols and services as defined in DODI 8551.01 unless those ports, protocols and services are specifically required by the control system specifications or otherwise specifically authorized by the Government. Do not use ports, protocols and services that are not specified in the control system specifications or required for operation of the control system.

For MODERATE Impact Systems, unless explicitly authorized, do not use IP networks if the same control functionality is available through the use of non-IP networks.

3.2.5.1 IP Network Routers

****

NOTE: This subpart is only included when the USACE CW tailoring option is selected.

For USACE systems, coordinate with the UCIC MCX to identify and coordinate IP routing requirements for the specified control system. Depending upon the type of system, routing may be required.

If routing is required, keep the first bracketed text and edit the requirements accordingly.

If routing is not required, keep the second

bracketed text.
****

[For IP-based communications across control systems, use Routers to control and restrict traffic flow between network and virtual local area network (VLAN) traffic. Configure routers using Access Control Lists (ACLs) using a deny-all, permit by exception approach. When network traffic is within the local perimeter use Traditional Network Routers. When network traffic leaves the local perimeter, use Integrated Service Routers (ISR) or Firewalls with VPN capability instead.]

[Do not install any device that performs IP routing.]

3.2.5.2 IP Devices With Multiple Ethernet Connections

****
NOTE: Some cases where devices with multiple IP connections might be desired or required as part of the control system design are:

1) Use of a field device with two Ethernet ports to separate the upstream (base-wide) network from the building network. This device lives on two separate networks and - while maintaining network separation - passes control data between the two different networks.

2) Use of a front end with two network cards to separate the control network from the operator interface network. Like the field device, this front end resides on two separate networks and passes control data from the control system to operator interfaces and commands from operator interfaces to the control system.

****

Except for Ethernet Switches and Daisy Chain IP Controllers, devices must not have more than one Ethernet connection to IP networks unless doing so is required by the project specifications and the specific application is approved. If a device with Multiple Ethernet Connections to IP networks is required, provide a Multiple Ethernet Connection Device Request using the Multiple Ethernet Connection Device Request Template at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-05-11 to request approval for each device. If a device with Multiple Ethernet Connections to IP networks is not required, instead provide a document stating that no approval is being requested.

3.2.6 Cryptographic Protection

****
NOTE: HTTPS is a form of cryptographic protection and hence is included here for all cases.

In general, additional cryptographic requirements should be avoided, or at least minimized. (Note that even for systems where cryptography is required, it may not be required at every node and interconnection in the system.)

With regard to other cryptography, there are 3 possibilities to consider:
1. The control system contains no classified information and cryptography has not been specifically required by the Authorizing Official. In that case, there are no UFGS requirements and this Subpart should be removed.
2. The control system contains no classified information, but the Authorizing Official has determined that cryptography is required. Select text requiring cryptography.
3. The control system contains classified information. First, confirm that the system truly needs to contain classified information - if this is only to fulfil some reporting requirement, consider removing the information from the CS and meeting the reporting requirement via some other means. If the requirement for cryptography cannot be eliminated, select text requiring cryptography.

Keep bracketed text only when cryptography is required. If cryptography is required, select whether to require it everywhere, only on the IP network, or only at specific locations within the system. Note that some systems will not support cryptography even at the IP level, and most systems will not support the use of cryptography at non-IP devices.
****

{For Government Reference Only: This subpart relates to IA-2(9), IA-3(1), SC-8, SC-13, SC-23(1), SC-23(3); CCI-001942, CCI-001959, CCI-001967, CCI-002418, CCI-002449, CCI-002450, CCI-001185, CCI-001188, CCI-001664.}

All remote user interfaces must use HTTPS for all traffic between the user interface client and user interface server.[

For devices that have STIG/SRGs related to cryptographic protection (CCI-002450), comply with the requirements of those STIG/SRGs. Ensure that [all][IP][_____] network traffic is encrypted using NSA-approved cryptography; provision of digital signatures and hashing, and FIPS-validated cryptography.]

3.2.6.1 Additional Cryptographic Protection Requirements for USACE Civil Works Systems

****
NOTE: This subpart is only included when the USACE CW tailoring option is selected.

When included through the USACE CW tailoring option, determine the need for this subpart and include only if needed, revising to meet project requirements.
****

Protect the following communications using NIST FIPS 140-2 compliant encryption methods:

a. Public switched telephone network

b. Leased lines

c. Any wireless communication

Establish Virtual Private Network IPSec tunnels between different facilities and between wireless devices. Provide firewalls to control communications between tunnels. Firewalls must meet STIG requirements. Network and wireless devices must be on the DISA approved product list (APL). See https://aplits.disa.mil/processAPList.

3.2.7 Device Identification and Authentication

****
NOTE: If site required use of IEEE 802.1x, keep bracketed text requiring its implementation. Otherwise remove bracketed text.
****

{For Government Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958. For MODERATE Impact systems, this subpart (and its subparts) also relates to SC-23, SC-23(5); CCI-001184, CCI-002470.}

All computers must support [and implement]IEEE 802.1x for device authentication to the network.

3.2.7.1 For HVAC Control System Devices

****
NOTE: If widely supported or specifically required by the project site, keep the bracketed text requiring Ethernet devices to meet 802.1x. Note many IP-based controllers do not support 802.1x, so only include this requirement if confident it can be sufficiently supported or if it is a specific project requirement.

Unless the project site specifically indicates that 802.1x is not a requirement, keep the bracketed text requiring Fox Protocol components to support 802.1x.

Do not require network security with BACnet (BACnet Secure Connect) without determining both a) that it is a specific project requirement, and b) that it can be met by multiple vendors.
****

Devices using HTTP as a control protocol must use HTTPS instead. [Devices using Ethernet must support IEEE 802.1x.][Devices using Fox Protocol must support IEEE 802.1x.][Devices using BACnet must support network security as specified for BACnet Secure Connect in ASHRAE 135.]

3.2.7.2 For Lighting Control System Devices

****
NOTE: If widely supported or specifically required by the project site, keep the bracketed text requiring Ethernet devices to meet 802.1x. Note

many IP-based controllers do not support 802.1x, so only include this requirement if confident it can be sufficiently supported or if it is a specific project requirement.

Unless the project site specifically indicates that 802.1x is not a requirement, keep the bracketed text requiring Fox Protocol components to support 802.1x.

Do not require network security with BACnet (BACnet Secure Connect) without determining both a) that it is a specific project requirement, and b) that it can be met by multiple vendors.

****

Devices using HTTP as a control protocol must use HTTPS instead. [Devices using Fox Protocol must support IEEE 802.1x.][Devices using Ethernet must support IEEE 802.1x.][Devices using BACnet must support network security as specified for BACnet Secure Connect in ASHRAE 135.]

3.2.7.3 [_____] Control System Devices

****

NOTE: Use this subpart if needed to add requirements for a specific control system type (e.g. electrical distribution etc.), similar to how HVAC and Lighting control system devices are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.

****

[_____]

3.2.7.4 Default Requirements for Control System Devices

****

NOTE: Do not edit these requirements (beyond selection of bracketed text). These default requirements should only be used in lieu of technology-specific requirements in the preceding paragraphs. If these default requirements are inappropriate, ensure that the preceding paragraphs provide appropriate technology-specific requirements.

If widely supported, require Ethernet devices to meet 802.1x. Note many IP-based controllers do not support 802.1x, so only include this requirement if confident it can be sufficiently supported or if it is a specific project requirement.

****

For control system devices where Device Identification and Authentication requirements are not otherwise indicated in this Section: [Devices using Ethernet must support IEEE 802.1x.]Devices using HTTP as a control protocol must use HTTPS instead.

3.2.8 Cryptographic Module Authentication

{For Government Reference Only: This subpart (and its subparts) relates to IA-7; CCI-000803}

For devices (including but not limited to NIST FIPS 140-2 compliant radios) that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.2.9 Secure Network Design

****
NOTE: This subpart is only included when the USACE CW Tailoring Option is selected.
****

Provide network segmentation for networks leaving a local physical boundary, containing multiple types of systems (such as control and electronic security systems), or controlling more than one process that does not require direct communication of the control system components amongst discrete processes. Dual-homed hosts are prohibited. Protect external connections to the outside with a router, firewall, VPN, and IDS.

Network Interface Cards (NICs) or network transceivers are considered to be network connected regardless of network protocol used. Unused NICs must be disabled. A device is considered to be wireless network connected unless the wireless network controller is physically disabled. It is not sufficient to disable the wireless NIC in settings.

3.2.10 OT Monitoring System (OTMS)

****
NOTE: This subpart is only included when the USACE CW Tailoring Option is selected.

Coordinate with the UCIC MCX to determine if monitoring will be implemented as part of the design. If monitoring is required, keep this subpart and edit to meet project requirements. Otherwise, remove this subpart during bracket replacement.
****

Provide provide [1 rack unit][2 rack units][[_____]rack units] of rack space for data taps to be furnished, installed, and configured by the Government.

3.3 ACCESS CONTROL REQUIREMENTS

3.3.1 User Accounts

****
NOTE: Ensure that control system specifications define roles (such as operator with view-only, operator with control, control system admin) for applications which FULLY support accounts. Different devices, particularly those with very different functions and residing at different places

in the system architecture, may require different account roles.

The determination of whether a device has a STIG or SRG, and the installation and configuration of devices in accordance with relevant STIGs or SRGs are contractor responsibilities. The designer/specifier is not expected to identify relevant STIGs or SRGs

****

{For Government Reference Only: This subpart (and its subparts) relate to AC-2(a), AC-3, AC-6(1), AC-6(10), AC-6(2), AC-6(9), CM-11(2), and IA-2; CCI-002110, CCI-000213, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-001812, and CCI-000764. For MODERATE Impact systems, this subpart (and its subparts) also relate to AC-2 (2), AC-2(3), AC-2(4), AC-6(1), and CM-5(1); CCI-001361, CCI-000017, CCI-000217, CCI-000018, CCI-001403, CCI-001404, CCI-001405, CCI-002130, CCI-001683, CCI-001684, CCI-001685, CCI-001686, CCI-002132, CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-001813.}

Any user interface supporting user accounts (either FULLY or MINIMALLY) must limit access according to specified limitations for each account. Install and configure any device having a STIG or SRG in accordance with that STIG or SRG.

All user interfaces FULLY supporting accounts must implement user-based authentication where each account is uniquely assigned to a specific user. User interfaces FULLY supporting accounts must implement at least three (3) levels of user account privilege including: 1) an account with read-only permissions 2) an account with full permissions including account creation and modification and 3) an account with greater permissions than read-only but without account creation and modification. Disable any unnecessary or unused accounts. Disable any "guest-level" accounts that are created on the system by default.

3.3.1.1 Computers

All computer operating systems must FULLY support user accounts and implement accounts for access. Each control system software application not supporting accounts and running on a computer must be installed such that use of the software is restricted by the computer operating system to specific users.

Applications running on computers must not require the user be logged in to a computer operating system administrator account for normal operation. It is permissible to require the computer operating system administrator account for initial application installation and configuration.

3.3.1.1.1 User Account Levels

****

NOTE: This Subpart is only included when the USACE CW tailoring option is selected.

****

Configure OT using three account access levels: operator level, service

level, and administration level. Configure normal operations to occur using an operator level account. Configure the operator level with minimum privileges required to operate the system that does not allow for configuration changes. Disable removable media devices and USB ports (with the exception of keyboard and mouse) for all levels except the administrator level. Submit an Account Level Permissions List (Encrypted) documenting the names all levels and which permissions are allowed for each level.

3.3.1.2 Controllers

****

NOTE: Note from the definition of Privileged User Interface: "In general however, user interfaces that do not offer significant capabilities above and beyond those available at that location via other means (e.g. such as a disconnect switch, breaker, or hand-off-auto switch, or physical attack) are not privileged."

For ESS, we assume that there is a possibility of sensitive information (either security or PII) being displayed.

The notes below provide guidance on how to select the appropriate requirement where a choice is given. Do not use guidance in this note to alter entries where no designer option is given.

Local Read Only UI:
For ESS, discuss with the project site to determine whether to require a key lock or to require at least MINIMAL support of accounts. For non-ESS, unless specifically requested by the site, select NONE (not required to support accounts).

Local Limited UI, Non-Privileged:
Unless specifically requested by the site, select None Required.

Local Limited UI, Privileged:
For LOW impact ESS, discuss with the project site to determine whether to allow a key lock along with at least MINIMALLY supporting accounts, or whether to require FULL support of accounts. For LOW impact non-ESS, unless specifically requested by the site, select MINIMALLY. For MODERATE systems, use great care before requiring FULL support of accounts as these interfaces may be difficult to obtain. Entries of “KEY and Physical Security” (or “MINIMALLY and Physical Security") are there as a reminder: This is an important function and everything associated with it, including the controlled equipment, should be protected by physical security in addition to other safeguards.

Local Full UI:
Verify that interfaces FULLY supporting accounts are available before selecting FULLY (requiring FULL support of accounts).

Remote Read Only UI:
For ESS, discuss with the project site to determine if there are any confidentiality issues associated with the interface. For non-ESS, unless specifically requested by the site, select None Required

****

For user interfaces provided by controllers, provide access control in accordance with the User Interface Requirements table for the applicable control system and user interface type.

a. For table entries of "NA": NA means Not Applicable, there are no interfaces in this category.

b. For table entries of "None Required": The user interface is not required to support user accounts.

c. For table entries of "MINIMALLY": The user interface must at least MINIMALLY support user accounts.

d. For table entries of "FULLY": The user interface must at FULLY support user accounts.

e. For table entries of "KEY": The user interface must have physical security in the form of either a key lock on the interface itself or be furnished inside a lockable enclosure. Where this is required for a read only interface, the lockable enclosure must prevent viewing of data on the interface; for other interfaces, this lockable enclosure must prevent using the interface to alter data.

f. For table entries of "Physical Security": For Local FULL interfaces, the interface must be located inside mission space. For Local Limited (not FULL) interfaces, the user interface must either a) be located within mission space or b) be protected by physical security at least as good as the control devices (and equipment controlled by the control devices) affected by the interface. For purposes of this requirement, 'affected' includes controllers with data that can be directly altered by the interface, as well as mechanical and/or electrical equipment directly controlled by those controllers, but does not include other interactions.

g. Entries of the form "X and Y" must meet both the requirement indicated for X and the requirement indicated for Y. For example, an entry of "MINIMALLY and Physical Security" indicates the user interface must both MINIMALLY support accounts and have physical security.

h. Entries of the form "X or Y" must meet either the requirement indicated for X or the requirement indicated for Y.

3.3.1.2.1 HVAC Control Systems

User Interface Requirements for LOW Impact HVAC Control Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY][Physical Security]
Local Full	MINIMALLY
Remote Read Only	None Required
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

User Interface Requirements for MODERATE Impact HVAC Control Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY and Physical Security][FULLY]
Local Full	MINIMALLY and Physical Security
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2.2 Lighting Control Systems

User Interface Requirements for LOW Impact Lighting Control Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY][Physical Security]
Local Full	MINIMALLY
Remote Read Only	None Required
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

User Interface Requirements for MODERATE Impact Lighting Control Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY and Physical Security][FULLY]
Local Full	MINIMALLY and Physical Security
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2.3 Electronic Security Systems (ESS)

User Interface Requirements for LOW Impact Electronic Security Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	[KEY][MINIMALLY]
Local Limited, Non-privileged	NA
Local Limited, Privileged	[MINIMALLY and KEY][FULLY]
Local Full	FULLY and Physical Security
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	NA
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

User Interface Requirements for MODERATE Impact Electronic Security Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only (see note 1)	[KEY][MINIMALLY]
Local Limited, Non-privileged	NA
Local Limited, Privileged	FULLY
Local Full	FULLY and Physical Security
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	NA
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2.4 Fire Protection Systems

User Interface Requirements for LOW Impact Fire Protection Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	None Required
Local Limited, Non-privileged	[None Required][KEY or MINIMALLY]
Local Limited, Privileged	KEY and Physical Security
Local Full	KEY
Remote Read Only	None Required
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged	

User Interface Requirements for MODERATE Impact Fire Protection Systems	
User Interface Type	**Access Control Requirement**
Local Read Only	None Required
Local Limited, Non-privileged	[None Required][KEY or MINIMALLY]
Local Limited, Privileged	[KEY and Physical Security][FULLY]
Local Full	KEY
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2.5 USACE Civil Works Control Systems

****

NOTE: This subpart is only included when the USACE CW tailoring option is selected

Typical Civil Works (CW) OT devices (e.g. PLCs,

meters, relays, etc.) do not have a local user interface. Adjust interface requirements for device type, application, and manufacturer-specific features.

For a CW Control System that utilizes a programmable logic controller (PLC), it is assumed that it can only provide the local read only interface and all other local interfaces are not applicable. The designer must edit the table and notes to ensure that all other local interfaces cannot be provided. With a PLC the local read only interface is likely limited to a few single or multi-color LEDs or an alpha-numeric display.

A Remote Full interface for the PLC system is assumed to be a programming PC, an operator interface terminal (touch panel) or human machine interface software running on a PC.

The Designer must determine whether a Remote Read Only interface is required for the application, although this could be implemented in the Remote Full interface based on user account permissions.

The user interface requirements table is different from the operational schemes used as part of USACE Civil Works Operational Technology. For example, the Remote Full user interface can be used to implement local or campus operation and does not necessarily indicate remote (offsite) operation of the facility.

****

User Interface Requirements for LOW Impact USACE Control Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	KEY
Local Limited, Non-privileged	[(see note 3)][MINIMALLY]
Local Limited, Privileged	[(see note 3)][MINIMALLY][Physical Security]
Local Full	[(see note 3)][NA]
Remote Read Only	[(see note 3)][FULLY]
Remote Limited, Non-Privileged	NA
Remote Limited, Privileged	NA
Remote Full (see note 2)	FULLY

User Interface Requirements for LOW Impact USACE Control Systems	
User Interface Type	**Access Control Requirement**
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged [3)Device or system should not be capable of providing the interface type, otherwise notify the COR]	

User Interface Requirements for MODERATE Impact USACE Control Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only	KEY
Local Limited, Non-privileged	[(see note 4)][MINIMALLY]
Local Limited, Privileged	[(see note 4)][MINIMALLY and Physical Security]
Local Full	[(see note 4)][NA]
Remote Read Only	[(see note 4][FULLY]
Remote Limited, Non-Privileged	NA
Remote Limited, Privileged	NA
Remote Full	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS") [4) Device or system should not be capable of providing the interface type, otherwise notify the COR]	

3.3.1.2.6 [_____] Control Systems

****

NOTE: Use this subpart if needed to add requirements for a specific control system type (e.g. electrical distribution etc.), similar to how other control systems are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.

****

User Interface Requirements for LOW Impact [_____] Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	[_____]
Local Limited, Non-privileged	[_____]
Local Limited, Privileged	[_____]
Local Full	[_____]
Remote Read Only	[_____]
Remote Limited, Non-Privileged	[_____]
Remote Limited, Privileged AND Remote Full (see note 2)	[_____]
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

User Interface Requirements for MODERATE Impact [_____] Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only	[_____]
Local Limited, Non-privileged	[_____]
Local Limited, Privileged	[_____]
Local Full	[_____]
Remote Read Only	[_____]
Remote Limited, Non-Privileged	[_____]
Remote Limited, Privileged AND Remote Full (see note 2)	[_____]

User Interface Requirements for MODERATE Impact [_____] Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.2.7 Default Requirements for Other Control Systems

****

NOTE: Do not edit these requirements (beyond selection of bracketed text). These default requirements should only be used in lieu of technology-specific requirements in the preceding paragraphs. If these default requirements are inappropriate, ensure that the preceding paragraphs provide appropriate technology-specific requirements.

****

For control system devices where User Interface Requirements are not otherwise indicated in this Section, use the Default User Interface Requirements tables.

Default User Interface Requirements for LOW Impact Control Systems	
User Interface Type	**Access Control Requirement**
Local Read Only (see note 1)	[None Required][MINIMALLY]
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY][Physical Security]
Local Full	[MINIMALLY][FULLY]
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	MINIMALLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY

Default User Interface Requirements for LOW Impact Control Systems	
User Interface Type	**Access Control Requirement**
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged	

Default User Interface Requirements for MODERATE Impact Control Systems	
User Interface Type	**Access Control Requirement** (See note 3)
Local Read Only (see note 1)	[None Required][MINIMALLY]
Local Limited, Non-privileged	[None Required][MINIMALLY]
Local Limited, Privileged	[MINIMALLY and Physical Security][FULLY]
Local Full	[MINIMALLY and Physical Security][FULLY]
Remote Read Only	[None Required][MINIMALLY]
Remote Limited, Non-Privileged	FULLY
Remote Limited, Privileged AND Remote Full (see note 2)	FULLY
Notes: 1)Local Read Only User Interfaces are always Non-Privileged 2)Remote Full User Interfaces are always Privileged 3)Devices outside mission space require physical security protections as indicated (in "PHYSICAL SECURITY IN MODERATE IMPACT SYSTEMS")	

3.3.1.3 Additional User Account Expiration Requirements In MODERATE Impact Systems:

In addition to other user account requirements, user account expiration and auditing must be configured as indicated.

3.3.1.3.1 For Control System Applications Running on Computers

If temporary accounts are supported, expire temporary accounts 72 hours after creation. Expire all other accounts after 35 days of inactivity.

3.3.1.3.2 For Other Control System Devices FULLY Supporting Accounts

If temporary accounts are supported, expire temporary accounts 72 hours after creation. Expire all other accounts after 365 days of inactivity.

3.3.2 Unsuccessful Logon Attempts

****

NOTE: Note that most field devices that only MINIMALLY support accounts (e.g. a Local Display

Panel) cannot be locked. Keep the bracketed text requiring that these devices lock ONLY if this is a specific project requirement. If keeping this text, include requirements on when the interface must lock and how to unlock. Some unlocking conditions to consider are: network command or a physical button which is protected by a locked enclosure.

Note that a requirement for a HIGH availability at the front end may preclude locking out an account for failed logon attempts. If the system includes high availability user interfaces which should not be locked, include the bracketed text exempting high availability interfaces and keep the bracketed table. Indicate in the table the exempt interfaces, their location and action to take for each in lieu of locking the screen. Use care with high availability user interfaces, as in most cases the control system should act without user intervention, and a high availability user interface depends on a "high availability" operator.

****

{For Government Reference Only: This subpart (and its subparts) relate to AC-7 (a), AC-7 (b); CCI-000043, CCI-000044, CCI-001423, CCI-002236, CCI-002237, CCI-002238}

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts. If a device cannot meet these requirements, document device capabilities to protect from subsequent logon attempts and propose alternate protections in a Device Account Lock Exception Request submittal. Do not implement alternate protection measures in lieu of the indicated requirements without explicit permission from the Government. If no Device Account Lock Exceptions are requested, provide a document stating that no approval is being requested as the Device Account Lock Exception Request.

3.3.2.1 Devices MINIMALLY Supporting Accounts

****

NOTE: For LOW Impact Systems: Indicate whether devices MINIMALLY supporting accounts must lock based on unsuccessful logon attempts. Generally, for LOW Impact control systems, locking is not required - keep the first bracketed text to indicate so.

Use care when requiring that devices minimally supporting accounts lock to specify a reasonable requirement that will not introduce an additional O&M burden.

****

For LOW Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts [are not required to lock based on unsuccessful logon attempts][must lock the user account [after [five][_____] consecutive failed login attempts][_____] and must unlock the user account after [15][_____] minutes have elapsed without an unsuccessful login attempt or

by a successful login to a separate administrator account].

For MODERATE Impact Systems: Devices which MINIMALLY (but not FULLY) support accounts must lock the user account account[after [five][_____] consecutive failed login attempts][_____] and must unlock the user account after [60][_____] minutes have elapsed without an unsuccessful login attempt or by a successful login to a separate administrator account.

3.3.2.2 Devices FULLY Supporting Accounts

****

NOTE: Select or indicate the number and time period for unsuccessful logon attempts to lock an account.

When a device has a single administrator account, that account cannot be manually unlocked (as unlocking requires an administrator account, and the only one is now locked). Select the time period for sole administrator accounts to remain locked before automatically unlocking.

****

Devices which FULLY support accounts must meet the following requirements.

a. It must lock the user account when [three][_____] unsuccessful logon attempts occur within a [15 minute][_____] interval.

b. Once an account is locked, the account must stay locked until unlocked by an administrator. If the account being locked is the sole administrator account on the device, the account must stay locked for [1 hour][_____] and then automatically unlock.

c. Once the indicated number of unsuccessful logon attempts occurs, delay further logon prompts by 5 seconds.

3.3.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

****

NOTE: Indicate whether or not there are high availability interfaces which are exempt from unsuccessful logon attempts requirements. If there are, specify them in the table provided.

****

[There are no high availability interfaces which are exempt from unsuccessful logon attempts requirements.][The following high availability interfaces are exempt from unsuccessful logon attempts requirements:

High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

User Interface	Location	Action to take in lieu of locking screen
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]

High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements		
User Interface	**Location**	**Action to take in lieu of locking screen**
[_____]	[_____]	[_____]

]

3.3.3 System Use Notification

****
NOTE: Note that the point of restricting the requirement to devices "connected to the network" is to exclude things like a thermostat that has a PIN to lockout changes but isn't networked.
****

{For Government Reference Only: This subpart (and its subparts) relates to AC-8; CCI-000048, CCI-002247, CCI-002243, CCI-002244, CCI-002245, CCI-002246, CCI-000050, CCI-002248}

3.3.3.1 System Use Notification for Remote User Interfaces

Remote user interfaces must display a warning banner meeting the requirements of DTM 08-060 on screen.

3.3.3.2 System Use Notification for Local User Interfaces

Devices which are connected to a network and have a local user interface must display a warning banner meeting the requirements of DTM 08-060 on the user interface screen if capable of doing so and must have a permanently affixed label with an approved banner from DTM 08-060 if unable to display the warning banner on the screen. Where it is impractical (perhaps due to device size) to affix the label to the device, affix the label to the device enclosure.

Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contrast between font and background colors.

3.3.4 Session Lock and Session Termination Requirements In MODERATE Impact Systems:

****
NOTE: Indicate duration of inactivity before terminating or locking a session.

Also indicate the maximum number of concurrent sessions to prevent a single user from being logged in multiple ("too many") times.
****

{For Government Reference Only: This subpart (and its subparts) relates to AC-11(a), AC-11(b), AC-11(1), AC-12, SC-10; AC-10; CCI-000058, CCI-000059, CCI-000056, CCI-000057, CCI-000060, CCI-002360, CCI-002361, CCI-001133, CCI-001134, CCI-000054, CCI-000055, CCI-002252}

3.3.4.1 Session Termination

When session termination is required for a User Interface, the User

Interface must implement session termination a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session Termination must result in logging out the user. A logged out User Interface may only perform actions as indicated in the "Permitted Actions Without Identification or Authentication" subpart of this Section or display a publicly viewable image or blank screen. User Interfaces must remain logged out (session terminated) until a user enters correct authentication information, which must initiate a new session. All User Interfaces running on computers and all Remote User Interfaces must also terminate network connections as part of session termination.

3.3.4.2 Session Lock

When session lock is required for a User Interface, the User Interface must implement session lock a) based on manual initiation, or b) based on lack of activity, or c) based on either manual initiation or lack of activity, as indicated.

Session lock must result in the User Interface being suspended and the user interface must display a publicly viewable image or blank screen. No interaction with the user interface must be possible until either a) the same user enters valid authentication information, in which case that session must be continued, or b) until a different user enters valid authentication information at which point the first session must be terminated and a new session initiated for the new user.

3.3.4.3 Session Lock and Termination for Computers

****

NOTE: Include bracketed text referring to Session Lock and Session Termination Exception Table only if the subpart containing the table is included below.

Unless specifically required by the site, do not include bracketed text with requirements for support of session lock.

****

[Except as shown in the Session Lock and Session Termination Exception Table,]User Interface sessions provided by computer operating systems must support the requirement for both Session Lock and Session Termination. Session Lock and Session Termination must be capable of being initiated by the user and must also be initiated by lack of activity. Session Lock must occur after [15][_____] minutes of inactivity, and Session Termination must occur after [30][_____] minutes total of inactivity (including, not in addition to, the time for Session Lock). When a user initiates a new session, terminate existing sessions if necessary to limit the total number of concurrent sessions to [1][_____].

[Except as shown in the Session Lock and Session Termination Exception Table,]Other User Interface sessions running on computers (for local user interfaces) or hosted on a computer (for remote user interfaces) and supporting accounts must support user initiation of Session Termination[and session lock. Session lock may be initiated by user initiation or automatically after [15][_____] minutes of inactivity]. In addition, remote User Interface sessions must also initiate Session Termination

after [30][_____] minutes of inactivity [unless otherwise indicated in the Session Lock and Termination Exceptions table].

3.3.4.4 Session Lock and Termination for Controllers

****
NOTE: Include bracketed text referring to Session Lock and Session Termination Exception Table only if the subpart containing the table is included below.

Unless specifically required by the site, do not include bracketed text with requirements for support of session lock.
****

[Except as shown in the Session Lock and Session Termination Exception Table,]Writable Remote User Interfaces must support requirements for Session Termination, and must both be capable of being initiated by the user and initiated by lack of activity. Session Termination must initiate after [30][_____] minutes of inactivity.

[Except as shown in the Session Lock and Session Termination Exception Table,]Local User Interfaces supporting accounts must support manual initiation of Session Termination. Privileged Local User Interfaces must also support timed initiation of Session Termination[, unless otherwise indicated in the Session Lock and Termination Exceptions table], with Session Termination initiated at [30][_____] minutes of inactivity.[They must also support session lock, where session lock may be initiated by user initiation or automatically after [15][_____] minutes of inactivity.]

[3.3.4.5 Session Lock and Termination Exceptions

****
NOTE: Include this subpart only when exceptions to the Session Lock and Termination requirements are being indicated using the provided table.
****

Table: Session Lock and Termination Exceptions

Device	Location	Session Lock and Termination Requirements for Device (or "none" to indicate session lock or session termination is not required)
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]

]3.3.5 Permitted Actions Without Identification or Authentication

****
NOTE: These requirements are specifically about user actions, not actions taken automatically by control system components.

Unless there is a project-specific confidentiality concern or other project-specific requirement keep the bracketed text "except read only actions".

Notes concerning how this requirement addresses cybersecurity when bracketed text "except read only actions" is NOT included:

1) This requirement indicates that there are no actions that can be taken without identification and authentication for any user interface where account support is required.

2) This requirement does not limit actions taken by a user on a user interface that does not support accounts, but other requirements limit this to READ-ONLY interfaces.

3) Thus the "permitted actions" referred to by control AC-14 are "read-only access to information from devices which are not required to have user accounts."

When "except read only actions" IS included, read-only actions even from devices supporting accounts are permitted without authentication and thus the "permitted actions" referred to by control AC-14 are "read-only access to information"

****

{For Government Reference Only: This subpart (and its subparts) relates to AC-14; CCI-000061, CCI-000232}

The control system must require identification and authentication before allowing any actions[except read-only actions] by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.3.6 Physical Security in MODERATE Impact Systems

{For Government Reference Only: This subpart relates to PE-3(1), PE-4, PE-5, SC-7(a), SC-7(c), SC-8, SC-8(1); CCI-000928, CCI-002926, CCI-000936, CCI-002930, CCI-002931, CCI-000937, CCI-001097, CCI-001109, CCI-002418, CCI-002419, CCI-002421.}

3.3.6.1 Physical Security for Media

3.3.6.1.1 Physical Security for Media Inside Mission Space

Install all non-IP network media located inside of the mission space in conduit. Install all IP network media located inside of the mission space in intermediate metallic conduit.

3.3.6.1.2 Physical Security for Media Outside Mission Space

Install all network media (both IP and non-IP) located outside of the mission space in rigid metallic conduit.

3.3.6.1.3 Physical Security for Non-Network Media in Fire Protection Systems

For Fire Suppression Systems which can be inhibited or forced to activate by manipulation of non-network wiring, install all non-network media outside of mission space, including analog and binary instrumentation wiring and power wiring, in rigid metallic conduit.

3.3.6.2 Physical Security for Devices

****

NOTE: For MODERATE impact system, all devices should be in spaces controlled by the mission being served. For such devices these requirements often add additional physical security requirements on devices above and beyond the user interface requirements specified in "ACCESS CONTROL REQUIREMENTS".

****

Install all devices (computers and controllers) which are located outside of mission space in lockable enclosures. (Recall that per definition of mission space, a room controlled by the mission is mission space regardless of whether it is contiguous with other mission space.)

Install all controllers, and other OT devices, connected to an IP network in lockable enclosures (both inside and outside of mission space).

3.3.6.2.1 Physical Security for Devices in Fire Protection Systems

For Fire Suppression systems with a release panel, install all components of the suppression system either inside mission space, or within locked enclosures. Components of these systems include: release panel, any relay or interface panels, analog and binary inputs or outputs, control valves, manual valves.

3.3.6.3 Physical Security for User Interfaces

Physical security requirements for User Interfaces are specified in the preceding paragraphs of this Section.

[3.3.6.4 Additional Physical Security for Confidentiality of User Interfaces and Printers

****

NOTE: If specific user interfaces or printers require additional security controls to protect the confidentiality of the information displayed or printed, keep this Subpart and indicate these requirements in the table. Otherwise remove this bracketed subpart.

These additional requirements will generally NOT be required as these are secured due to the multiple MODERATE controls already applied. It's possible additional requirements will be needed for systems containing PII or other sensitive data.

Additional controls may include increased physical

security, locating shredders/burn bags near printers, and installing privacy screens on monitors.
****

For each user interface or printer indicated in the "User Interfaces and Printers Requiring Additional Security Controls" table, implement the additional confidentiality controls indicated.

User Interfaces and Printers Requiring Additional Security Controls		
User Interface or Printer	Location	Additional Confidentially Control to be Implemented
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]

]3.3.7 Enclosures

Prior to final acceptance of the system, lock all lockable enclosures. Submit an Enclosure Keys submittal with all copies of keys for all enclosures and a key inventory list documenting all keys. Label each key with the matching enclosure identifier.

3.4 USER IDENTIFICATION AND AUTHENTICATION

****
NOTE: Remove all requirements for multifactor authentication unless:
1) specifically required by the project site
AND
2) either (a) the project includes the IT infrastructure required to support multifactor authentication or (b) the project site already has the needed infrastructure.

Note that if there are a very limited number of devices requiring something other than passwords, it might be better to simply always allow passwords in general and list the specific device exceptions in the Device Specific IA Requirements table.

Also note that the default implementation of multifactor authentication (if selected) is the use of PIV (typically a CAC).
****

{For Government Reference Only: This subpart (and its subparts) relates to IA-2, IA-2(1),IA-2(12), IA-5 IA-5(b), IA-5(c), IA-5(e), IA-5(g), IA-5(1), IA-5(11); CCI-000764, CCI-000765, CCI-001953, CCI-001954, CCI-001544, CCI-001989, CCI-000182, CCI-001610, CCI-000192, CCI-000193, CCI-000194, CCI-000205, CCI-001619, CCI-001611, CCI-001612, CCI-001613,

CCI-001614, CCI-000195, CCI-001615, CCI-000196, CCI-000197, CCI-000199, CCI-000198, CCI-001616, CCI-001617, CCI-000200, CCI-001618, CCI-002041, CCI-002002, CCI-002003. For MODERATE Impact systems, this subpart also relates to AC-6 (1), AC-6(10), AC-6(2), AC-6(9)IA-2(4), IA-5(13); CCI-001558, CCI-002221, CCI-002222, CCI-002223, CCI-002235, CCI-000039, CCI-001419, CCI-002234, CCI-000768, CCI-002007.}

This subpart indicates requirements for specific methods of identification and authentication for users and user accounts. Where these requirements conflict apply the following order of precedence: 1) If present, Device Specific Requirements take precedence over any other requirements; and then 2) multifactor authentication requirements take precedence over password requirements.

3.4.1 User Identification and Authentication for All System Types

****

NOTE: The bracketed requirement for LOW impact systems, and the first bracketed requirement for MODERATE impact systems are equivalent to the typical computer requirement that users login with PIV, which in DoD means CAC. These requirements will still need infrastructure support within the control system and should only be included when required and supported by the project site.

The other three bracketed requirements for MODERATE Impact systems go beyond the above requirements and require, in addition to infrastructure support, support by control system specific interfaces. Before including any of these options, ensure that there is a requirement for and infrastructure to support these requirements, and that there are control system vendors who can support the requirement.

****

Unless otherwise indicated, all user interfaces supporting accounts (either FULLY or MINIMALLY) must implement Identification and Authorization via passwords.

[For LOW Impact Systems: User interfaces provided by computer operating systems must implement multifactor authentication via PIV.]

For MODERATE Impact Systems:[User interfaces provided by computer operating systems must implement multifactor authentication via PIV.][User interfaces supporting accounts (FULLY or MINIMALLY) on computers must implement multifactor authentication via PIV.][Devices with writable remote user interfaces must implement multifactor authentication via PIV.][Devices with Privileged Remote User Interfaces must implement multifactor authentication via PIV.] Software running on computers and computer operating systems must manage cached authenticators in accordance with the relevant STIGs. All other devices and software must not use cached authenticators.

3.4.2 User Identification and Authentication for Specific System Types

****

NOTE: This subpart allows system type specific

requirements which supersede the general requirements in the previous subpart (User IA for All System Types). Only include additional requirements here when specifically required by the project; otherwise select the "no additional requirements" text.

Note there is a later subpart allowing for specification of requirements for specific devices. Should a small number of devices have a requirement use that subpart and list those specific devices rather than creating a more general requirement here.

****

System specific requirements are in addition to and supersede those indicated for all system types. When no additional requirements are indicated for a specific system type the requirements for all systems still apply to that system type.

3.4.2.1 HVAC Control Systems Devices

[No additional system specific requirements apply.][User Interfaces which FULLY support accounts and which run on a computer must use multifactor authentication via PIV.]

3.4.2.2 Lighting Control Systems Devices

[No additional system specific requirements apply][User Interfaces which FULLY support accounts and which run on a computer must use multifactor authentication via PIV.]

3.4.2.3 Electronic Security System Devices

****

NOTE: Select whether to require PIV, or allow alternate mechanisms.

****

User interfaces which FULLY support accounts and which run on a computer must use multifactor authentication via PIV.[Other user interfaces which FULLY support accounts must use multifactor authentication via PIV.][User interfaces which MINIMALLY support accounts must use either passwords or multifactor authentication via PIV.]

3.4.2.4 [_____] Control System Devices

****

NOTE: Use this subpart if needed to add requirements for a specific control system type (e.g. lighting, electrical distribution etc.), similar to how HVAC and Lighting control system devices are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.

****

[_____]

3.4.3 User Identification and Authentication for Specific Devices

****
NOTE: If there are specific devices (e.g. "Rm 17 lighting user interface", "all model 17 controllers"), keep the bracketed text including the table and list them along with the required methods in the table. Otherwise keep bracketed text indicating there are no device specific user interface requirements
****

[There are no additional device specific user interface requirements][Additional user identification and authentication requirements are defined in the TABLE.

TABLE: Additional Device Specific User Identification and Authentication Requirements

User Interface Device or Description	**Identification and Authorization Requirements**
[_____]	[_____]
[_____]	[_____]
[_____]	[_____]
[_____]	[_____]

]
[3.4.3.1 [_____]

****
**NOTE: Use this subpart (and make additional copies as needed) to define any unique Identification and Authorization Requirements used in the table above. Two common alternate methods for multifactor authentication are:
1) Text/SMS/email Based - where a message (code) is sent as a text to a cell phone or to an email address.
2) Hardware Token Based - where there is a hardware device such as a USB key or a pseudo random number generator (RSA token) that is used instead of a PIV card.**
****

[_____]

]

3.4.4 Implementation of Identification and Authorization Requirements

Identification and Authorization must be met by one of the following methods:

a. Direct implementation in the user interface.

b. For user interfaces on a computer: inheriting the Identification and Authorization from the computer operating system, either by the operating system limiting access to specific applications by user, or by the application itself having permissions based on the user logged into the computer.

c. For remote interfaces: an implementation shared between the remote user interface server and the remote user interface client. For example, a requirement for PIV authentication may be met on a remote user interface by a PIV reader on a web browser client which sends the authentication information via HTTPS to the remote server.

3.4.5 Password-Based Authentication Requirements

3.4.5.1 Passwords for Software and Applications Running on Computers

All software and applications running on computers supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 12 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a minimum lifetime of 24 hours.

g. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

h. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).

i. Passwords must be cryptographically protected during storage and transmission.

3.4.5.2 Passwords for Controllers FULLY Supporting Accounts

All controllers FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 12 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters.

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.3 Passwords for Remote Interfaces

Passwords for connecting to a Remote User Interface supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 12 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character. The list of supported special characters must include at least 4 separate characters.

f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do not lock accounts due to expired passwords.

g. Password must differ from previous five passwords, where differ is defined as changing at least 50 percent of the characters (where location is significant, a character may be reused if it is in a different position).

h. Passwords must be cryptographically protected during storage and transmission.

3.4.5.4 Passwords for Devices Minimally Supporting Accounts

****

NOTE: Indicate minimum password requirements for devices MINIMALLY supporting accounts. Use as large a value as practical, but use caution to pick a number that is supportable by the components.

Never allow a minimum length less than four characters. For HVAC control systems, simple Local Display Panels may not support more than four characters, and keeping four as the minimum is generally recommended.

****

Devices MINIMALLY supporting accounts must support passwords with a minimum length of [four][_____] characters.

3.4.5.5 Password Configuration and Reporting

****
NOTE: Select whether the contractor will change passwords and submit a copy of the passwords or accompany site personnel while they change passwords.

In the case of contractor changing the passwords: Provide a POC for password coordination. This will generally be a supervisor or other senior member of the project site maintenance organization.

The Password Summary Report is needed by the project site system owner or O&M staff. This report is required to be delivered as hardcopy in a sealed envelope to keep passwords more confidential. Note that the contractor will know the passwords, so there remains a risk, but by changing the default the number of individuals knowing the password for a specific device is greatly reduced (from "everyone" to "the contractor and the installation")

In the case of site personnel changing the passwords, indicate the POC for coordination.
****

[For all devices with a password, change the password from the default password. Coordinate selection of passwords with the Password Point of Contact. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Confidential Password Report documenting the password for each device and describing the procedure to change the password for each device.

Do not provide the Password Summary Report in electronic format. Provide [two][_____] hardcopies of the Password Summary Report, each copy in its own sealed envelope.

][For all devices with a password, coordinate the changing of passwords with the project site following testing of the system but prior to turnover to the Government. Coordinate with Password Point of Contact to determine appropriate project site personnel to complete password changes. Accompany identified personnel to each device with a password and instruct personnel on the process of changing password. Record the time, date and personnel present when each device's password is changed and submit a Password Change Summary Report documenting this information.

Provide the Password Summary Report electronically in both PDF and Microsoft Excel.
]

3.4.6 Authenticator Feedback

{For Government Reference Only: This subpart relates to IA-6; CCI-000206}

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is

entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

[3.4.7 Implementation of PKI Infrastructure in Moderate Impact Systems (Except USACE Civil Works Systems)

****

NOTE: When the USACE CW Tailoring Option is selected, a subpart covering Implementation of PKI Infrastructure is included below. When using the USACE CW tailoring option, remove this subpart during bracket replacement.

For MODERATE Impact Systems: Most systems will not use PKI (typically implemented as PIV (CAC) authentication). If PKI is supported at the front end, it may be implemented by the base-wide network (Platform Enclave) and not the controls contractor. If there is a requirement for the contractor to support PKI, include this subpart, otherwise remove it.

Note, PKI Infrastructure is not required to support the requirement for use of HTTPS for remote user interfaces.

****

Coordinate with the PKI Infrastructure Point of Contact to configure the system to implement PKI such that the system validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; the system enforces authorized access to the corresponding private key; the system maps the authenticated identity to the account of the individual or group; and the system implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

]3.4.8 Implementation of PKI Infrastructure in USACE Civil Works Systems

****

NOTE: This subpart is only included when the USACE CW tailoring option is selected.

****

Coordinate with the PKI Infrastructure Point of Contact to configure the PKI system. Implement PKI digital certificates for communications where possible, such that the system validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information. Configure the system to enforce authorized access to the corresponding private key, to map the authenticated identity to the account of the individual or group, and to implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. [Self-signed certificates are acceptable.]Document communications devices that cannot be Certificate protected in a Certificate Protection Status (Encrypted) submittal for all communication devices prior to any equipment requiring certificates arriving at the site.

3.5 CYBERSECURITY AUDITING

****

NOTE: Auditing within the control system is a complex requirement. For standard information systems, DoD has extensive auditing requirements, which largely cannot be met within a typical control system. For more information on auditing, see UFC 4-010-06, Cybersecurity for Facility-Related Control Systems

DoD requires (see AU-2) the capability to audit the following events:

a. ***Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. Classification levels)*** **- generally only applicable to computers.**

b. ***Successful and unsuccessful logon attempts*** **- generally only applicable to computers and devices FULLY supporting accounts.**

c. ***Privileged activities or other system level access*** **- generally only applicable to computers.**

d. ***Starting and ending time for user access to the system*** **- generally only applicable to computers and devices FULLY supporting accounts.**

e. ***Concurrent logons from different workstations*** **- generally only applicable to computers and devices with web interfaces.**

f. ***Successful and unsuccessful accesses to objects*** **- generally only applicable to computers.**

g. ***All program initiations*** **- generally only applicable to computers; for a controller, this is covered under kernel module actions, below.**

h. ***All direct access to the information system*** **- generally only for computers.**

i. ***All account creations, modifications, disabling, and terminations*** **- generally only applicable to devices that FULLY support accounts.**

j. ***All kernel module load, unload, and restart*** **- this could apply to computers or controllers.**

DoD also requires that the selection of which events get audited is under the control of the Information

System Security Manager (ISSM).

DoD requires (see AU-3) that audit records contain the following:
- type of event
- time of the event
- location of the event
- source of the event
- result of the event
- the identity of any individuals or subjects associated with the event.

Note that much of this information will be not applicable for field control system devices.

DoD requires that all devices in the system be capable of auditing events, but allows the ISSM to select which devices must perform auditing (see AU-12 (b)).

Note that there is a large gap between what is theoretically required in terms of a capability ("audit all events at all devices") vs. what is practical and reasonable to implement in a specific control system. The designer needs to provide input on what can and cannot be done in terms of what devices in the system can perform auditing, and what events can they audit.

Require implementation for what is possible but do not require unreasonable requirements. Be prepared to document/explain impractical requirements if required by the System Owner (SO) or Authorizing Official (AO)

Control System Alarms:
Control system alarms should have similar requirements. The designer should specify what alarms should be generated, which devices should perform alarm generation, the accuracy of alarm time stamps, response to alarm generation failures (e.g. loss of communication with a field device), and sufficient storage capacity at the front end to maintain alarm/event logs for a specified period of time. These requirements should be defined in the relevant control system specifications, not in this Section.

Note the ability for the control system to send emails is dependent on the site having the proper infrastructure in place. Coordinate with the site if this capability is required and is not already available as part of existing control system requirements or functionality.

****
****

NOTE: When the USACE CW tailoring option is selected, the below text about email notification is in brackets and a statement indicating that email notification is not permitted is included. For

USACE Civil Works systems, delete the bracketed text.
****

[Where an auditing requirement exists for email notification, notify via email the application administrator and Information System Security Officer (ISSO) of the event. Coordinate with the Email Address Point of Contact for email addresses. If outgoing email is not available to the system, disable email notifications.]

USACE Civil Works systems do not permit email notification. Disable all email notification. Auditing requirements for email notification in this section do not apply to USACE Civil Works control systems

3.5.1 Audit Events, Content of Audit Records, and Audit Generation

{For Government Reference Only: This subpart (and its subparts) relates to AU-2(a), AU-2(c), AU-2(d), AU-3, AU-10, AU-12, AU-14(b), AU-14(1), AU-14(2), AU-14(3), CM-5(1), SC-7 (9); CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-001230, CCI-000133, CCI-000134, CCI-001487, CCI-000166, CCI-001899, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910, CCI-001914, CCI-001919, CCI-001464, CCI-001462, CCI-001920, CCI-001814, CCI-002400. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-3 (1); CCI-000135, CCI-001488}

For devices that have STIG/SRGs related to audit events, content of audit records or audit generation, comply with the requirements of those STIG/SRGs.

If auditing requirements can be met using existing control system alarm or event capabilities, those existing capabilities may be used to meet these requirements.

3.5.1.1 Computers

For each computer, provide the capability to select audited events and the content of audit logs. Configure computers to audit the indicated events, and to record the indicated information for each auditable event. Send logs to a syslog server that is only accessible via accounts on the system with privileged level access.

3.5.1.1.1 Audited Events

Configure each computer to audit the following events:

a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)

b. Successful and unsuccessful logon attempts

c. Successful logouts

d. Privileged activities or other system level access

e. Concurrent logons from different workstations

f. Successful and unsuccessful accesses to objects

g. Program initiations

h. Direct access to the information system

i. Account creations, modifications, disabling, and terminations. For MODERATE Impact Systems, also provide email notification when these audit events occur.

j. Kernel module load, unload, and restart

k. Operator actions related to operation of the system

3.5.1.1.2 Audit Event Information To Record

Configure each computer to record, for each auditable event, the following information (where applicable to the event):

a. What type of event occurred

b. When the event occurred

c. Where the event occurred

d. The source of the event

e. The outcome of the event

f. The identity of any individuals or subjects associated with the event

g. For MODERATE Impact Systems: For all privileged commands, full-text recording of the executed command and the user executing the command

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation.

3.5.1.2 For HVAC Control System Controllers

3.5.1.2.1 HVAC Control System Controllers FULLY Supporting User Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.2.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful logon attempts to the controller

b. Successful logouts

c. All account creations, modifications, disabling, and terminations. For MODERATE Impact Systems, also provide email notification when these audit events occur.

d. All controller shutdown and startup

e. For privileged user interfaces in MODERATE Impact Systems: All user commands.

3.5.1.2.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. the identity of any individuals or subjects associated with the event

d. For privileged user interfaces in MODERATE Impact Systems: Full text recording of the executed command and the user executing the command.

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation.

3.5.1.2.2 Other HVAC Control System Controllers

There are no requirements to perform auditing at HVAC field controllers that do not FULLY support accounts.

3.5.1.3 For Lighting Control System Controller

3.5.1.3.1 Lighting Control System Controllers FULLY Supporting User Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.3.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful logon attempts to the controller

b. Successful logouts

c. All account creations, modifications, disabling, and terminations. For MODERATE Impact Systems, also provide email notification when these audit events occur.

d. All controller shutdown and startup

e. For privileged user interfaces in MODERATE Impact Systems: All user commands.

3.5.1.3.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. the identity of any individuals or subjects associated with the event

d. For privileged user interfaces in MODERATE Impact Systems: Full text recording of the executed command and the user executing the command.

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation

3.5.1.3.2 Other Lighting Control System Controllers

There are no requirements to perform auditing at Lighting field controllers that do not FULLY support accounts.

3.5.1.4 [_____] Control System Controllers

****
NOTE: Use this subpart if needed to add requirements for a specific control system type (e.g. lighting, electrical distribution etc.), similar to how HVAC and Lighting control system controllers are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.
****

[_____]

3.5.1.5 Default Requirements for Control System Controllers

****
NOTE: Do not edit these requirements. These default requirements should only be used in lieu of technology-specific requirements in the preceding paragraphs. If these default requirements are inappropriate, ensure that the preceding paragraphs provide appropriate technology-specific requirements.
****

For control system controllers where Audit Events, Content of Audit Records, and Audit Generation are not otherwise indicated in this Section:

3.5.1.5.1 Controllers Which FULLY Support Accounts

For each controller which FULLY supports accounts, provide the capability to select audited events and the content of audit logs. Configure controllers to audit the indicated events, and to record the indicated information for each auditable event.

3.5.1.5.1.1 Audited Events

Configure each controller to audit the following events:

a. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels)

b. Successful and unsuccessful logon attempts

c. Successful logouts

d. Concurrent logons from different workstations

e. All account creations, modifications, disabling, and terminations. For MODERATE Impact Systems, also provide email notification when these audit events occur.

f. All kernel module load, unload, and restart

g. For privileged user interfaces in MODERATE Impact Systems: All user commands.

3.5.1.5.1.2 Audit Event Information To Record

Configure each controller to record, for each auditable event, the following information (where applicable to the event):

a. what type of event occurred

b. when the event occurred

c. where the event occurred

d. the source of the event

e. the outcome of the event

f. the identity of any individuals or subjects associated with the event

g. For privileged user interfaces in MODERATE Impact Systems: Full text recording of the executed command and the user executing the command.

For MODERATE Impact Systems: Audit records must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation

3.5.1.5.2 Controllers Which Do Not FULLY Support Accounts

For each controller which does not FULLY support accounts configure the controller to audit all controller shutdown and startup events and to record for each event the type of event and when the event occurred.

3.5.2 Audit Time Stamps

{For Government Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890. For MODERATE Impact systems, this subpart (and its subparts) also relates to AU-8 (1); CCI-001891, CCI-001892, CCI-002046.}

Any device (computer or controller) generating audit records must have an internal clock capable of providing time with a resolution of one second. Clocks must not drift more than 10 seconds per day. Configure the system

so that each device (computer or controller) generating audit records maintains accurate time to within 1 second. Note that if the control system specifications include requirement for clocks, the most stringent requirement applies.

3.5.3 Auditing Front End Software

****

NOTE: Auditing Front End Software may be a component of the control system front end or a separate software package. In either case - but particularly when it is part of an existing control system front end -- the site may already have this software.

Confirm with the project site whether they already have this software. If they do, indicate the current software.

Use the bracketed text to indicate where software is to be installed (either on the control system front end computer or indicate another computer) or to require that the software be provided for installation by the project site.

****

****

NOTE: For USACE CW Systems, the Designer must coordinate with the UCIC MCX to determine the auditing software requirements for the system being designed. Given the size and/or type of system, auditing software may not be required and should be removed from the spec section during bracket replacement.

Although some auditing functions may be implemented by the ISSO/SA upon acceptance of the system, it could require software to be provided by the Contractor. In this scenario edit the paragraph as needed to identify the auditing software contract requirements for the Civil Works application.

****

The project site currently has the following software to support control system auditing: [none][_____]. If there is no existing auditing front end software or the software is not compatible with the provided control systems, provide Auditing Front End Software with audit log import and upload, export, notification, and analysis functionality. The Auditing Front End Software may be provided as a component of the control system front end or as a separate software package, and a single package may serve multiple control systems provided under the same projects if they are sharing a cybersecurity authorization.

When the Auditing Front End Software is neither existing nor installed under the requirements of another Section, furnish the Auditing Front End Software media and license [for subsequent Government installation][and install the software on [_____]][the control system front end computer in

[_____]]. Submit copies of Auditing Front End Software if this function is not part of the software provided with the control system to meet requirements of other Sections.

3.5.3.1 Import and Upload Requirements

Auditing Front End Software must be capable of importing audit logs from the Device Audit Record Upload Software and of uploading audit logs over the network from all control system devices supporting network upload of audit logs.

3.5.3.2 Export Requirements

Auditing Front End Software must be capable of exporting to a file format supported by Microsoft Excel.

3.5.3.3 Notification Of Audit Failure in Devices in MODERATE Impact Systems

The auditing front end software must be capable of receiving notifications of audit failure from control system devices and computers and be able to provide email notification based on receipt of the notification.

3.5.3.4 Audit Reduction and Report Generation In MODERATE Impact Systems

****

NOTE: Indicate the time stamp discrepancy between audit logs that the system must be able to accommodate for correlating audit logs. This accounts for timestamp errors between different auditing devices, and will allow for multiple entries to be linked to the same event. The 2-second default is based on the time stamp accuracy requirement in the Time Stamps subpart, and accounts for device clocks being plus or minus 1 second (total of a 2 second span).

****

{For Government Reference Only: This subpart (and its subparts) relates to AU-6(4), AU-7(a), AU-7(b), AU-7(1), AU-12(1); CCI-000154, CCI-001875, CCI-001876, CCI-001877, CCI-001878, CCI-001879, CCI-001880, CCI-001881, CCI-001882, CCI-000158, CCI-000173, CCI-000174, CCI-001577.}

Auditing Front End Software must provide audit reduction and reporting capabilities that supports on-demand review and analysis, on demand reporting, and after the fact investigations of security incidents. The software must be able to combine audit records from all components within the system and analyze them as a single audit record. The software must correct for discrepancies in timestamps of audit logs from different sources and be able to account for discrepancies up to [2][_____] seconds between sources. The software must not alter original audit record content or time ordering of audit records. The software must have the capability to filter audit records using user-defined fields within the audit records.

The audit reduction and reporting capabilities may incorporate third party application, such as Excel or Access.

3.5.4 Audit Storage Capacity and Audit Upload

****
NOTE: Select or indicate duration and rate of audit record generation for field devices. Unless there is a known need, do not add requirements for computer storage capability.
****

{For Government Reference Only: This subpart (and its subparts) relates to AU-4; CCI-001848, CCI-001849}

The creation of audit records must never interfere with normal device operation. Devices must cease collection of auditing information if required to maintain normal operation.

a. For devices that have STIG/SRGs related to audit storage capacity (CCI-001848 or CCI-001849) comply with the requirements of those STIG/SRGs.

b. For controllers capable of generating audit records, provide [60][_____] days worth of secure local storage, assuming [10][_____] auditable events per day.[

c. For computers, provide storage for at least [_____] audit records.]

3.5.4.1 Audit Log Storage Notification In MODERATE Impact Systems

****
NOTE: Indicate who, in addition to the ISSO and ISSM, will receive notification that audit logs are nearly full. Indicate who to coordinate with for email addresses.
****

{For Government Reference Only: This subpart (and its subparts) relates to AU-5(1); CCI-001855.}

Controllers storing audit logs must provide notification when audit logs reach 75 percent of capacity either directly through email or indirectly by sending a notification to a computer, and the computer sending an email. Computers storing audit logs must provide notification when audit logs reach 75 percent of capacity directly through email.

3.5.4.2 Device Audit Record Upload Software

****
NOTE: If you indicated an installation location for the Auditing Front End Software, keep bracketed text requiring the Device Audit Record Upload Software to be installed on the same computer.

Note that this software may not be required for every project if all devices and computers can upload to the Auditing Front End.
****

For each device (computer or controller) required to audit events and for which audit logs cannot be uploaded over the network by the Auditing Front

End Software, provide and license to the Government software implementing a secure mechanism of uploading audit records from the device and exporting them to the Auditing Front End Software. Where different devices use different software, provide software of each type required to upload audit logs from all devices.

[When Device Audit Record Upload Software is capable of uploading audit logs over the network, install Device Audit Record Upload Software on the same computer as the Auditing Front End Software.] Submit copies of device audit record upload software if this function is not part of the software provided with the control system to meet requirements of other Sections. If there are no devices requiring this software, provide a document stating this in lieu of this submittal.

3.5.5 Response to Audit Processing Failures

****

NOTE: The requirement that audit processing failures notify a person implies that this control can only be met at a computer with network access, not by a control device within the control system. The action taken should be "overwrite oldest audit records" if possible; it should almost certainly never be "shut down information system". Provide a POC to notify, either the Security Controls Assessor (SCA) or the Information System Security Officer (ISSO). Provide a default action.

****

{For Government Reference Only: This subpart (and its subparts) relates to AU-5; CCI-000139, CCI-000140, CCI-001490.}

In the case of a failure in the auditing system, computers associated with auditing must provide email notification[and must [_____]]. For MODERATE Impact systems, the computer must also notify the associated auditing front end software. In case of an audit failure, if possible, continue to collect audit records by [overwriting existing audit records][_____].

For MODERATE Impact Systems: In the case of an audit failure at a controller performing auditing, the device must notify the associated auditing front end software of the audit failure if able, and must continue to collect audit records by [overwriting existing audit records][_____] if able. The auditing front end software must provide notification as indicated, treating the notification of failure from the device as a failure in the auditing system.

3.6 REQUIREMENTS FOR LEAST FUNCTIONALITY

****

NOTE: The control system should be designed to have the least capability possible while still meeting the minimum needs of the government. This means disabling unnecessary functionality. Do not install unnecessary software. Ensure that unnecessary accounts, maintenance passwords, etc. are all changed, disabled, or removed.

For systems other than HVAC control systems:
Consider disallowing unrequested user interfaces and consider disallowing networked sensors/actuators

where they are not required.
****

{For Government Reference Only: This subpart (and its subparts), along with the Network Communication, Ports, Protocols and Services Report submittal specified elsewhere in this section, relates to CM-6(a), CM-6(c), CM-7, CM-7(1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546. For MODERATE Impact systems, this subpart (and its subparts) also relates to CM-7(2), CM-7(5)(a), CM-7(5)(b); CCI-000381, CCI-000380, CCI-000382, CCI-001761, CCI-001762}

For devices that have a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port and device I/O access for least functionality), install and configure the device in accordance with that STIG or SRGs.

3.6.1 Device Capabilities

For HVAC Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For Lighting Control Systems: Do not provide devices with remote user interfaces or with full user interfaces where one was not required.

For Other Control Systems: For LOW Impact Systems: [Do not provide devices with remote user interfaces or with full user interfaces where one was not required.] [Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.]

For Other Control Systems: For MODERATE Impact Systems: Do not provide devices with remote user interfaces or full user interfaces where one was not required. Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.

For all MODERATE Impact Systems: Unless specifically required by the government, do not provide a capability to update device firmware over the network.

3.6.2 Software

For software that has a STIG or SRG related to Requirements for Least Functionality (such as configuration settings and port access for least functionality), install and configure the software in accordance with that STIG or SRG.

Do not install software that is not specifically required to meet a contract requirement. Remove any previously installed that is not specifically required to meet a contract requirement. Do not implement functionality within software
that is not specifically required to meet contract requirements.

3.7 SYSTEM AND COMMUNICATION PROTECTION

****
NOTE: For electrical systems, coordination studies

are performed and breaker setting coordinated such that a fault is cleared by the tripping of the first upstream breaker. Consider the possibility that the settings of that first upstream breaker may be altered in a deliberate attempt to cause an outage of an unrelated load via tripping of the second upstream breaker. In extreme cases, provide additional protection for that first upstream breaker, or provide additional series breakers in secure locations."

****

3.7.1 Collaborative Computing

{For Government Reference Only: This subpart relates to SC-15(a), SC-15(b); CCI-001150, CCI-001152.}

Without explicit approval from the project site, control systems must not use collaborative computing technologies.

3.7.2 Denial of Service Protection and Application Partitioning In MODERATE Impact Systems:

****

NOTE: Note that reducing the dependence on the network helps mitigate threats caused by a weak boundary defense.

****

{For Government Reference Only: This subpart relates to SC-5, SC-12, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097. For MODERATE Impact systems, this subpart also relates to SC-2; CCI-001082.}

To the greatest extent practical, implement control logic without reliance on the network. Except when required to meet the requirements of the control system Section (where the requirement can only be met using computer hardware), do not implement control logic in computers. For MODERATE Impact systems, do not implement control logic in a device providing (i.e. acting as a server for) a Full Remote User Interface.

3.7.2.1 Network Reliance in MODERATE Impact HVAC Control Systems

Except for networked input and outputs on input-output buses specifically designed to provide high reliability or redundancy, sensors and actuators must not rely on the network to exchange data with the controller executing the sequence of operation which uses the sensor value or determines the actuator command.

Sensor values required by multiple devices may be shared over the network provided they are connected to a controller requiring the value for execution of the sequence and that controller shares the value on the network.

3.7.2.2 Network Reliance in MODERATE Impact Lighting Control Systems

Except for networked input and outputs on input-output buses specifically designed to provide high reliability or redundancy, sensors and actuators must not rely on the network to exchange data with the controller executing the sequence of operation which uses the sensor value or

determines the actuator command.

Sensor values required by multiple devices may be shared over the network provided they are connected to a controller requiring the value for execution of the sequence and that controller shares the value on the network.

[3.7.2.3 Network Reliance in MODERATE Impact [_____] Control Systems

****
NOTE: Use this bracketed subpart if needed to add requirements for a specific control system type (e.g. electrical distribution etc.), similar to how HVAC and Lighting control system devices are covered above.

If adding a new control system type, submit a Criteria Change Request with the relevant requirements to have that system included in the published UFGS.
****

[_____]

]3.7.2.4 Default Requirements for MODERATE Impact Control Systems

****
NOTE: Do not edit these requirements (beyond selection of bracketed text). These default requirements should only be used in lieu of technology-specific requirements in the preceding paragraphs. If these default requirements are inappropriate, ensure that the preceding paragraphs provide appropriate technology-specific requirements.

****

Except for networked input and outputs on input-output buses specifically designed to provide high reliability or redundancy, sensors and actuators must not rely on the network to exchange data with the controller executing the sequence of operation which uses the sensor value or determines the actuator command.

Sensor values required by multiple devices may be shared over the network provided they are connected to a controller requiring the value for execution of the sequence and that controller shares the value on the network.

3.7.3 Mobile Code In MODERATE Impact Systems:

****
NOTE: In general, do not allow exceptions to the Web Browsers and Application SRG.

Unless compelling reasons exist, keep the bracketed text restricting the source of mobile code downloads
****

{For Government Reference Only: This subpart relates to SC-18(a),

SC-18(b),
SC-18(c), SC-18(1), SC-18(3), SC-18(4); CCI-001160, CCI-001161,
CCI-001162, CCI-001163, CCI-001164, CCI-001165, CCI-001166, CCI-001662,
CCI-002457, CCI-002458, CCI-001169, CCI-001695, CCI-001170, CCI-002469}

Devices with STIGs/SRGs related to Mobile Code and to Security Control SC-18 must be installed in accordance with the relevant STIGs/SRGs. All remote user interfaces must meet the requirements of the "Web Browsers and Application SRG".

[Mobile code may only be downloaded from a specifically authorized mobile code repository. Coordinate with the Mobile Code Point of Contact for the location of a repository.]

3.7.4 Protection of Information at Rest In MODERATE Impact Systems:

{For Government Reference Only: This subpart relates to SC-28, SC-28(1); CCI-001199, CCI-002472, CCI-002475, CCI-002476}

Computers must protect information at rest in accordance with applicable STIGs.

Any control system device storing personally identifiable information (PII), controlled unclassified information (CUI), or classified information must be protected by an Information At Rest encryption solution or by a physical security solution. Provide a Protection of Information At Rest Proposal indicating each device storing PII, CUI, or classified information and the encryption or physical security solution proposed for that device for government approval. If no devices stores PII, CUI, or classified information, provide a document stating this as the Protection of Information At Rest Proposal submittal. Do proceed with device selection and installation until the Protection of Information At Rest Proposal is approved. Once approved, implement approved Information At Rest protections.

3.7.5 Process Isolation and Boundary Protection in Moderate Impact Fire Protection Systems

{For Government Reference Only: This subpart relates to SC-7(a), SC-7(c), SC-7(4)(a), SC-7(4)(c), SC-7(5), SC-7(7), SC-7(9)(a), SC-7(11), SC-7(13), SC-7(13), SC-7(18); CCI-001097, CCI-001098, CCI-001102, CCI-002396, CCI-001109, CCI-002397, CCI-002398, CCI-002399, CCI-002403, CCI-001120, CCI-001119, CCI-001126}

****

NOTE: For many FRCS (Fire Protection being a notable exception), implementation of boundary protection is typically outside the scope of the controls contractor. The site IT staff should implement boundary protection via rules (e.g. a firewall) isolating the control system from the wider network. This is true even for a control system which will be later integrated to a larger system; the field point of connection (FPOC) should be configured to allow the minimum traffic necessary for operation. Critical to this is the Cybersecurity Interconnection Schedule, which defines what traffic must be allowed through the boundary for the proper operation of the system.

For Fire Protection Systems, some aspects of boundary protection are likely the responsibility of the installing contractor. In general, the ability to play a live audio message will be required and include the bracketed text. However, in many cases, the ability to play live audio is a vulnerability and in some cases, the site may not be willing to accept the risk. Coordinate with the site to determine whether to allow this functionality.

Select whether relays must use the normally open or normally closed contact. If a code requirement exists, follow the code. Otherwise coordinate with the fire protection specification and the project site and consider whether the greater risk is the potential to send a message when none should be sent, or the failure to send a message when one should be sent. If it is clear that one case is of greater concern than the other, select the appropriate bracketed text, otherwise remove the bracketed text to not introduce a specific requirement.

Coordinate requirements with those of "Safe Mode and Fail Safe Operation" in the following paragraph.

****

3.7.5.1 Radio Interfaces for Fire Protection Systems

When radios interfacing a local fire protection system to a supervisory system are not NIST FIPS 140-2 validated, use a relay panel interface between the local fire protection system and the radio. Install and configure the relay panel to prohibit initiating any action within the local fire protection system other than causing the system to play a pre-recorded message[or causing the system to play a live audio message]. [Install relays using the normally open contact such that they pass a signal when they close, and so that a relay that loses power or has a failed coil does not pass a signal][Install relays using the normally closed contact such that they pass a signal when they open, and so that a relay that loses power or has a failed coil passes the signal]

3.7.5.2 Fire Suppression System Network Isolation

For fire suppression systems including a release panel, any network used in these systems must be dedicated to these systems and must be isolated from any other network, including other components of the Fire Alarm and Fire Suppression systems. Use only dry contacts and relays to transfer signals from these systems to any other systems. [Install relays using the normally open contact such that they pass a signal when they close, and so that a relay that loses power or has a failed coil does not pass a signal][Install relays using the normally closed contact such that they pass a signal when they open, and so that a relay that loses power or has a failed coil passes the signal]

3.7.6 Application Separation

****

NOTE: This subpart is only included when the USACE

CW tailoring option is selected
****

Configure operating systems, applications, and network accessible devices using application separation. Utilize the operating system on the primary partition of the hard drive. Install application databases on a different partition than the operating system. Install web servers on a different partition than the operating system. Do not install web servers and database servers on the same computer. Do not host web servers and database servers on the same Virtual Machine.

3.8 SAFE MODE AND FAIL SAFE OPERATION

****
NOTE: The designer should determine, based on the criticality of the controlled equipment, what conditions to consider and which actions, if any, including possible alarm requirements, the control system should take when these conditions are true. This should include external conditions (e.g. loss of off-site utility power), internal conditions (e.g. network or sensor failure), and operator input (e.g. manual command to a safe mode of operation). This should all be specified in the control logic (e.g. sequence of operations), in particular by addressing normal/failed positions of output devices, including default positions upon loss of network, and in the overall system design. Where high reliability is required, the analysis should consider the addition of redundant equipment to the design. See also guidance on SC-24 (Fail in Known State), guidance on SI-17 (Fail-Safe Procedures) and the MINIMUM CYBERSECURITY DESIGN REQUIREMENTS in UFC 4-010-06, Cybersecurity for Facility-Related Control Systems.

Note that any requirements in the control system needed to meet CP-12 (Safe Mode) or SI-17 (Fail-Safe Procedures) should be specified in existing specifications and design, for example, redundant AHUs in the mechanical design and sequences of operation. Any specific requirements for CP-12 or SI-17 should be addressed in those sections, not in this UFGS.
****

{For Government Reference Only: This subpart (and its subparts) relates to CP-12, SI-10(3), SI-17; CCI-002855, CCI-002856, CCI-002857, CCI-002754, CCI-002773, CCI-002774, CCI-002775}

For all control system components with an applicable STIG or SRG, configure the component in accordance with all applicable STIGs and SRGs.

3.9 SYSTEM MAINTENANCE TOOL SOFTWARE

****
NOTE: Indicate the number of hardcopy manuals required.
****

{For Government Reference Only: This subpart (and its subparts) relates to MA-3; CCI-000865.}

Submit and license to the Government all software required to operate, maintain and modify the control system such the Government or their agents are able to perform repair, replacement, upgrades, and expansions of the system, including programming of devices, without subsequent or future dependence on the Contractor, Vendor or Manufacturer. Submit hard copies of user manuals for each software with the software submittal. Provide any hardware keys or dongles, software keys, license numbers, and other information required to enable the Government to access or change the system.

For software provided and licensed to the Government under the requirements of another Section, submit a statement indicating the Section and Submittal under which the software was provided. For software provided to meet the requirements of this Section and not provided and licensed under another Section, submit software and software user manuals on DVD or CD as a Technical Data Package and submit [one hard copy][[_____] hard copies] of the software user manual for each piece of software.

3.10 DEVICE POWER

****

NOTE: A long term alternate power supply is almost never required by the control system itself (independent of the controlled equipment). Alternate long term power, if required, will be because of a tenant requirement or by the overall system design and should seldom be added as an ad-hoc requirement. Control systems for underlying systems with alternate power should use that alternate power source.

A UPS may be desired for specific control system components where rapid recovery after a power outage is required, or where the control system itself is necessary for restoration of power. Again, this should be driven by mission requirements and control system specifications should already require adequate system restoration after loss of power. If there are specific requirements for either short-term (UPS) or long-term (generator or alternate power source), include them as part of the design and in the relevant specification sections rather than adding requirements to this section.

Note that use of small local UPSes creates additional maintenance burdens due to the requirements for periodic battery replacement and may ultimately result in a less reliable system. For MODERATE Impact Systems: This is a particularly important consideration and designers are strongly cautioned against small per-controller UPS and recommended to use a central UPS instead.

Brackets are provided here for the EXTREMELY RARE

case in which emergency power requirements must be specified here. In most cases, keep the bracketed text indicating emergency power requirements are in accordance with the control system and equipment specifications. For MODERATE Impact Systems: As the system has a MODERATE impact there is a particularly strong presumption the mission already requires and is providing emergency power, and the control system should therefore use the same emergency power as the underlying equipment.

****

****

NOTE: For MODERATE Impact Systems, the requirement is for redundant power cabling paths. For this to result in significantly increased availability, the paths must be fed from independent power sources (i.e. the cable paths must be redundant all the way back to redundant power sources). Coordinate with the electrical designer to see if this level of power redundancy has been designed into the system.

If this level of redundancy is required for availability, coordinate with the designer of the controlled equipment (e.g., for HVAC controls, coordinate with the HVAC system designer) to determine if there is a requirement for redundant controlled equipment as well - redundant power to a single piece of controlled equipment still has a single point of failure at the controlled equipment.

The specification requirement covers these issues by simply requiring the controller power to be as reliable as the equipment power. If there is no requirement for redundant (controlled) equipment power or redundant (controlled) equipment, then there is little value in trying to provide redundant power to the control system as the most likely failures are mechanical or electrical failures in the controlled equipment or loss of equipment power, not independent loss of power to the control system.

Note that sequences of operation often lock out equipment in case of failure. Consider carefully how to address general loss of power to ensure that automatic recovery after loss of power is possible.

****

{For Government Reference Only: This subpart (and its subparts) relates to PE-11, PE-11(1); CCI-002955, CCI-000961. For MODERATE Impact systems, this subpart (and its subparts) also relates to PE-9, PE-9(1); CCI-000952, CCI-002953, CCI-002954.}

[For LOW Impact Systems: [Provide emergency power in accordance with the control system and equipment specification Sections, [_____]]

] For MODERATE Impact Systems: Provide control system with power supply meeting or exceeding the reliability of the controlled equipment. Powering control system devices using the same power source as the

equipment controlled by the device is a permissible method of meeting this requirement. Without explicit approval from the government, do not install local uninterruptible power supplies (UPSes) as a source of device power.

3.10.1 Device Behavior on Loss of Power In MODERATE Impact Systems:

****
NOTE: The requirement that "In the event of a loss of power, when power is restored, controllers (and the underlying equipment) must recover and resume their normal sequences of operation." may conflict with the sequence of operation specified in the control system specification. For example, the sequence may normally "lock out" a piece of equipment when power is out (for example, a motor proof). Coordinate with the control system specifications to make sure that equipment can restart after power failure.
****

Application programs and configuration settings must be stored in devices in manner such that a loss of power does not result in a loss of the application program or configuration settings: Loss of power must never result in the loss of application programs, regardless of the length of time power is lost; and loss of power for less than 2,500 hours must not result in the loss of configured settings.

In the event of a loss of power, when power is restored, controllers and computers executing control logic (and the underlying equipment) must recover and resume their normal sequences of operation. Note that the sequence of operation may require specific actions (e.g. startup sequences) upon recovery from loss of power.

3.11 VULNERABILITY SCANNING

****
NOTE: In general, it won't be possible to assume that devices will respond to an IT scanning tool. There might be specific cases where it is desirable for devices to provide specific responses to specific IT tools. If so, add the appropriate requirements to indicate the scanning tools and response information.
****

{For Government Reference Only: This subpart (and its subparts) relates to RA-5 RA-5(a),RA-5(b),RA-5(c),RA-5(d); CCI-001054, CCI-001055, CCI-000156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059. For MODERATE Impact systems, this subpart (and its subparts) also relates to RA-5(1), RA-5(5); CCI-001062, CCI-001067, CCI-001645, CCI-002906.}

All IP devices must be scannable, such that the device can be scanned by industry standard IP network scanning utilities without harm to the device, application, or functionality.

3.11.1 Computers and Software Running on Computers

Computers and applications running on computers must meet relevant

vulnerability scanning STIGs/SRGs and respond to approved DoD vulnerability scanning tools.

3.11.2 Controllers

Provide controllers that are scannable by standard control system discovery tools or control system browsers and return meaningful status information including the network inputs and outputs for the controller. This information must contain sufficient detail to detect vulnerabilities or exploits of the controller.

Provide all software needed to scan the control system as the Control System Scanning Tools submittal. If the software required to scan the system is already installed at the project site or is provided under a separate section instead provide a statement indicating this.

3.12 VULNERABILITY ALERTS

****
NOTE: This subpart is included only when the USACE CW tailoring option is selected
****

Prior to installation, adhere to all vendor-specific and CISA Information Assurance Vulnerability Alert (IAVA, see https://www.cisa.gov/uscert/ncas/alerts) requirements for reporting, patching, and/or mitigating. For alerts which occur after installation but before government acceptance:

a. Notify the Contracting Officer within 48 hours of receipt of the alert and within 48 hours of resolution of vulnerabilities.

b. Resolve the vulnerabilities within 30 days of the alert.

c. Submit a Vulnerability Resolution Report within 14 days of resolving the vulnerabilities in the alert. The report must identify the vulnerability alert ID and the date of resolution for each component.

3.13 FIPS 201-2 REQUIREMENT

****
NOTE: Select brackets to indicate if any systems require devices using PIV to be on the FIPS 201-2 approved product list.

Many control systems will not be able to meet a requirement for devices to be on the FIPS 201-2 approved product lists. Only require this when necessary.
****

{For Government Reference Only: This subpart (and its subparts) relates to SA-4 (10); CCI-003116}

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list (https://www.idmanagement.gov/approved-products-list/): [NONE][electronic security systems(ESS)][_____].

3.14 BIOS/UEFI PROTECTION

****
NOTE: This subpart is included only when the USACE CW tailoring option is selected
****

Provide a protection mechanism to prevent unwanted changes to the system BIOS/UEFI for all devices on the system, where technically feasible. BIOS/UEFI Protection Mechanisms must utilize passwords or passphrases that conform to DoD STIG requirements. BIOS/UEFI Protection passwords must be used to allow access by system engineering and administrative personnel after initial commissioning of the system. Enable UEFI Secure Boot if hardware and Operating System support the option. Provide a BIOS/UEFI Protection Password/Passphrase List (Encrypted) documenting all passwords and passphrases.

3.15 SYSTEM AND INTEGRATION INTEGRITY

3.15.1 Malicious Code Protection

****
NOTE: Malware protection software media may be government or contractor furnished; it may be either Government or contractor installed, and the license may be government or contractor furnished.

For each of media, license and installation select the bracketed text indicating contractor or Government responsibility.

This subpart uses the USACE CW tailoring option. When selected, additional requirements for virus protection and a submittal are included.

****

{For Government Reference Only: This subpart (and its subparts) relates to SI-3(c); CCI-001241, CCI-002623}

For all computers installed under this project, provide malware protection software media, provide licenses, and install and configure malware protection software as indicated. Provide the most up-to-date DoD approved software with up-to-date signatures. Verify that the software does not negatively affect the operation of the OT system. Computers being installed must be configured with up-to-date signatures, not older than 10 days, prior to deployment. Submit Antivirus/Antimalware Scan Results to show evidence of a clean scan. Coordinate with the Government Computer Access Point of Contact as required.

a. [Provide malware protection software licenses.][Malware protection software licenses will be Government furnished.]

b. [Provide malware protection software media.][Malware protection software media will be Government furnished.]

c. [Install and configure malware protection software in accordance with the relevant STIGs.][Malware protection software will be Government installed.]

3.15.2 Software, Firmware, and Information Integrity In MODERATE Impact Systems:

****

NOTE: Integrity checks are a desirable characteristic of critical control systems, but many controls technologies (for example, commercial HVAC controls) do not support their implementation. One example of a controls technology that does meet this is a redundant PLC system where the dual PLCs are set up in a hot swap standby configuration and each PLC has self-check routines to detect a failure and transfer control to the other PLC. Note, however, that the requirement for redundancy is above and beyond what SI-7 control requires (which does not mention redundancy).

If you already have a requirement for redundant controls and if your control technology supports meeting these requirements, then consider adding language (if not already present) similar to the following to your controls specification:
"Controllers that are redundant must be fully redundant and implement hot-standby redundancy where each controller continually monitors its own integrity and process control seamlessly passes from one controller to the other if a loss of integrity is detected."

Including these requirements where not generally supported by the technology will certainly raise the project cost and may result in less reliable systems as the project may be implemented by people who can meet this requirement, but are otherwise inexperienced in the other requirements of the project. (i.e. a factory automation company that does not understand the thermodynamics of HVAC control).

If no integrity verification software is available a compensating approach is to provide fully redundant mechanical systems and a sequence of operation where the two mechanical systems (and their controls) are fully independent such that failure of one controller does not compromise the other redundant system. This will also increase system cost and complexity and should be carefully considered and only implemented when there is a strong project need.

{This paragraph relates to SI-10, Information Input Validation, CCI-001310, CCI-002744.} For MODERATE systems, consider requiring redundant sensors where sensed values are critical inputs to the sequence. User input which could have serious adverse impact on the system should have confirmation dialogs prior to user input. In extreme cases, user inputs should require validation by an additional user prior to input.

{This paragraph relates to SI-11, Error Handling, CCI-001312.} Designer should require alarm messages and other control system feedback to provide notification of errors in support of corrective action. (Note that the DoD definition of recipients for this CCI is not applicable for a control system, and the recipient of these messages should be the entities responsible for the control system operation.)

****

{For Government Reference Only: This subpart relates to CM-5(3); CCI-001749, CCI-002704, CCI-002726}

If there exists Integrity Verification Software that can check boot process, software, firmware, or information in the control system and verify its integrity, provide it. If no such software exists, provide a statement to this affect in lieu of the software.

[The system prevents the installation of software and firmware without verification of the digital signature using an approved certificate.]

[3.15.3 Information System Monitoring

****

NOTE: Delete this subpart unless specifically required for the project. If required, indicate requirements for the monitoring of the control system.

****

{For Government Reference Only: This subpart relates to SI-4 (a),(b); CCI-001253, CCI-002645}

[_____]

]3.16 CONTROL SYSTEM CYBERSECURITY TESTING

{For Government Reference Only: For MODERATE Impact systems, this subpart (and its subparts) relates to SA-11(a), SA-11(b), SA-11(c), SA-11(d), SA-11(e); CCI-003171, CCI-003172, CCI-003173, CCI-003174, CCI-003175, CCI-003176, CCI-003177, CCI-003178.}

3.16.1 Control System Cybersecurity Testing Procedures

Prepare and submit Control System Cybersecurity Testing Procedures explaining step-by-step, the actions and expected results that will demonstrate that the control system meets the requirements of this Section. The Control System Cybersecurity Testing Procedures may be submitted as a Technical Data Package.

3.16.2 Control System Cybersecurity Testing Execution

Using the Control System Cybersecurity Testing Procedures verify that the control system meets the requirements of this Section. UNLESS GOVERNMENT WITNESSING OF A TEST IS SPECIFICALLY WAIVED BY THE GOVERNMENT, PERFORM ALL TESTS WITH A GOVERNMENT WITNESS. If testing reveals deficiencies in the system, correct the deficiency and retest until successful.

3.16.3 Control System Cybersecurity Testing Report

Prepare and submit a Control System Cybersecurity Testing Report documenting all tests performed and their results. Include all tests in the Control System Cybersecurity Testing Procedures and any additional tests performed during testing. Document test failures and repairs conducted with the test results. The Control System Cybersecurity Testing Report may be submitted as a Technical Data Package

3.17 FIELD QUALITY CONTROL, CYBERSECURITY VALIDATION SUPPORT

****

NOTE: Coordinate with the entity performing cybersecurity testing to determine support requirements for cybersecurity testing.

Some possible values to consider:

1) A control system with no IP devices: 1-2 days.

2) A control system with IP devices: 5 days

3) If the system includes a new front-end (server): +5 additional days

****

In addition to testing and testing support required by other Sections, provide a minimum of [_____] hours of technical support for cybersecurity testing of control systems to support the DoD Risk Management Framework process Cybersecurity assessment of the control system. This support is independent of (and in addition to) the Control System Cybersecurity Testing specified in this section.

3.18 CYBERSECURITY TRAINING

****

NOTE: Indicate the number of hours of training and number of attendees. Unless training is specifically waived by the project site, DO NOT remove training requirements.

****

Provide [eight][_____] hours of classroom[and hands-on] training for [six][_____] Government personnel on the cybersecurity operation and maintenance of the control system provided. This training is in addition to and must be coordinated with control system training specified in other Sections.

The Government will provide the training location. Training must cover, at a minimum: (a) applying software and firmware updates, (b) user account creation, modification and deletion, (c) audit log upload procedures and (d) identification of privileged user interfaces and system impact of those interfaces. Training session must include a question and answer period during which government staff questions about cybersecurity aspects of the control system are answered.

-- End of Section --