UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2021
****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS

11/17

PART 1 GENERAL

1.1 CONTROL SYSTEM APPLICABILITY
1.2 RELATED REQUIREMENTS
1.3 REFERENCES
1.4 DEFINITIONS
1.4.1 Computer
1.4.2 Network Connected
1.4.3 User Account Support Levels
1.4.3.1 FULLY Supported
1.4.3.2 MINIMALLY Supported
1.4.3.3 NOT Supported
1.4.4 User Interface
1.4.4.1 Limited Local User Interface
1.4.4.2 Full Local User Interface
1.4.4.3 Remote User Interface
1.5 ADMINISTRATIVE REQUIREMENTS
1.5.1 Coordination
1.6 SUBMITTALS
1.7 QUALITY CONTROL
1.7.1 Regulatory Requirements
1.7.2 [Certifications][Qualifications]
1.7.3 Pre-Construction Testing
1.8 DELIVERY, STORAGE, AND HANDLING
1.9 CYBERSECURITY DOCUMENTATION
1.9.1 Cybersecurity Interconnection Schedule
1.9.2 Network Communication Report
1.9.3 Control System Inventory Report
1.9.4 Software Recovery and Reconstitution Images
1.9.5 Cybersecurity Riser Diagram
1.9.6 Control System Cybersecurity Documentation
1.9.6.1 Software Applications
1.9.6.2 For HVAC Control System Devices
1.9.6.2.1 HVAC Control System Devices FULLY Supporting User Accounts
1.9.6.2.2 All Other HVAC Control System Devices
1.9.6.3 [_____] Control System Devices

1.9.6.4 Default Requirements for Control System Devices
1.10 SOFTWARE UPDATE LICENSING
1.11 CYBERSECURITY DURING CONSTRUCTION
1.11.1 Contractor Computer Equipment
1.11.1.1 Operating System
1.11.1.2 Anti-Malware Software
1.11.1.3 Passwords and Passphrases
1.11.1.4 Contractor Computer Cybersecurity Compliance Statements
1.11.2 Temporary IP Networks
1.11.2.1 Network Boundaries and Connections
1.11.3 Government Access to Network
1.11.4 Temporary Wireless IP Networks
1.11.5 Passwords and Passphrases
1.11.6 Contractor Temporary Network Cybersecurity Compliance Statements
1.12 CYBERSECURITY DURING WARRANTY PERIOD

PART 2 PRODUCTS

PART 3 EXECUTION

3.1 ACCESS CONTROL REQUIREMENTS
3.1.1 User Accounts
3.1.1.1 Computers
3.1.1.2 For HVAC Control System Devices
3.1.1.3 [_____] Control System Devices
3.1.1.4 Default Requirements for Control System Devices
3.1.2 Unsuccessful Logon Attempts
3.1.2.1 Devices MINIMALLY Supporting Accounts
3.1.2.2 Devices FULLY Supporting Accounts
3.1.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements
3.1.3 System Use Notification
3.1.3.1 User Interface Banner Schedule
3.1.4 Permitted Actions Without Identification or Authentication
3.1.5 Wireless Access
3.1.5.1 Wireless IP Communications
3.1.5.2 Non-IP Wireless Communication
3.1.5.3 Wireless Communication Request
3.1.5.4 Wireless Communication Testing
3.2 CYBERSECURITY AUDITING
3.2.1 Audit Events, Content of Audit Records, and Audit Generation
3.2.1.1 Computers
3.2.1.1.1 Audited Events
3.2.1.1.2 Audit Event Information To Record
3.2.1.2 For HVAC Control System Devices
3.2.1.2.1 HVAC Control System Devices FULLY Supporting User Accounts
3.2.1.2.2 Other HVAC Control System Devices
3.2.1.3 [_____] Control System Devices
3.2.1.4 Default Requirements for Control System Devices
3.2.1.4.1 Devices Which FULLY Support Accounts
3.2.1.4.1.1 Audited Events
3.2.1.4.1.2 Audit Event Information To Record
3.2.1.4.2 Devices Which Do Not FULLY Support Accounts
3.2.2 Audit Storage Capacity and Audit Upload
3.2.2.1 Device Audit Record Upload Software
3.2.3 Response to Audit Processing Failures

3.2.4 Time Stamps
3.2.4.1 Computers
3.2.4.2 For HVAC Control System Devices
3.2.4.3 [_____] Control System Devices
3.2.4.4 Default Requirements for Control System Devices
3.3 REQUIREMENTS FOR LEAST FUNCTIONALITY
3.3.1 Non-IP Control Networks
3.3.2 IP Control Networks
3.4 SAFE MODE AND FAIL SAFE OPERATION
3.5 IDENTIFICATION AND AUTHENTICATION
3.5.1 User Identification and Authentication
3.5.1.1 HVAC Control Systems Devices
3.5.1.2 Electronic Security System Devices
3.5.1.3 [_____] Control System Devices
3.5.1.4 Default Requirements for Control System Devices
3.5.2 Authenticator Management
3.5.2.1 Authentication Type
3.5.2.1.1 For HVAC Control System Devices
3.5.2.1.2 [_____] Control System Devices
3.5.2.1.3 Default Requirements for Control System Devices
3.5.2.2 Password-Based Authentication Requirements
3.5.2.2.1 Passwords for Computers
3.5.2.2.2 Passwords for Non-Computer Devices FULLY Supporting Accounts
3.5.2.2.3 Passwords for Web Interfaces
3.5.2.2.4 Passwords for Devices Minimally Supporting Accounts
3.5.2.2.5 Password Configuration and Reporting
3.5.2.3 Hardware Token-Based Authentication Requirements
3.5.3 Authenticator Feedback
3.5.4 Device Identification and Authentication
3.5.4.1 For HVAC Control System Devices
3.5.4.2 [_____] Control System Devices
3.5.4.3 Default Requirements for Control System Devices
3.5.5 Cryptographic Module Authentication
3.6 EMERGENCY POWER
3.7 DURABILITY TO VULNERABILITY SCANNING
3.7.1 HVAC Control System Devices Other Than Computers
3.7.2 [_____] Control System Devices Other Than Computers
3.7.3 Default Requirements for Control System Devices
3.8 FIPS 201-2 REQUIREMENT
3.9 DEVICES WITH CONNECTION TO MULTIPLE IP NETWORKS
3.10 SYSTEM AND COMMUNICATION PROTECTION
3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection
3.10.2 Cryptographic Protection
3.11 SYSTEM AND INTEGRATION INTEGRITY
3.11.1 Malicious Code Protection
3.11.2 Information System Monitoring
3.12 FIELD QUALITY CONTROL
3.12.1 Tests

-- End of Section Table of Contents --

****
USACE / NAVFAC / AFCEC / NASA **UFGS-25 05 11 (November 2017)**

Preparing Activity: USACE

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated January 2021
****

SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
11/17

****
NOTE: This guide specification covers the requirements for cybersecurity for facility-related control systems.

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.

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: Control System Cybersecurity Center of Expertise,
Huntsville Engineering and Support Center

Navy: Naval Facilities Engineering Command,
Command Information Office (CIO)

Air Force: Civil Engineer Maintenance,
Inspection, and Repair Team (CEMIRT)
ICS Branch, Tyndall AFB

Marine Corps: Contact Navy POC for Marine Corps
POC information

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 Section is for use on control systems with no impact rating higher than LOW. If the project includes systems where there systems with impact ratings of MODERATE or 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 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.

****

****

NOTE: This specification makes use of SpecsIntact Tailoring Options.

Services tailoring options:
Army
Air Force

Control system type tailoring options:
HVAC Control Systems
Electronic Security Systems (ESS)

****

PART 1 GENERAL

****

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.

****

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 are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

[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

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.

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	(2016) 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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

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 Computer

As used in this Section, 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 OS, where Android is considered separate from Linux

e. a device running a version of Apple iOS

1.4.2 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 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).

Any device that supports wireless communication is network connected, regardless of whether the device is communicating using wireless.

1.4.3 User Account Support Levels

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

1.4.3.1 FULLY Supported

Device supports configurable individual accounts. Accounts can be created, deleted, modified, etc. Privileges can be assigned to accounts.

1.4.3.2 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 "user name and password" structure).

1.4.3.3 NOT Supported

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

1.4.4 User Interface

Generally, a user interface is hardware on a device allowing user interaction with that device via input (buttons, switches, sliders, keyboard, touch screen, etc.) and a screen. There are three types of user interfaces defined in this Section: Limited Local User Interface, Full Local User Interface and Remote User Interface. In this Section, when the term "User Interface" is used without specifying which type, it refers only to Full Local User Interface and Remote User Interface (NOT to Limited Local User Interface).

1.4.4.1 Limited Local User Interface

A Limited Local User Interface is a user interface where the interaction is limited, fixed at the factory, and cannot be modified in the field. The user must be physically at the device to interact with it.

Examples of Limited Local User Interface include thermostats (Space Sensor Modules as defined in Section 23 09 13 INSTRUMENTATION AND CONTROL DEVICES FOR HVAC).

1.4.4.2 Full Local User Interface

A Full Local User Interface is a user interface where the interaction and displays are field-configurable.

Examples of a Full Local User Interface include local applications on a computer and user interfaces to Variable Speed Drives.

1.4.4.3 Remote User Interface

A Remote User Interface is a user interface on a Client device allowing user interaction with a different Server device. The user need not be physically at the Server device to interact with it.

Examples of Remote User Interfaces include web browsers and Local Display Panels as defined in Section 23 09 00 INSTRUMENTATION AND CONTROL FOR HVAC.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Coordination

****

NOTE: This subpart deals with 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 communication, the Wireless Communication Request submittal must be approved prior to control system device selection and integration.

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 integration.

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

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. 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, HTTP web server certificates must be obtained from the indicated contact for the project site.

j. Contractor Computer Cybersecurity Compliance Statements 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, Air Force, and NASA projects.

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.

Choose the first bracketed item for Navy, Air Force and NASA projects, or choose the second bracketed item for Army projects.
****

****
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.
****

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.][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

Wireless Communication Request; G[, [_____]]

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

Multiple IP Connection Device Request; G[, [_____]]

Contractor Computer Cybersecurity Compliance Statements; G[, [_____]]

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

SD-02 Shop Drawings

User Interface Banner Schedule; G[, [_____]]

Network Communication Report; G[, [_____]]

Cybersecurity Riser Diagram; G[, [_____]]

Control System Inventory Report; G[, [_____]]

Cybersecurity Interconnection Schedule; G[, [_____]]

SD-03 Product Data

Control System Cybersecurity Documentation; G[, [_____]]

SD-06 Test Reports

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

SD-07 Certificates

Software Licenses; G[, [_____]]

SD-11 Closeout Submittals

Password Summary Report; G[, [_____]]

Software Recovery And Reconstitution Images; G[, [_____]]

Device Audit Record Upload Software; G[, [_____]]

1.7 QUALITY CONTROL

[1.7.1 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: [_____].

][1.7.2 [Certifications][Qualifications]

****

NOTE: 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: [_____].

][1.7.3 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.

****

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

][1.8 DELIVERY, STORAGE, AND HANDLING

****

NOTE: If there are delivery, storage or handling requirements, 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.

****

[_____]

]1.9 CYBERSECURITY DOCUMENTATION

[1.9.1 Cybersecurity Interconnection Schedule

****

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 Reference Only: This subpart (and its subparts) relates to CA-3(b), CCI-00258}

Provide a completed Cybersecurity Interconnection Schedule documenting connections between the installed system and other systems. Provide the following information for each device communicating between systems: Device Identifier, 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.] 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 http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic

]1.9.2 Network Communication 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 Reference Only: This subpart (and its subparts) relates to CA-9; CCI-002102, CCI-002103, CCI-002104, CCI-002105 and also the submittal requirements associated with CM-6, CM-7 and SC-41}

Provide a network communication report. For each networked controller, document the communication characteristics of the controller including communication protocols, services used, and a general description of what information is communicated over the network. For each controller using IP, document all TCP and UDP ports 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 Report as an editable Microsoft Excel file.

1.9.3 Control System Inventory Report

****

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.
****

{For Reference Only: This subpart (and its subparts) relates to CM-8(a), CP-12, SI-17, IA-3; CCI-000389, CCI-000392, CCI-000398, CCI-002855, CCI-002856, CCI-002857, CCI-002773, CCI-002774, CCI-002775, CCI-000777, CCI-000778, CCI-001958}

Provide a Control System Inventory report using the Inventory Spreadsheet listed under this Section at http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic documenting 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)]. 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 Report as an editable Microsoft Excel file.

1.9.4 Software Recovery and Reconstitution Images

****

NOTE: This requirement covers disk images to allow recovery and reconstitution of applications on computers. 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.

This requirement covers computers only. If recovery images of other control system devices (controllers) are needed, that should be specified in the relevant control system Section or added here. Use caution when adding a requirement for controllers here as not all systems have the same capabilities and a general requirement here could result in a conflicting or impractical requirement.

If the contractor is installing software on a Government Furnished computer to which they may not have sufficient permissions, include the bracketed text and indicate a POC for assistance with creating the image.

****

{For 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. 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 [_____].]

1.9.5 Cybersecurity Riser Diagram

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

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

Provide a cybersecurity riser diagram of the complete control system including all network and controller hardware. 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][_____].

1.9.6 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:

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 [fill in the blank] control devices
4) Default requirements for control system devices (when not covered in 1-3 above)

If the project incorporates devices other than HVAC devices, and the general requirements in sub-paragraph 4 are not satisfactory, add requirements to subparagraph 3. If multiple different requirements are needed (e.g. the project incorporates a micro-grid and and an electronic security system, both with specific requirements) add additional paragraphs similar to paragraph 3. Leave the "devices not otherwise covered" at the end of the list and do not edit those requirements.

Note that within HVAC 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 control devices.
****

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

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

1.9.6.1 Software Applications

For all software applications running on computers provide:

a. administrator documentation that describes secure configuration of the software {relates to CCI-003124}

b. administrator documentation that describes secure installation of the software {relates to CCI-003125}

c. administrator documentation that describes secure operation of the software {relates to CCI-003124}

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

e. administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software {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 {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 {relates to CCI-003130}

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

1.9.6.2 For HVAC Control System Devices

1.9.6.2.1 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 reference only: relates to CCI-003124}

b. Documentation that describes secure operation of the device {for reference only: relates to CCI-003124}

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {for 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 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 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 reference only: relates to CCI-003130}

1.9.6.2.2 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 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 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 reference only: relates to CCI-003130}

[1.9.6.3 [_____] 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 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.
****

[_____]

]1.9.6.4 Default Requirements for Control System Devices

****
NOTE: Do not edit these requirements. If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.
****

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

reference only: relates to CCI-003124}

b. Documentation that describes secure installation of the device {for reference only: relates to CCI-003125}

c. Documentation that describes secure operation of the device {for reference only: relates to CCI-003124}

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device {for 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 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 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 reference only: relates to CCI-003130}

h. Documentation that describes user responsibilities in maintaining the security of the device {for reference only: relates to CCI-003131}

1.10 SOFTWARE UPDATE 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 Reference Only: This subpart (and its subparts) relates to SI-2 (a),(c); CCI-001227, CCI-002605}

In addition to all other licensing requirements, all software licensing must include licensing of the following software updates for a period [of no less than 5 years][____]:

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

1.11 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.
****

{For Reference Only: This subpart (and its subparts) relates to AC-18, SA-3, CCI-00258}

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

1.11.1 Contractor Computer Equipment

Contractor owned computers may be used for construction. When used, contractor computers must meet the following requirements:

1.11.1.1 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.

1.11.1.2 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. All computers used on this project must be scanned using the installed software at least once per day.

1.11.1.3 Passwords and Passphrases

The passwords and passphrases for all computers 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.

1.11.1.4 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 http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic Each Statement must be signed by a cybersecurity representative for the

relevant company.

1.11.2 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 must meet the following requirements:

1.11.2.1 Network Boundaries and Connections

The network must not extend outside the project site and must not connect to any IP network other than IP networks provided under this project or Government furnished IP networks provided for this purpose. Any and all network access from outside the project site is prohibited.

1.11.3 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

1.11.4 Temporary Wireless IP Networks

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

1.11.5 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.

1.11.6 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 http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic 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.

1.12 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

(NOT USED)

PART 3 EXECUTION

3.1 ACCESS CONTROL REQUIREMENTS

3.1.1 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.

DO NOT ALLOW AN INTERFACE THAT DOES NOT SUPPORT ACCOUNTS TO HAVE THE CAPABILITY TO ALTER THE CONTROL SYSTEM.

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 Reference Only: This subpart (and its subparts) relate to AC-2(a)and AC-3; CCI-002110, CCI-000213.}

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

3.1.1.1 Computers

All computers must FULLY support user accounts.

3.1.1.2 For HVAC Control System Devices

Devices with web interfaces must either FULLY support user accounts or have their web interface disabled. Field devices with full local user interfaces allowing modification of data must at least MINIMALLY support user accounts.

[3.1.1.3 [_____] 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 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.

****

[_____]

]3.1.1.4 Default Requirements for Control System Devices

****

NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.

****

****

NOTE: Select the appropriate minimum account support for web interfaces.

Select the appropriate minimum account support for local user interfaces allowing modification of data. In general, keep "at least MINIMALLY" unless otherwise required for the project.

Keep or include user account requirements for read-only interfaces. If keeping the requirement, select the appropriate user account support. In general either remove this text (to allow read-only interfaces with no accounts) or keep "at least MINIMALLY" unless otherwise required for the project.

Unless specifically required by the project DO NOT keep bracketed text requiring all devices to at least MINIMALLY support accounts as this increases system complexity and cost and requires operation and maintenance staff to maintain passwords for all devices.

****

For control system devices where User Account requirements are not otherwise indicated in this Section:

a. Devices with web interfaces must either [FULLY][at least MINIMALLY] support user accounts or have their web interface disabled.

b. Field devices with full local user interfaces allowing modification of data must [at least MINIMALLY][FULLY] support user accounts.

[c. Field devices with read-only full local user interfaces must [at least MINIMALLY][FULLY] support user accounts.

][d. All devices must at least MINIMALLY support user accounts.

]3.1.2 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.

****

{For Reference Only: This subpart (and its subparts) relate 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.

3.1.2.1 Devices MINIMALLY Supporting Accounts

****

NOTE: 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 account lock to specify a reasonable requirement that will not introduce an additional O&M burden.

****

Devices which MINIMALLY support accounts [are not required to lock based on unsuccessful logon attempts][must lock the user input when [_____] and must support unlocking of the user input when [_____]].

3.1.2.2 Devices FULLY Supporting Accounts

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

Devices which FULLY support accounts must meet the following requirements. If a device cannot meet these requirements, document device capabilities to protect from subsequent unsuccessful logon attempts and propose alternate protections in a Device Account Lock Exception Request submittal. Do not implement alternate protection measures without explicit permission from the Government.

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.

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

3.1.2.3 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**
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]
[_____]	[_____]	[_____]

]

3.1.3 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 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}

Web interfaces must display a warning banner meeting the requirements of DTM 08-060.

Devices which are connected to a network and have a user interface must display a warning banner meeting the requirements of DTM 08-060 if capable of doing so. Devices which are connected to a network and have a user interface but are not capable of displaying a banner must have a permanently affixed label displaying an approved banner from DTM 08-060.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 contract between font and background colors.

3.1.3.1 User Interface Banner Schedule

Provide a User Interface Schedule using the format indicated showing each user interface provided and how the information banner requirement has been implemented for each user interface.

User Interface Schedule Format (with sample entries)			
User Interface Description	**User Interface Location**	**Type of User Interface**	**Banner Implementation**
Sample 1	Room 1	Remote	DTM 08-060 Banner "A" Displayed at Logon
Sample 2	Room 2	Limited Local	DTM 08-060 Banner "B" on Affixed Label
Sample 3	Room 3	Full Local	DTM 08-060 Banner "B" Displayed on Screen

3.1.4 Permitted Actions Without Identification or Authentication

****

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

Notes concerning how this requirement addresses cybersecurity:

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 "viewing read-only information from devices which are not required to have user accounts."

****

{For 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 by a user acting from a user interface which MINIMALLY or FULLY supports accounts.

3.1.5 Wireless Access

****

NOTE: Avoid wireless to the greatest extent possible. Wireless may be considered for retrofits where running wires would be prohibitive, but other technologies (such as powerline carrier) should be considered first.

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

Unless explicitly authorized by the Government, do not use any wireless communication. Any device with wireless communication capability is considered to be using wireless communication, regardless of whether or not the device is actively communicating wirelessly, except when wireless communication has been physically permanently disabled (such as through the removal of the wireless transceiver).

3.1.5.1 Wireless IP Communications

[Unless specifically approved and installed in accordance with the project site requirements, d][D]o not install wireless 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.

3.1.5.2 Non-IP Wireless Communication

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.

3.1.5.3 Wireless Communication Request

****

NOTE: The wireless 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 communication prior to beginning construction using the Wireless Communication Request Schedule at http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic

For each device proposed to use wireless 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, RF Frequency, Radiated Power in dBm (decibel with a milliwatt reference), free-space range, and the expected as-installed range.

3.1.5.4 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 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 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 devices.**

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 timestamps, 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.

****

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

{For Reference Only: This subpart (and its subparts) relates to AU-2(a),(c),(d), AU-3, AU-12; CCI-000123, CCI-001571, CCI-000125, CCI-001485, CCI-000130, CCI-000131, CCI-000132, CCI-00133, CCI-000134, CCI-001487, CCI-000169, CCI-001459, CCI-000171, CCI-000172, CCI-001910}

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.

3.2.1.1 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

3.2.1.1.1 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)

a. Successful and unsuccessful logon attempts

b. Privileged activities or other system level access

c. Starting and ending time for user access to the system

d. Concurrent logons from different workstations

e. Successful and unsuccessful accesses to objects

f. All program initiations

g. All direct access to the information system

h. All account creations, modifications, disabling, and terminations

i. All kernel module load, unload, and restart

3.2.1.1.2 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

3.2.1.2 For HVAC Control System Devices

3.2.1.2.1 HVAC Control System Devices FULLY Supporting User Accounts

For devices FULLY supporting accounts, provide the capability to select audited events, and the contents of audit logs. Configure devices to audit the following events:

a. Successful and unsuccessful logon attempts to the device

b. Starting and ending time for user access to the device

c. All account creations, modifications, disabling, and terminations

d. All device shutdown and startup

Configure the device to record for each event the following information (as applicable): the type of event, when the event occurred and the identity of any individuals or subjects associated with the event

3.2.1.2.2 Other HVAC Control System Devices

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

[3.2.1.3 [_____] 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 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.
****

[_____]

]3.2.1.4 Default Requirements for Control System Devices

****
NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.
****

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

3.2.1.4.1 Devices Which FULLY Support Accounts

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

3.2.1.4.1.1 Audited Events

Configure each device 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)

a. Successful and unsuccessful logon attempts

b. Privileged activities or other system level access

c. Starting and ending time for user access to the system

d. Concurrent logons from different workstations

e. All account creations, modifications, disabling, and terminations

f. All kernel module load, unload, and restart

3.2.1.4.1.2 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

3.2.1.4.2 Devices Which Do Not FULLY Support Accounts

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

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

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 non-computer control system devices 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.]

3.2.2.1 Device Audit Record Upload Software

****
NOTE: Select or indicate desired export target for audit upload software.

Select and indicate where upload software is to be

installed, if it is to be installed. If there is no front end on which to install the software and there are no computers installed under this project onto which is should be loaded remove both sets of bracketed text.

Note that this software may not be required if there are no devices other than computers which audit events.

****

For each non-computer device required to audit events, provide, and license to the Government, software implementing a secure mechanism of uploading audit records from the device to a computer and of exporting the uploaded audit records as a [Microsoft Excel file][comma separated value text file][Microsoft Excel file or comma separated value text file][_____]. Where different devices use different software, provide software of each type required to upload audit logs from all devices.

[Install device audit record upload software on the furnished front end computer in [_____].][Install device audit record upload software on [_____].]Submit copies of device audit record upload software. If there are no non-computer devices requiring auditing, provide a document stating this in lieu of this submittal.

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

Front end computers associated with auditing must, in the case of a failure in the auditing system, notify [_____] via [e-mail][_____]. In case of an audit failure, if possible, continue to collect audit records by [overwriting existing audit records][_____].

3.2.4 Time Stamps

{For Reference Only: This subpart (and its subparts) relates to AU-8; CCI-000159, CCI-001889, CCI-001890}

3.2.4.1 Computers

****

NOTE: Note that the timing requirement for computers may require communication through a firewall to allow NTP or SNTP to get time updates.

****

Computers generating audit records must have internal clocks capable of providing time with a resolution of 1 second. Clocks must not drift more than 10 seconds per day.

Configure the system so that each computer generating audit records maintains accurate time to within 1 second.

3.2.4.2 For HVAC Control System Devices

****

NOTE: For HVAC Control Systems, the timing requirements inherent in the control systems and specified in Section 23 09 23.01 LONWORKS DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS, Section 23 09 23.02 BACNET DIRECT DIGITAL CONTROL FOR HVAC AND OTHER BUILDING CONTROL SYSTEMS, and Section 25 10 10 UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION should be sufficient.

Unless otherwise required, keep the first bracketed text ("Time stamp requirements for HVAC Control Systems are as indicated in the HVAC Control System specifications.") and remove the timing requirements in the second bracketed text.

Note that HVAC control devices may not be able to meet the timing requirements in the second set of bracketed text.

****

[Time stamp requirements for HVAC Control Systems are as indicated in the HVAC Control System specifications.][Devices generating audit records must have internal clocks capable of providing time with a resolution of 1 second. Clocks cannot drift more than 10 seconds per day. Configure the system so that each device generating audit records maintains accurate time to within 1 second.]

[3.2.4.3 [_____] 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 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.

****

****

NOTE: Indicate the control system and select or indicate the timing requirements for that control system.

****

[_____][Time stamp requirements for [_____] Control Systems are as indicated in the Control System specifications.][Devices generating audit records must have internal clocks capable of providing time with a resolution of 1 second. Clocks cannot drift more than 10 seconds per day. Configure the system so that each device generating audit records maintains accurate time to within 1 second.]

]3.2.4.4 Default Requirements for Control System Devices

****

NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.

****

For control system devices where Time Stamps requirements are not otherwise indicated in this Section: Devices generating audit records must have internal clocks capable of providing time with a resolution of 1 second. Clocks must not drift more than 10 seconds per day. Configure the system so that each device generating audit records maintains accurate time to within 1 second.

3.3 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 Reference Only: This subpart (and its subparts), along with the network communication report submittal specified elsewhere in this section, relates to CM-6 (a), (c), CM-7, CM-7 (1)(b), SC-41; CCI-000363, CCI-000364, CCI-000365, CCI-001588, CCI-001755, CCI-000381, CCI-000380, CCI-00382, CCI-001761, CCI-001762, CCI-002544, CCI-002545, CCI-002546.}

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.

For HVAC Control Systems: Do not provide devices with 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: [Do not provide devices with user interfaces

where one was not required.] [Do not use a networked sensor or actuator where a non-networked sensor or actuator would suffice.]

3.3.1 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, or use any protocol on ports other than those specified.

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

3.3.2 IP Control Networks

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.

3.4 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 Reference Only: This subpart (and its subparts) relates to CP-12,

SI-17; CCI-002855, CCI-002856, CCI-002857, 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.

3.5 IDENTIFICATION AND AUTHENTICATION

3.5.1 User Identification and Authentication

{For Reference Only: This subpart (and its subparts) relates to IA-2,(1),(12); CCI-000764, CCI-000765, CCI-001953, CCI-001954}

a. Devices that FULLY support accounts must uniquely identify and authenticate organizational users.

b. Devices which allow network access to privileged accounts must implement multifactor authentication for network access to privileged accounts.

3.5.1.1 HVAC Control Systems Devices

Identification and Authentication for network access to privileged accounts must be implemented by either accepting and electronically verify Personal Identity Verification (PIV) credentials or inheriting identification and authentication from the operating system.

3.5.1.2 Electronic Security System Devices

****

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

****

Identification and Authentication for network access to privileged accounts must be implemented by [accepting and electronically verifying Personal Identity Verification (PIV) credentials][or][inheriting identification and authentication from the operating system][or][_____].

[3.5.1.3 [_____] 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 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.

****

[_____]

]3.5.1.4 Default Requirements for Control System Devices

****

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

Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.

****

For control system devices where User Identification and Authentication requirements are not otherwise indicated in this Section, User Identification and Authentication for network access to privileged accounts must be implemented by [accepting and electronically verify Personal Identity Verification (PIV) credentials][or][inheriting identification and authentication from the operating system][or][_____].

3.5.2 Authenticator Management

{For Reference Only: This subpart (and its subparts) relates to IA-5 (b),(c),(e),(g),(1),(11); CCI-000176, 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}

3.5.2.1 Authentication Type

3.5.2.1.1 For HVAC Control System Devices

****

NOTE: Coordinate with the project site to determine the appropriate authenticator type for software.

****

Unless otherwise indicated:

a. Software which FULLY supports accounts and which runs on a computer must use [password-based authentication or hardware token-based authentication][password-based authentication][hardware token-based authentication].

b. Other devices which FULLY support accounts must use password-based authentication.

c. Devices MINIMALLY supporting accounts must use password-based authentication.

[3.5.2.1.2 [_____] 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 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.
****

[_____]

]3.5.2.1.3 Default Requirements for Control System Devices

****
NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.
****

****
NOTE: Indicate required authenticator type. Unless specifically required by the project, do not require all devices that FULLY support accounts to use hardware token-based authentication.

****

For control system devices where Authentication Type requirements are not otherwise indicated in this Section:

a. Software which FULLY supports accounts and which runs on a computer must use [password-based authentication or hardware token-based authentication][password-based authentication][hardware token-based authentication].

b. Other devices which FULLY support accounts must use [either password-based authentication or hardware token-based authentication][password-based authentication][hardware token-based authentication].

c. Devices MINIMALLY supporting accounts must use [either password-based authentication or hardware token-based authentication][password-based authentication][hardware token-based authentication].

3.5.2.2 Password-Based Authentication Requirements

3.5.2.2.1 Passwords for Computers

All 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.

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 no 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.

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

3.5.2.2.2 Passwords for Non-Computer Devices FULLY Supporting Accounts

All non-computer devices FULLY supporting accounts and supporting password-based authentication must enforce the following requirements:

a. Minimum password length of twelve (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.

f. Password must have a maximum lifetime of sixty (60) days. When passwords expire, prompt users to change passwords. Do no lock accounts due to expired passwords.

g. Password must differ from previous five (5) passwords, where differ is defined as changing at least fifty percent of the characters.

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

3.5.2.2.3 Passwords for Web Interfaces

Passwords for connecting to a web 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.

f. Password must have a maximum lifetime of 60 days. When passwords expire, prompt users to change passwords. Do no 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.

3.5.2.2.4 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.

3.5.2.2.5 Password Configuration and Reporting

****

NOTE: 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 DPW. This report is required to be delivered as hardcopy in a sealed envelope to keep passwords more confidential.

****

For all devices with a password, change the password from the default password. Coordinate selection of passwords with [_____]. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Password Summary 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.

3.5.2.3 Hardware Token-Based Authentication Requirements

Devices supporting hardware token-based authentication must use Personal Identity Verification (PIV) credentials for the hardware token.

3.5.3 Authenticator Feedback

{For 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.

3.5.4 Device Identification and Authentication

****

NOTE: Indicate whether certificates for HTTPS will be provided by a Government POC, and if so who will provide them. Coordinate this requirement with the project site, and with thecontrol system specification as this may already be specified there.

Wireless IP communication needs to be explicitly permitted via the wireless communication request submittal, and requires an existing Government-provided WiFi network. If a WiFi network is available for potential contractor use, include the bracketed text requiring wireless IP authentication and coordinate with the IT staff to indicate the authentication mechanism. If no WiFi network will be available, remove this bracketed text.

****

{For Reference Only: This subpart (and its subparts) relates to IA-3; CCI-000777, CCI-000778, CCI-001958}

All computers must use IEEE 802.1x for authentication to the network. All web servers running on computers must use HTTPS[and must implement HTTPS using web server certificates obtained from [_____]].[When wireless IP devices are permitted, they must use [_____] for authentication.]

3.5.4.1 For HVAC Control System Devices

****

NOTE: Indicate whether certificates for HTTPS will be provided, and if so who will provide them.

Unless otherwise required, if the project allows the Niagara Framework, require Fox Protocol components to support 802.1x.

If widely supported, require Ethernet devices to meet 802.1x. Note many IP-based controller 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.

Do not require Network Security with BACnet without determining both a) that it is a specific project requirement, and b) that it can be met by multiple vendors.

****

Devices using Fox Protocol must use HTTPS[using a web server certificate obtained from [_____]]. [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 in Clause 24 of ASHRAE 135.]

[3.5.4.2 [_____] 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 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.
****

[_____]

]3.5.4.3 Default Requirements for Control System Devices

****
NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.

If widely supported, require Ethernet devices to meet 802.1x. Note many IP-based controller 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.

Indicate whether certificates for HTTPS will be provided, and if so who will provide them.
****

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[using a web server certificate obtained from [_____]] instead.

3.5.5 Cryptographic Module Authentication

****
NOTE: As of July 2017 there are no known STIGs/SRGs related to this requirement which apply to HVAC control systems.
****

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

For devices that have STIG/SRGs related to cryptographic module authentication (CCI-000803), comply with the requirements of those STIG/SRGs.

3.6 EMERGENCY POWER

****

NOTE: A long term alternate power supply is almost never required by the control system itself, this will usually be required (if at all) by tenant requirements 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.

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 Reference Only: This subpart (and its subparts) relates to PE-11,(1); CCI-02955, CCI-000961}

[Emergency power is specified in the control system and equipment specifications.][_____]

3.7 DURABILITY TO VULNERABILITY SCANNING

****

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

For computers, select whether the computer must respond in specific ways to scans. If so, keep the bracketed text and define specific scanning tools and response. If not, remove the bracketed text.

****

{For Reference Only: This subpart (and its subparts) relates to RA-5 (a),(b),(c),(d); CCI-001054, CCI-001055, CCI-0010156, CCI-001641, CCI-001643, CCI-001057, CCI-001058, CCI-001059}

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.

[Computers must respond to scans from [_____] by responding with a [_____].]For control system devices other than computers:

3.7.1 HVAC Control System Devices Other Than Computers

HVAC control system devices other than computers are not required to respond to scans.

[3.7.2 [_____] Control System Devices Other Than Computers

****
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 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.
****

****
NOTE: Select whether control system devices must respond to scans and, if so, indicate the tools and the response required.
****

[_____] control system devices other than computers [must respond to scans from [_____] by responding with a [_____]][are not required to respond to scans].

]3.7.3 Default Requirements for Control System Devices

****
NOTE: Do not edit these requirements (beyond selection of bracketed text). If these requirements do not apply to a specific control system used on the project, include requirements for that control system using the bracketed subpart provided above.
****

****
NOTE: Select whether control system devices must respond to scans and, if so, indicate the tools and the response required.
****

Non-computer control system devices where Durability to Vulnerability

Scanning requirements are not otherwise indicated in this Section [must respond to scans from [_____] by responding with a [_____]][are not required to respond to scans].

3.8 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 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: [NONE][electronic security systems(ESS)][_____].

3.9 DEVICES WITH CONNECTION TO MULTIPLE IP NETWORKS

Except for Ethernet switches, do not use more than one physical connection to IP networks on the same device unless doing so is both required by the project specifications and the specific application is approved. If a device with multiple IP connections is required, provide a Multiple IP Connection Device Request using the Multiple IP Connection Device Request Schedule at http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphic to request approval for each device.

3.10 SYSTEM AND COMMUNICATION PROTECTION

3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection

****

NOTE: 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.

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

****

{For Reference Only: This subpart (and its subparts) relates to SC-5, SC-39, SC-7(a); CCI-001093, CCI-002385, CCI-002386, CCI-002430, CCI-001097}

To the greatest extent practical, implement control logic in non-computer hardware and without reliance on the network.

[3.10.2 Cryptographic Protection

****

NOTE: With regard to cryptography, there are 3 possibilities to consider:

1. The control system contains no classified information and no cryptography is required. In that case, there are no UFGS requirements.

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.

In generally, the need for cryptography 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.)

If cryptography is required, select whether to require it everywhere, only on the IP network, or only at specific locations within the system.

****

{For Reference Only: This subpart (and its subparts) relates to SC-13; CCIs: CCI-002449, CCI-002450}

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.

]3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

{For Reference Only: This subpart (and its subparts) relates to SI-3(c); CCI-001241, CCI-002623}

For all computers installed under this project, install and configure malware protection software in accordance with the relevant STIGs.

[3.11.2 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 Reference Only: This subpart relates to SI-4 (a),(b); CCI-001253, CCI-002645}

[_____]

]3.12 FIELD QUALITY CONTROL

3.12.1 Tests

****
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.

-- End of Section --