Solicitation No. W912PP23R0009

Date: December 2022

U.S. ARMY CORPS OF ENGINEERS

Combat Rescue Helicopter (CRH) Simulator Facility ADAL

Solicitation No. W912PP23R0009

Kirtland AFB

New Mexico

Ready to Advertise

Volume 4—Specifications
Division 25

PROJECT TABLE OF CONTENTS

-- End of Project Table of Contents --

SECTION 25 05 11.21

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
FIRE AND LIFE SAFETY

PART 1 GENERAL

This section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

1.1 CONTROL SYSTEM APPLICABILITY

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: Fire and Life Safety.

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

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.

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

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

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. Submittals with an "S" are for inclusion in the Sustainability eNotebook, in conformance with Section 01 33 29 SUSTAINABILITY REPORTING. 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

Qualifications; 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 Cybersecurity Representative

Provide a Cybersecurity Representative as the key person to implement and manage the cybersecurity related control systems of the project. This individual must have a minimum of two years of cybersecurity control systems experience, including two projects of similar size and complexity. Submit the Cybersecurity Representative's certification of qualifications no later than 60 calendar days after Notice to Proceed. Submit one hard copy and an electronic copy.

1.7.1.1 Duties

The Cybersecurity Representative must lead and oversee the cybersecurity control systems work specified herein and be the primary point of contact for the Government regarding the cybersecurity work.

1.7.1.2 Qualifications

The individual must have a minimum of 2 years with Risk Management Framework implementation experience and experience with Facility Related Control System cybersecurity implementation such as a control system related training or certification.

1.7.2 Cybersecurity Kickoff Meeting

Within 60 calendar days after contract award, the Cybersecurity Representative must schedule a Cybersecurity Kickoff Meeting with the Contracting Officer, system owner, system program manager, and Information System Security Manager (ISSM). The meeting will be located at a specific time and place to be determined by the Contracting Officer.

1.8 CYBERSECURITY DOCUMENTATION

1.8.1 Cybersecurity Interconnection Schedule

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 https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphics-tables).

1.8.2 Network Communication Report

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.

1.8.3 Control System Inventory Report

Provide a Control System Inventory report using the Inventory Spreadsheet listed under this Section at https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphics-tables documenting all 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.

1.8.4 Software Recovery and Reconstitution Images

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.

1.8.5 Cybersecurity Riser Diagram

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 overlayed on a facility schematic.

1.8.6 Control System Cybersecurity Documentation

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

1.8.6.1 Software Applications

For all software applications running on computers provide:

a. Administrator documentation that describes secure configuration of the software.

b. Administrator documentation that describes secure installation of the software.

c. Administrator documentation that describes secure operation of the software.

d. Administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software.

e. Administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software.

f. User documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms.

g. User documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner.

h. User documentation that describes user responsibilities in maintaining the security of the software.

1.8.6.2 Default Requirements for Control System Devices

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.

b. Documentation that describes secure installation of the device.

c. Documentation that describes secure operation of the device.

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device.

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device.

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms.

g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner.

h. Documentation that describes user responsibilities in maintaining the security of the device.

1.9 SOFTWARE UPDATE LICENSING

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.

1.10 CYBERSECURITY DURING CONSTRUCTION

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

1.10.1 Contractor Computer Equipment

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

1.10.1.1 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.

1.10.1.2 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.

1.10.1.3 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.

1.10.1.4 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-graphics-tables. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.10.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks must meet the following requirements:

1.10.2.1 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.

1.10.3 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

1.10.4 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.

1.10.5 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.

1.10.6 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-graphics-tables. 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.

1.11 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

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.

Implement a warning banner on terminal interfaces that conforms to DoD warning banner guidelines. Configure each component of the product to operate using the principle of least privilege. This includes operating communications, and energy delivery system services.

Provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. Provide a system administration mechanism for changing user(s') role (e.g., group) associations.

Configure the product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side. Provide a method for protecting against unauthorized privilege escalation.

Document options for defining access and security permissions, user accounts, and applications with associated roles. Configure these options as specified.

Prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware and document if not feasible, provide mitigation recommendations.

Verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

3.1.1.1 Computers

All computers must FULLY support user accounts.

3.1.1.2 Default Requirements for Control System Devices

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

a. Devices with web interfaces must either FULLY support user accounts or have their web interface disabled.

b. Field devices with full local user interfaces allowing modification of data must FULLY support user accounts.

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

3.1.2 Account Management

Document all accounts (including but not limited to, generic or default)

that need to be active for proper operation of the product. Change default account settings to specific settings (e.g., length, complexity, history, and configurations) provided by government representative. Changed account information will not be published. All new account information will be provided by a protected mechanism. Remove or disable any accounts that are not needed for normal or maintenance operations of the control system. Accounts for emergency operations shall be placed in a highly secure configuration and documentation must be provided.

3.1.3 Unsuccessful Logon Attempts

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts.

3.1.3.1 Devices MINIMALLY Supporting Accounts

Devices which MINIMALLY support accounts must lock the user input after three unsuccessful logon attempts and must support unlocking of the user input when unlocked by an administrator.

3.1.3.2 Devices FULLY Supporting Accounts

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.

3.1.3.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

Contact local ISSM and System Owner/Program Manager for requirements for high availability interfaces that are exempt from unsuccessful logon attempts. Work with local ISSM and local CIO to complete the following:

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

3.1.4 System Use Notification

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.

3.1.4.1 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

3.1.5 Permitted Actions Without Identification or Authentication

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.

3.1.6 Wireless Access

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).

3.1.6.1 Wireless IP Communications

Do 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.

3.1.6.2 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.

3.1.6.3 Wireless Communication Request

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-graphics-tables.

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.

3.1.6.4 Wireless Communication Testing

As part of Performance Verification Testing (PVT), 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. 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

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

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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

f. Successful and unsuccessful accesses to objects

g. All program initiations

h. All direct access to the information system

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

j. 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 Default Requirements for Control System Devices

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

3.2.1.2.1 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

3.2.1.2.1.1 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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

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

g. All kernel module load, unload, and restart

3.2.1.2.1.2 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

3.2.1.2.2 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

a. For devices that have STIG/SRGs related to audit storage capacity 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 audit records in conformance with applicable STIG/SRGs.

3.2.2.1 Device Audit Record Upload Software

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 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.

Contact local ISSM and System Owner/Program Manager for device audit record upload software requirements. 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

Front end computers associated with auditing must, in the case of a

failure in the auditing system, notify ISSM 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

3.2.4.1 Computers

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 Control System Devices

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.

3.2.4.3 Default Requirements for Control System Devices

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

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.

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

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

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 Default Requirements for Control System Devices

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.

3.5.2 Authenticator Management

3.5.2.1 Authentication Type

3.5.2.1.1 Default Requirements for Control System Devices

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.

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

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

Devices minimally supporting accounts must support passwords with a minimum length of four characters.

3.5.2.2.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with ISSM. 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 hard copies 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

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, comply with the requirements of those STIGS/SRGs.

3.5.4 Device Identification and Authentication

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 ISSM.

3.5.4.1 Default Requirements for Control System Devices

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 ISSM.

3.5.5 Cryptographic Module Authentication

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

3.6 EMERGENCY POWER

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

3.7 DURABILITY TO VULNERABILITY SCANNING

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 Assured Compliance Assessment Solution (ACAS) by responding with a valid credentialed scan. For control system devices other than computers:

3.7.1 Default Requirements for Control System Devices

Non-computer control system devices where Durability to Vulnerability Scanning requirements are not otherwise indicated in this Section are not required to respond to scans.

3.8 FIPS 201-2 REQUIREMENT

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list.

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-graphics-tables to request approval for each device.

3.10 SYSTEM AND COMMUNICATION PROTECTION

3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection

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

3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

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

3.12 FIELD QUALITY CONTROL

3.12.1 Tests

In addition to testing and testing support required by other Sections, provide a minimum of 80 hours of technical support for cybersecurity testing of control systems.

-- End of Section --

THIS PAGE INTENTIONALLY LEFT BLANK

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002110	AC-2 (a)	The organization defines the information system account types that support the organizational missions/business functions.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions.	N/A
CCI-000015	AC-2(1)	The organization employs automated mechanisms to support the information system account management functions	The organization being inspected/assessed configures the information system to employ automated mechanisms to support the information system account management functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	N/A
CCI-001682	AC-2(2)	The information system automatically removes or disables emergency accounts after an organization-defined time period for each type of account	The organization being inspected/assessed configures the information system to never automatically remove or disable emergency accounts. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-000016	AC-2(2)	The information system automatically removes or disables temporary accounts after an organization-defined time period for each type of account	The organization being inspected/assessed configures the information system to automatically remove or disable temporary accounts after 72 hours. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001361	AC-2(2)	The organization defines a time period after which temporary accounts are automatically terminated	DoD has defined the time period as 72 hours. The time period of 72 hours applies to temporary user accounts.	Impractical
CCI-001365	AC-2(2)	The organization defines a time period after which emergency accounts are automatically terminated.	DoD has defined the time period as never. The time period of never applies to emergency admin accounts.	Impractical
CCI-000017	AC-2(3)	The information system automatically disables inactive accounts after an organization-defined time period.	The organization being inspected/assessed configures the information system to disable inactive accounts after 30 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-000217	AC-2(3)	The organization defines a time period after which inactive accounts are automatically disabled.	DoD has defined the time period as 30 days.	Impractical
CCI-000018	AC-2(4)	The information system automatically audits account creation actions.	The organization being inspected/assessed configures the information system to automatically audit account creation actions. For information system components that have applicable STIGs or SRGs, the	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001403	AC-2(4)	The information system automatically audits account modification actions.	The organization being inspected/assessed configures the information system to automatically audit account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-001404	AC-2(4)	The information system automatically audits account disabling actions.	The organization being inspected/assessed configures the information system to automatically audit account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-001405	AC-2(4)	The information system automatically audits account removal actions.	The organization being inspected/assessed configures the information system to automatically audit account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-002130	AC-2(4)	The information system automatically audits account enabling actions.	The organization being inspected/assessed configures the information system to automatically audit account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-001683	AC-2(4)	The information system notifies organization-defined personnel or roles for account creation actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account creation actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001684	AC-2(4)	The information system notifies organization-defined personnel or roles for account modification actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account modification actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-001685	AC-2(4)	The information system notifies organization-defined personnel or roles for account disabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account disabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-001686	AC-2(4)	The information system notifies organization-defined personnel or roles for account removal actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account removal actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-002132	AC-2(4)	The information system notifies organization-defined personnel or roles for account enabling actions.	The organization being inspected/assessed configures the information system to notify the system administrator and ISSO for account enabling actions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-000213	AC-3	The information system enforces approved authorizations for logical access to	Any device supporting accounts (either fully or partially) must limit access to the device according to specified limitations for each account. Install and configure any device having a Security Technical Implementation	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information and system resources in accordance with applicable access control policies.	Guide (STIG) or Security Requirements Guide (SRG) in accordance with that STIG or SRG.	
CCI-001368	AC-4	The information system enforces approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	The organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information within the system based on information flow control policies. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE Vendor to provide data flow diagram.
CCI-001414	AC-4	The information system enforces approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies	The organization being inspected/assessed configures the information system to enforce approved authorizations for controlling the flow of information between interconnected systems based on information flow control policies. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE Vendor to provide interconnection information.
CCI-001548	AC-4	The organization defines the information flow control policies for	The organization being inspected/assessed defines and documents the information flow control policies for controlling the flow of information within the system. DoD has	APPLICABLE Vendor to provide data flow diagram.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		controlling the flow of information within the system.	determined the information flow control policies are not appropriate to define at the Enterprise level.	
CCI-001549	AC-4	The organization defines the information flow control policies for controlling the flow of information between interconnected systems	The organization being inspected/assessed defines and documents the information flow control policies for controlling the flow of information between interconnected systems. DoD has determined the information flow control policies are not appropriate to define at the Enterprise level.	N/A
CCI-001550	AC-4	The organization defines approved authorizations for controlling the flow of information within the system	The organization being inspected/assessed defines and documents approved authorizations for controlling the flow of information within the system.	APPLICABLE Contractor to provide information
CCI-001551	AC-4	The organization defines approved authorizations for controlling the flow of information between interconnected systems.	The organization being inspected/assessed defines and documents approved authorizations for controlling the flow of information between interconnected systems.	APPLICABLE Vendor to provide interconnection information
CCI-002220	AC-5(c)	The organization defines information system access authorizations to	The organization being inspected/assessed defines and documents the information system access authorizations to support separation of duties.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		support separation of duties.		
CCI-000225	AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	The organization being inspected/assessed documents and implements the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	N/A
CCI-001558	AC-6(1)	The organization defines the security functions (deployed in hardware, software, and firmware) for which access must be explicitly authorized	DoD has defined the security functions as all functions not publicly accessible.	N/A
CCI-002221	AC-6(1)	The organization defines the security-relevant information for which access must be explicitly authorized.	DoD has defined the security-relevant information as all security-relevant information not publicly available.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002222	AC-6(1)	The organization explicitly authorizes access to organization-defined security functions	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all functions not publicly accessible. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security functions as all functions not publicly accessible.	N/A
CCI-002223	AC-6(1)	The organization explicitly authorizes access to organization-defined security-relevant information	The organization being inspected/assessed documents and implements a process to explicitly authorize access to all security-relevant information not publicly available. Explicit authorization can be in the form of an acceptable use policy signed by the user at the time of access being granted. DoD has defined the security-relevant information as all security-relevant information not publicly available.	N/A
CCI-000039	AC-6(2)	The organization requires that users of information system accounts or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing non-security functions.	The organization being inspected/assessed documents and implements a process to require that users of information system accounts or roles, with access to any privileged security functions or security-relevant information, use non-privileged accounts, or roles, when accessing non security functions. DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001419	AC-6(2)	The organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access	DoD has defined the security functions and security-relevant information as any privileged security functions or security-relevant information.	N/A
CCI-002234	AC-6(9)	The information system audits the execution of privileged functions.	The organization being inspected/assessed configures the information system to audit the execution of privileged functions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-000043	AC-7(A)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	APPLICABLE if system has capability
CCI-000043	AC-7(a)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-	DOD policy requires the system to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval. Control System field devices to implement these requirements to the greatest extent possible.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined time period.	Document any device incapable of meeting the defined requirement and state actual implementation.	
CCI-000044	AC-7(a)	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.	The information system shall be set to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval. Devices which Partially support accounts shall implement the requirements of a FULLY supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel. Document any device incapable of meeting the defined requirement and state actual implementation.	APPLICABLE if system has capability.
CCI-001423	AC-7(a)	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occurs.	DOD policy requires the system to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval.	APPLICABLE if system has capability.
CCI-002236	AC-7(a)	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires for systems that once an account is locked, the account must stay locked until unlocked by an administrator. This may have safety implications in control system environment. Implement with caution.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002237	AC-7(a)	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires that once the indicated number of unsuccessful login attempts occurs, delay login prompts by **[5] seconds**. If the provided software cannot meet these requirements, document software capabilities to protest from subsequent unsuccessful login attempts and propose alternate protections. Do not implement alternate protection measures without explicit permission from the System Owner.	APPLICABLE if system has capability.
CCI-002238	AC-7(a)	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The information system shall be configured to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Devices which Partially support accounts shall implement the requirements of a Fully supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel.	APPLICABLE if system has capability.
CCI-000048	AC-8(a)	The information system displays an organization-defined system	All devices (PC's, BPOCs, Network switches, etc…) with a user interface supporting the use of a password or PIN, and capable of displaying 50 or more alphanumeric	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	characters shall be configured to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. The DOD Consent Banner can be found on the RMF Knowledge Service site at https://rmfks.osd.mil/rmf/Guidance/GoverningPolicy/Pages/ConsentBanner.aspx Devices connected to a network, with a user interface supporting use of a password or PIN, and **not capable** of displaying 50 or more alphanumeric characters must have a permanently affixed label displaying an approved banner from the policy listed above.	
CCI-002247	AC-8(a)	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-002243	AC-8(a)(1)	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information system.		
CCI-002244	AC-8(a)(2)	The organization-defined information system use notification message or banner is to state that information system usage may be monitored, recorded, and subject to audit.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002245	AC-8(a)(3)	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002246	AC-8(a)(4)	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		monitoring and recording.		
CCI-000050	AC-8(a)(4)	The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.	Configure the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if system has capability.
CCI-002248	AC-8(C)(1)	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-000058	AC-11(a)	The information system provides the capability for users to directly initiate session lock mechanisms.	The organization being inspected/assessed configures the information system to provide the capability for users to directly initiate session lock mechanisms. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if system has capability.
CCI-000059	AC-11(a)	The organization defines the time period of inactivity after which the information system initiates a session lock.	DoD has defined the time period as 15 minutes. This should only be implemented if required by System Owner due to potential safety concerns.	Impractical unless required by System Owner

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000056	AC-11(b)	The information system retains the session lock until the user reestablishes access using established identification and authentication procedures	The organization being inspected/assessed configures the information system to retain the session lock until the user reestablishes access using established identification and authentication procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	Impractical unless required by System Owner
CCI-000060	AC-11(1)	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	The organization being inspected/assessed configures the information system to conceal, via the session lock, information previously visible on the display with a publicly viewable image. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	Impractical unless required by System Owner
CCI-002360	AC-12	The organization defines the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session.	The organization being inspected/assessed defines and documents the conditions or trigger events requiring session disconnect to be employed by the information system when automatically terminating a user session. DoD has determined the conditions or trigger events are not appropriate to define at the Enterprise level. The organization being inspected/assessed must comply with the STIG/SRG guidance. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by System Owner

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002361	AC-12	The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.	The organization being inspected/assessed configures the information system to automatically terminate a user session after conditions or trigger events requiring session disconnect. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by System Owner
CCI-000061	AC-14(a)	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following: • Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by the System Owner.
CCI-000232	AC-14(b)	The organization documents and provides supporting rationale in the security plan for the information system, user	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following:	Impractical unless required by the System Owner.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		actions not requiring identification and authentication	• Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	
CCI-001438	AC-18(a)	The organization establishes usage restrictions for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001439	AC-18(a)	The organization establishes implementation guidance for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-002323	AC-18(a)	The organization establishes configuration/connection requirements for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001441	AC-18(b)	The organization authorizes wireless access to the information system prior to allowing such connections.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001443	AC-18(1)	The information system protects wireless access to the system using authentication of	The organization being inspected/assessed configures the information system to protect wireless access to the system using authentication of users and/or devices. For information system components that have	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		users and/or devices.	applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Required if system relies on RF connectivity.	
CCI-001444	AC-18(1)	The information system protects wireless access to the system using encryption.	The organization being inspected/assessed configures the information system to protect wireless access to the system using encryption. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. This control is required for systems which use RF for connectivity.	APPLICABLE
CCI-000123	AU-2(a)	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	HW (workstations, servers, network switches/infrastructure, etc…) capable of auditing shall audit the following: • Successful and unsuccessful logon attempts • Privileged activities or other system level access • Starting and ending time for user access to the system • Concurrent logons from different workstations. • Successful and unsuccessful accesses to objects • All program initiators • All direct access to the information system • All account creations, modifications, disabling, and terminations • All kernel module load, unload, and restart	APPLICABLE if capability exists
CCI-001571	AU-2(a)	The organization defines the information	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security	APPLICABLE only if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system auditable events.	levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	
CCI-000125	AU-2(c)	The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	The organization documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	N/A
CCI-001485	AU-2(d)	The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	N/A
CCI-000130	AU-3	The information system generates audit records containing information that	The information system shall be configured to generate audit records containing information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		establishes what type of event occurred.	being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (FPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	
CCI-000131	AU-3	The information system generates audit records containing information that establishes when an event occurred.	The information system shall be configured to generate audit records containing information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000132	AU-3	The information system generates audit records containing information that establishes where the event occurred.	The information system shall be configured to generate audit records containing information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000133	AU-3	The information system generates audit records containing information that establishes the source of the event.	The information system shall be configured to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	
CCI-000134	AU-3	The information system generates audit records containing information that establishes the outcome of the event.	The information system shall be configured to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-001487	AU-3	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The information system shall be configured to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance that pertains to CCI 1487. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000135	AU-3(1)	The information system generates audit records containing the organization-defined additional, more detailed	The organization being inspected/assessed configures the information system to generate audit records containing the organization defined additional, more detailed information as defined in AU-3 (1), CCI 1488 that is to be included in the audit records.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information that is to be included in the audit records.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001488	AU-3(1)	The organization defines additional, more detailed information to be included in the audit records.	The organization being inspected/assessed defines and documents additional, more detailed information to be included in the audit records. The additional information must include at a minimum, full-text recording of privileged commands or the individual identities of group account users. The additional information must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation. DoD has determined that additional, more detailed information must include, at a minimum, full-text recording of privileged commands or the individual identities of group account users. DoD has determined that all additional, more detailed information is not appropriate to define at the Enterprise level.	N/A
CCI-001848	AU-4	The organization defines the audit record storage requirements	Devices that have STIG/SRGs must comply with the requirements of those STIG/SRGs. For BPOCs and field devices (not front end computers) capable of generating audit records, the front end server shall be configured to retrieve audit records from the devices. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-001849	AU-4	The organization allocates audit record storage capacity in accordance with organization-	The organization allocates and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 001848. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined audit record storage requirements.	guidance. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	If the front end server can be configured to automatically archive full logs or write audit logs to an audit server (from all connected audit capable devices), then this control shall be considered not-applicable (NA). Otherwise, if email services are available, configure the workstations and servers to alert at a minimum, the system administrator (SA) and or the designated Information System Security Officer/Manager in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. If email services are not available then the workstations and servers shall configure the system to provide an alert on the screen in the event of an audit processing failure.	APPLICABLE if capability exists
CCI-000140	AU-5(b)	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	In case of an audit failure, if possible, configure the system to continue to collect audit records by overwriting existing audit records starting with the oldest records first. Ideal configuration would be to configure the system to send audit records directly to an audit server, or automatically archive full logs and document as such with the ISSO. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	APPLICABLE if capability exists
CCI-001490	AU-5(b)	The organization defines actions to be taken by the information system upon audit	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure as described in CCI-000139 and CCI-000140.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).		
CCI-001875	AU-7(a)	The information system provides an audit reduction capability that supports on-demand audit review and analysis.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001876	AU-7(a)	The information system provides an audit reduction capability that supports on-demand reporting requirements.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001877	AU-7(a)	The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.	The organization being inspected/assessed must employ information systems that provide an audit reduction capability that support after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1877.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001878	AU-7(a)	The information system provides a report generation capability that supports on-demand audit review and analysis.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support on-demand audit review and analysis (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001879	AU-7(a)	The information system provides a report generation capability that supports on-demand reporting requirements.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support on-demand reporting requirements (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001880	AU-7(a)	The information system provides a report generation capability that supports after-the-fact investigations of security incidents.	The organization being inspected/assessed must employ information systems that provide a report generation capability that support after-the-fact investigations of security incidents (either natively or through the use of third-party tools). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001881	AU-7(b)	The information system provides an audit reduction capability that does not alter original content or	The organization being inspected/assessed must ensure that the audit reduction capability does not alter the original audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		time ordering of audit records.	comply with the STIG/SRG guidance that pertains to CCI 1881.	
CCI-001882	AU-7(b)	The information system provides a report generation capability that does not alter original content or time ordering of audit records.	The organization being inspected/assessed must ensure that the report generation capability does not alter the original audit records. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-00158	AU-7(1)	The information system provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records.	The organization being inspected/assessed must employ information systems that provide the capability to process audit records for events of interest based on audit fields within audit records defined in AU-7 (1), CCI 1883. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000159	AU-8(a)	The information system uses internal system clocks to generate time stamps for audit records.	Workstations and servers on the domain shall be configured to synchronize with domain controllers. If an NTP server is configured it should synchronize with a secure, authorized source. If not on a domain or NTP server, workstations, server or other components that generate audit records, the timing requirement inherent in the control system will be sufficient. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001889	AU-8(b)	The information system records time stamps for	DoD has defined the granularity of time measurement as one second. For information system components that have applicable	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		audit records that meets organization-defined granularity of time measurement.	STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001890	AU-8(b)	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	All devices which provide audit capabilities, configure them to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001891	AU-8(1)	The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.	The organization being inspected/assessed configures the information system to synchronize internal information system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS) when the time difference is greater than the difference defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1891. DoD has defined the frequency as every 24 hours for networked systems. DoD has defined the authoritative time source as an authoritative time server which is	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).	
CCI-001892	AU-8(1)	The organization defines the time difference which, when exceeded, will require the information system to synchronize the internal information system clocks to the organization-defined authoritative time source.	The organization being inspected/assessed defines and documents the time difference, which, when exceeded, will require the information system to synchronize the internal information system clocks. DoD has determined the time difference is not appropriate to define at the Enterprise level.	APPLICABLE if capability exists
CCI-002046	AU-8(1)	The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.	The organization being inspected/assessed configures the information system to synchronize the internal system clocks to the authoritative time source when the time difference is greater than the time period defined in AU-8 (1), CCI 1892. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2046.	APPLICABLE if capability exists
CCI-000169	AU-12(a)	The information system provides audit record generation capability for the	CCI-000123 defines auditable events for an information system. Level 4 devices (workstations, servers, network switches, routers, etc.) shall implement to the extent possible the requirements in CCI-000123 and	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		auditable events defined in AU-2(a) at organization defined information system components.	AU-2(a). Requirements that cannot be implemented must be documented and justification provided. Other devices (non level 4) that provide auditing capabilities shall implement the requirements in CCI-000123 where the capability exists and the ISSM deems relevant. Example, for components. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	
CCI-001459	AU-12(a)	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components. Devices which ARE NOT capable of generating an audit log are exempt. System documentation should define which components are capable and are not capable of generating audit logs.	APPLICABLE if capability exists
CCI-000171	AU-12(b)	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system	Configure all capable devices to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM. System administrator personnel will inherently have the rights associated with their accounts to select auditable events, however, organizational policy shall only authorize the ISSM or individuals appointed by the ISSM to select and make those necessary changes.	N/A
CCI-001910	AU-12(b)	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		components of the information system.		
CCI-000172	AU-12(c)	The information system generates audit records for the events defined in AU-2(d) with the content defined in AU-3.	Audit record requirements are defined in CCI-000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487 above. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	APPLICABLE if capability exists
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.	Interconnections to other systems WILL NOT be implemented. Front end servers and workstations may reside on the local Network Enterprise Center's (NECs) network allowing a connection into the control system (CS) components.	N/A No Interconnects
CCI-002102	CA-9(a)	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	Define and document the information system components or classes of components that that are authorized internal connections to the information system. (e.g. Network Controllers, switches, routers, etc…)	APPLICABLE
CCI-002103	CA-9(b)	The organization documents, for each internal connection, the interface characteristics.	The organization documents, for each internal connection (network controllers, etc…) the communication protocols used and a general description of what information is communicated over the network. This can be accomplished through a network communication report.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002104	CA-9(b)	The organization documents, for each internal connection, the security requirements.	The organization documents, for each internal connection, the security requirements.	N/A
CCI-002105	CA-9(b)	The organization documents, for each internal connection, the nature of the information communicated.	See CCI-002103	APPLICABLE
CCI-000293	CM-2	The organization develops and documents a current baseline configuration of the information system.	Develop and document a current baseline configuration of the information system to include, drawings, software licenses, source code, hardware, etc…	APPLICABLE
CCI-000298	CM-2(1)(c)	The organization reviews and updates the baseline configuration of the information system as an integral part of information system component installations.	The organization being inspected/assessed reviews and updates the baseline configuration of the information system as an integral part of information system component installations. The organization must document each occurrence of the reviews and update actions as an audit trail.	N/A
CCI-001737	CM-2(7)a	The organization defines the information systems, system components, or devices that are to	The organization being inspected/assessed defines and documents, in the configuration management policy, the information systems, system components, or devices that are to have configurations defined in CM-2 (7), CCI 1738 applied when located in areas of	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		have organization-defined configurations applied when located in areas of significant risk	significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	
CCI-001738	CM-2(7)a	The organization defines the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk.	The organization being inspected/assessed defines and documents, in the configuration management policy, the security configurations to be implemented on information systems, system components, or devices when they are located in areas of significant risk. DoD has determined that this value is not appropriate to define at the Enterprise level.	N/A
CCI-000363	CM-6(a)	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). Document in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components. Field Devices (BPOCs, etc…) that do not have STIGs, SRGs, etc…obtain vendor configuration guides.	N/A
CCI-000364	CM-6(a)	The organization establishes configuration settings for information technology products employed within	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		the information system using organization-defined security configuration checklists.	(e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	
CCI-000365	CM-6(a)	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001588	CM-6(a)	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001755	CM-6(c)	The organization defines the information	DoD has defined the information system components as all configurable information system components.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system components for which any deviation from the established configuration settings are to be identified, documented and approved.		
CCI-000381	CM-7(a)	The organization configures the information system to provide only essential capabilities.	Disable all ports, protocols and services not specifically needed by any device or component within the Control system (server, workstations, field devices, BPOCS, switches, etc…) Remove all software not specifically needed for use in the control system.	APPLICABLE
CCI-000380	CM-7(b)	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.		APPLICABLE
CCI-000382	CM-7(b)	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.		APPLICABLE
CCI-001761	CM-7(1)(b)	The organization defines the functions, ports, protocols and services within the information	Define and document in the system security plan, the functions, ports, protocols and services within the control system that are to be disabled when deemed unnecessary.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system that are to be disabled when deemed unnecessary and/or non-secure.		
CCI-001762	CM-7(1)(b)	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	Disable functions, ports, protocols, and services within the control system deemed to be unnecessary and/or nonsecure, nonsecure functions, ports, protocols, and services.	APPLICABLE
CCI-001592	CM-7(2)	The organization defines the rules authorizing the terms and conditions of software program usage on the information system.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551.01. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	N/A
CCI-001763	CM-7(2)	The organization defines the policies regarding software program usage and restrictions.	The organization being inspected/assessed defines and documents their rules for approval of software program usage. For network capable software programs, the organization being inspected/assessed complies with DoDI 8551.01. DoD has determined that the rules authorizing the terms and conditions of software program usage on the information system are not appropriate to define at the Enterprise level.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001764	CM-7(2)	The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage	The organization being inspected/assessed configures the information system to prevent the execution of programs not authorized in accordance with CM-7 (2) CCIs 1592 and 1763.	APPLICABLE if capability exists
CCI-001772	CM-7(5)a	The organization defines the software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system. DoD has determined that a comprehensive list of unauthorized software programs is not appropriate to define at the Enterprise level.	APPLICABLE
CCI-001773	CM-7(5)a	The organization identifies the organization-defined software programs authorized to execute on the information system.	The organization being inspected/assessed must define and document software programs that are authorized to execute on the information system.	APPLICABLE
CCI-001774	CM-7(5)b	The organization employs a deny-all, permit-by-	The organization being inspected/assessed configures the information system to deny-all and only permit by exception the execution of	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		exception policy to allow the execution of authorized software programs on the information system.	authorized software programs on the information system.	
CCI-000389	CM-8(a)(1)	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	Provide a Control System inventory report covering all networked, including network infrastructure devices. Provide the following information (where applicable): • If the device has (in other project documentation) a unique identifier • Description, make, mode, serial number, location • Software/firmware version Network information: protocol, network address	APPLICABLE
CCI-000392	CM-8(a)(2)	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.	See CCI-000389	APPLICABLE
CCI-000398	CM-8(a)(4)	The organization defines information deemed necessary to achieve	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		effective information system component accountability.	networked component/device, the machine name.	
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization must develop a contingency plan (CP) addressing recovery and reconstitution of the control system to a known state after a disruption In essence, restoring the system to the appropriate operational state. The CP will be site specific and should be developed in conjunction with stakeholders of the system. Copies of required software, backup data, hardware list and baseline configurations should be identified in the CP. NOTE-known state shall also include the accepted “as-built” documentation and include any custom programming and configuration for controllers or workstations.	APPLICABLE
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan. See also CCI-000550	APPLICABLE
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization must identify the selected method in the contingency plan. See also CCI-000550	APPLICABLE
CCI-002855	CP-12	The information system, when organization-defined conditions	Configure the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 002857 when conditions defined in CP-12, CCI	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	
CCI-002856	CP-12	The organization defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	When the following conditions are detected, the control system shall enter a safe mode of operation. • Commercial Power Loss • Fire • Water	APPLICABLE
CCI-002857	CP-12	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	**Commercial Power Failure:** Upon loss of commercial power, the control system will switch to Generator power and only Mission Critical Infrastructure (deemed by the organization) will received continued control system service. All other infrastructure/areas services will cease until commercial power is restored. **Fire:** The system shall be integrated with fire detectors. Upon detection of fire, the system will ensure dampers and air handlers are shut down to prevent the propagation of smoke, gasses and fire through the system. The system shall remain in a shutdown/closed state until manually restarted/rebooted by organization personnel.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			Water: Upon detection of water (sprinkler system), the servers shall perform a graceful shutdown in order to minimize component failure due to water.	
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	All components capable of user accounts will be configured to uniquely identify and authenticate users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.	Multifactor authentication shall be implemented for users that require privileged level accounts to servers and workstations residing on the network (not standalone or PRIVATE VLAN segregated systems). Multifactor authentication can be implemented with through common access card (CAC) authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		Verification (PIV) credentials.	STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-000777	IA-3	The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system.	All network connected endpoint devices (including but not limited to: workstations, printers, servers) shall be identified and authenticated before establishing a connection to the information system. Any device incapable of being authenticated to the system shall be documented.	APPLICABLE if capability exists
CCI-000778	IA-3	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to identify all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001958	IA-3	The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to authenticate all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001959	IA-3(1)	The organization defines the specific devices and/or type of devices the information system is to authenticate before establishing a connection.	DoD has defined the value as all network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	APPLICABLE if capability exists
CCI-001967	IA-3(1)	The information system authenticates organization-defined devices and/or types of devices before establishing a local, remote and/or network connection using bidirectional authentication that is cryptographically based.	The organization being inspected/assessed configures the information system to use cryptographically based bidirectional authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000176	IA-5(b)	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001544	IA-5(c)	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	APPLICABLE if capability exists
CCI-001989	IA-5(e)	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	Document and implement procedures to change default authenticators (passwords, etc.) or apply authenticators to all capable components prior to system installation.	N/A
CCI-000182	IA-5(g)	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	Document and implement procedures for changing/refreshing authenticators in the following time periods: • Password: 60 days.	N/A
CCI-001610	IA-5(g)	The organization defines the time period (by authenticator	DoD has defined the time period of Password: 60 days. Biometrics: every 3 years.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		type) for changing/refreshing authenticators.		
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	APPLICABLE if capability exists
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	APPLICABLE if capability exists
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	APPLICABLE if capability exists
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	
CCI-001611	IA-5(1)(a)	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	APPLICABLE if capability exists
CCI-001612	IA-5(1)(a)	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	APPLICABLE if capability exists
CCI-001613	IA-5(1)(a)	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	APPLICABLE if capability exists
CCI-001614	IA-5(1)(a)	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	APPLICABLE if capability exists
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		minimum number of special characters used.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	
CCI-000195	IA-5(1)(b)	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195.	APPLICABLE if capability exists
CCI-001615	IA-5(1)(b)	The organization defines the minimum number of characters that are changed when new passwords are created.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	APPLICABLE if capability exists
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-protected passwords.	Configure the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	APPLICABLE if capability exists
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-	Configure the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		protected passwords.	the STIG/SRG guidance that pertains to CCI 197.	
CCI-000198	IA-5(1)(d)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	APPLICABLE if capability exists
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.	Configure the information system to enforce maximum password lifetime restrictions. For capable components, set maximum password age to 60 days or less (excluding “0”). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	APPLICABLE if capability exists
CCI-001616	IA-5(1)(d)	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	APPLICABLE if capability exists
CCI-001617	IA-5(1)(d)	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days and not being “0”.	APPLICABLE if capability exists
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. All other components utilizing passwords, the password reuse should be set to 24. If the components are incapable of being set to 24 then implement the maximum possible.	APPLICABLE if capability exists
CCI-001618	IA-5(1)(e)	The organization defines the number of	Per the STIGs for Windows based systems, the DOD has defined this to be set at a minimum of 24.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		generations for which password reuse is prohibited.		
CCI-002041	IA-5(1)(f)	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	APPLICABLE if capability exists
CCI-000185	IA-5(2)(a)	The information system, for PKI-based authentication validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.	The information system performing hardware token-based authentication must be configured to validate DoD-approved PKI credentials in accordance with RFC 5280. The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 185.	APPLICABLE if capability exists
CCI-000186	IA-5(2)(b)	The information system, for PKI-based authentication enforces authorized access to the corresponding private key.	Information systems must not have access to users' private keys. The cryptographic container in which the private keys are stored (e.g. smart card or software module) implements access controls and protections to ensure that only the authorized user can activate the private key. DoD users agree to protect their PKI credentials in accordance with the DD-2842 agreement that is executed	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			for each credential. They are reminded of these responsibilities in annual IA training. The private key identifying the information system must be stored in a cryptographic container that is FIPS 140-2 validated. Only authorized information system operators should have access to activation data (e.g. password or PIN) for the private key.	
CCI-000187	IA-5(2)(c)	The information system, for PKI-based authentication, maps the authenticated identity to the account of the individual or group.	The information system performing PKI-based authentication must be configured to map the authenticated PKI credential to a corresponding network or information system account or role in accordance with DoDI 8520.03. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 187.	APPLICABLE if capability exists
CCI-001991	IA-5(2)(D)	The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	The information system must be configured to locally cache revocation data to support path discovery and validation in case of inability to access revocation information via the network. The information system may meet this requirement by locally caching certificate revocation lists (CRLs), Online Certificate Status Protocol (OCSP) responses, or a combination thereof. Cached revocation data must include revocation information from all PKIs serving known or anticipated users of the information system. Cached data must be refreshed with a frequency shorter than the life of the data (e.g. if a CRL is valid for 7 days, a new CRL must be retrieved and cached more frequently than every 7 days) to ensure that cached data is valid and not expired. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			the STIG/SRG guidance that pertains to CCI 1991.	
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.	APPLICABLE if capability exists
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000206	IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Configure the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206. Applicable to networked devices. Does not apply to devices that have NO feedback during password/PIN entry. Devices shall 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 CCI-000206, comply with the requirements of those STIGS/SRGs.	APPLICABLE if capability exists
CCI-000803	IA-7	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	For devices that have STIG/SRGs related to CCI-000803, comply with the requirements of those STIG/SRGs.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000865	MA-3	The organization approves information system maintenance tools.	The organization being inspected/assessed documents the approved maintenance tools within the Security Plan.	N/A
CCI-000936	PE-4	The organization controls physical access to organization-defined information system distribution and transmission lines within organizational facilities using organization-defined security safeguards.	The organization being inspected/assessed controls physical access to information system distribution and transmission lines defined in PE-4, CCI 2930 within organizational facilities using security safeguards defined in PE-4, CCI 2931.	APPLICABLE
CCI-002930	PE-4	The organization defines information system distribution and transmission lines within organizational facilities to control physical access using organization-defined security safeguards.	The organization being inspected/assessed defines and documents information system distribution and transmission lines within organizational facilities to control physical access using organization-defined security safeguards. If transmission lines carry classified information, a protected distribution system (PDS) must be used to transmit unencrypted classified information through an area of lesser classification or control. For additional information, see NSTISSI No. 7003. DoD has determined the information system distribution and transmission lines are not appropriate to define at the Enterprise level.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002931	PE-4	The organization defines security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities.	The organization being inspected/assessed defines and documents security safeguards to control physical access to organization-defined information system distribution and transmission lines within organizational facilities. DoD has determined the security safeguards are not appropriate to define at the Enterprise level.	APPLICABLE
CCI-000937	PE-5	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output		Impractical
CCI-000952	PE-9	The organization protects power equipment and power cabling for the information system from damage and destruction.	The organization being inspected/assessed provides a list of protective measures in place to prevent damage and/or destruction of power equipment and power cabling for their information system environment, IAW CP-2 (1), CCI 469.	APPLICABLE
CCI-002953	PE-9(1)	The organization employs redundant power cabling paths that are physically		APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		separated by organization-defined distance		
CCI-002954	PE-9(1)	The organization defines the distance to physically separate redundant power cabling paths.		N/A
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	Develop a diagram and explain within the system security plan (SSP) the authorization boundary for the complete control system including all networked devices and controller hardware.	N/A
CCI-003053	PL-2(a)(4)	The organization's security plan for the information system provides the security categorization of the information system including supporting rationale.	The NIST SP800-60, Vol 2, Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency. The recommended Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)} Therefore the system shall be categorized as a LOW-LOW-LOW system.	N/A
CCI-003071	PL-7(a)	The organization develops a security Concept of Operations (CONOPS) for the information	Concept of Operations is responsibility of the organization and System Owner.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system containing at a minimum, how the organization intends to operate the system from the perspective of information security.		
CCI-003072	PL-8(a)	The organization develops an information security architecture for the information system.	The organization being inspected/assessed develops and documents an information security architecture for the information system.	APPLICABLE
CCI-003073	PL-8(a)(1)	The organization's information security architecture for the information system describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	The organization being inspected/assessed describes within the information security architecture for the information system, the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.	APPLICABLE
CCI-003075	PL-8(a)(3)	The organization's information security architecture for the information	The organization being inspected/assessed describes within the information security architecture for the information system, any information security assumptions about, and dependencies on, external services.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system describes any information security assumptions about, and dependencies on, external services.		
CCI-000207	PM-5	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	APPLICABLE
CCI-000236	PM-11(b)	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	No additional protection needs are needed aside from what the network provider supplies. Control system components (not including servers and workstations) would generally be on a private PRIVATE VLAN without public access thereby further segregating the components from the cyber domain.	N/A
CCI-001048	RA-3(a)	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the	The conducting of a Risk Assessment will most likely be site specific. The owning organization will need to conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction. The Designer can assist in identifying risk to the owing organization in order to complete the risk assessment.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		unauthorized access, use, disclosure, disruption, modification, or destruction.		
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	Servers, workstations and network infrastructure on the network will be scanned for vulnerabilities by the network provider. All other IP devices associated with the system (whether on the public or private side of the network) 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. The owning organization will need a service level agreement (SLA) with the network provider to perform scanning of IP devices on a private PRIVATE VLAN or dark fiber network, or have in-house personnel assigned to perform the vulnerability scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities	Conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		potentially affecting the system/applications are identified and reported.		
CCI-001641	RA-5(a)	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001643	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	Servers, workstations and network infrastructure on the network will follow the process for random scans as defined by the Network Provider. The organization will conduct random vulnerability scans every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) for all other control system components on a PRIVATE VLAN or the portion not scannable by the Network Provider. The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of	The organization whether through the Network Provider or otherwise, employs the DoD Enterprise scanning tool.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.		
CCI-001058	RA-5(c)	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	N/A
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001062	RA-5(1)	The organization employs vulnerability scanning tools that include the capability to readily update the information	The organization being inspected/assessed will employ scanning tools that maintain currency with industry standard information system vulnerabilities to ensure that scanning activities are conducted with the most up to date list of known vulnerabilities to include USCYBERCOM issued IAVMs.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system vulnerabilities to be scanned.	DoD has provided an enterprise scanning tool that fully meets this requirement. Organizations that choose not to use the enterprise scanning tool must identify which scanning tool they are using and ensure that it meets these requirements.	
CCI-001067	RA-5(5)	The information system implements privileged access authorization to organization-identified information system components for selected organization-defined vulnerability scanning activities.	The organization being inspected/assessed configures the information system to implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1067. DoD has defined the information system components as all information systems and infrastructure components.	N/A
CCI-001645	RA-5(5)	The organization identifies the information system components to which privileged access is authorized for selected organization-defined vulnerability scanning activities.	DoD has defined the information system components as all information systems and infrastructure components.	N/A
CCI-002906	RA-5(5)	The organization defines the vulnerability	The organization being inspected/assessed defines and documents the vulnerability scanning activities in which the information	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		scanning activities in which the information system implements privileged access authorization to organization-identified information system components.	system implements privileged access authorization to organization-identified information system components. DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level.	
CCI-000623	SA-4(1)	The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	DoDI 8510.01 system categorization meets the DoD requirement for providing a description of the functional properties of the security controls to be employed. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DoDI 8510.01.	N/A
CCI-003101	SA-4(2)	The organization requires the developer of the information system, system component, or information system service to provide design information for the security controls to be	The organization being inspected/assessed defines and documents in contracts/agreements, the design information for the security controls that the developer will employ in the information system to include security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics and/or design/information defined in SA-4 (2), CCI 3103 at the level of detail defined in SA-4 (2), CCI 3105.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics and/or organization-defined design/information at organization-defined level of detail.		
CCI-003102	SA-4(2)	The organization requires the developer of the information system, system component, or information system service to provide implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics organization-defined	The organization being inspected/assessed defines and documents in contracts/agreements, the implementation information for the security controls that the developer will employ in the information system to include security-relevant external system interfaces, high-level design, low-level design, source code and/or hardware schematics and/or implementation information defined in SA-4 (2), CCI 3104 at the level of detail defined in SA-4 (2), CCI 3106.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		implementation information at organization-defined level of detail.		
CCI-003103	SA-4(2)	The organization defines the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed	The organization being inspected/assessed defines and documents the design information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the design information is not appropriate to define at the Enterprise level.	Impractical
CCI-003104	SA-4(2)	The organization defines the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed.	The organization being inspected/assessed defines and documents the implementation information that the developer of the information system, system component, or information system service is required to provide for the security controls to be employed. DoD has determined the implementation information is not appropriate to define at the Enterprise level.	Impractical
CCI-003105	SA-4(2)	The organization defines the level of detail the design information of the security controls is	The organization being inspected/assessed defines and documents the level of detail the design information of the security controls is required to be provided by the developer of the information system, system component,	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		required to be provided by the developer of the information system, system component, or information system services	or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level..	
CCI-003106	SA-4(2)	The organization defines the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services.	The organization being inspected/assessed defines and documents the level of detail the implementation information of the security controls is required to be provided by the developer of the information system, system component, or information system services. DoD has determined the level of detail is not appropriate to define at the Enterprise level.	Impractical
CCI-003114	SA-4(9)	The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended	The organization being inspected/assessed documents within contracts/agreements, the requirement that the developer of the information system, system component, or information system service identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. Ports identified shall be assessed and planned for in light of DISA's PPSM requirements.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		for organizational use.		
CCI-003116	SA-4(10)	The organization employs only information technology products on the FIPS PUB 201-2-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	Impractical
CCI-003124	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	APPLICABLE
CCI-003125	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		component, or information system services that describes secure installation of the system, component, or service.	secure installation of the system, component, or service.	
CCI-003126	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	APPLICABLE
CCI-003127	SA-5(a)(2)	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003128	SA-5(a)(3)	The organization obtains administrator	Document within contracts/agreements, requirements that the developer provide administrator documentation for the	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		documentation for the information system, system component, or information system services that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.	information system, system component or information system service that describe known vulnerabilities of the system, component, or service. To the extent possible this should also apply to Control System software applications.	
CCI-003129	SA-5(b)(1)	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003130	SA-5(b)(2)	The organization obtains user documentation for the information system, system component or information system service	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner.	To the extent possible this should also apply to Control System software applications.	
CCI-003131	SA-5(b)(3)	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003155	SA-10(A)	The organization requires the developer of the information system, system component, or information system service to perform configuration management during system, component or service design, development,	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service perform configuration management during system, component or service design, development, implementation and/or operation. The configuration management process applies to: 1. Documentation developed or used in the lifecycle, including requirements and interface specifications; 2. Elements including design libraries; 3. Tools including design tools and test tools; 4. Technical data including test data; and 5. Information on element and system	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		implementation and/or operation.	lifecycle processes	
CCI-003156	SA-10(b)	The organization requires the developer of the information system, system component, or information system service to document the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	N/A
CCI-003157	SA-10(b)	The organization requires the developer of the information system, system component, or information system service to manage the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements the requirement that the developer of the information system, system component, or information system service manage the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-003158	SA-10(b)	The organization requires the developer of the information system, system component, or information system service to control the integrity of changes to organization-defined configuration items under configuration management.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service control the integrity of changes to configuration items under configuration management defined in SA-10, CCI 3159.	N/A
CCI-003159	SA-10(b)	The organization defines the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled.	The organization being inspected/assessed defines and documents the configuration items under configuration management that require the integrity of changes to be documented, managed and controlled. DoD has determined the configuration items are not appropriate to define at the Enterprise level.	N/A
CCI-000692	SA-10(c)	The organization requires the developer of the information system, system component, or information system service to implement only	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service implement only organization-approved changes to the system, component, or service throughout its life cycle.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		organization-approved changes to the system, component, or service.		
CCI-000694	SA-10(d)	The organization requires the developer of the information system, system component, or information system service to document approved changes to the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document approved changes to the system, component, or service.	N/A
CCI-003160	SA-10(d)	The organization requires the developer of the information system, system component, or information system service to document the potential security impacts of approved changes to the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service document the potential security impacts of approved changes to the system, component, or service.	N/A
CCI-003161	SA-10(e)	The organization requires the developer of the information	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system, system component, or information system service to track security flaws within the system, component, or service.	track security flaws within the system, component, or service.	
CCI-003162	SA-10(e)	The organization requires the developer of the information system, system component, or information system service to track flaw resolution within the system, component, or service.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service track flaw resolution within the system, component, or service.	N/A
CCI-003163	SA-10(e)	The organization requires the developer of the information system, system component, or information system service to report security flaws and flaw resolution within the system, component, or service findings to organization-defined personnel.	The organization being inspected/assessed requires within contracts/agreements that the developer of the information system, system component, or information system service report security flaws and flaw resolution within the system, component, or service findings to at a minimum, the ISSO and ISSM. DoD has defined the personnel as at a minimum, the ISSO and ISSM.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-003171; 003172	SA-11(a)	The organization requires the developer of the information system, system component, or information system service to create a security assessment plan	The organization being inspected/assessed requires that the developer create and document a security assessment plan that includes: 1. The types of analyses, testing, evaluation, and reviews of software and firmware components; 2. The degree of rigor to be applied; and 3. The types of artifacts produced during those processes.	N/A
CCI-003173	SA-11(b)	The organization requires the developer of the information system, system component, or information system service to perform unit, integration, system, and/or regression testing/evaluation at organization	The organization being inspected/assessed documents within the contracts/agreements, the requirement that the developer of the information system, system component, or information system service perform unit, integration, system, and/or regression testing/evaluation at depth and coverage defined in SA-11, CCI 3174.	N/A
CCI-003174	SA-11(b)	The organization defines the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation	The organization being inspected/assessed defines and documents the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation. Examples of approaches or tool types that could be required are: 1. Approaches such as static analyses, dynamic analyses, binary analysis, or a hybrid of the three approaches; and 2. Tools such as web-based application scanners, static analysis tools, binary	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			analyzers. DoD has determined the depth and coverage are not appropriate to define at the Enterprise level.	
CCI-003175	SA-11(c)	The organization requires the developer of the information system, system component, or information system service to produce evidence of the execution of the security assessment plan	The organization being inspected/assessed requires the developer to produce and provide evidence of the execution of the security assessment plan.	N/A
CCI-003176	SA-11(c)	The organization requires the developer of the information system, system component, or information system service to produce the results of the security	The organization being inspected/assessed requires the developer to produce and provide results of the security testing/evaluation.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-003177	SA-11(d)	The organization requires the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process	The organization being inspected/assessed requires the developer to implement a verifiable flaw remediation process.	N/A
CCI-003178	SA-11(e)	The organization requires the developer of the information system, system component, or information system service to correct flaws identified during security testing/evaluation	The organization being inspected/assessed requires the developer to correct flaws identified during security testing/evaluation and to document and provide evidence that the flaws were corrected.	N/A
CCI-001082	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	The organization being inspected/assessed configures the information system to separate user functionality (including user interface services) from information system management functionality. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001093	SC-5	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	Definition of the types of denial of service attacks will be defined at the Network Provider level.	APPLICABLE
CCI-002385	SC-5	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-defined security safeguards.	For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE
CCI-002386	SC-5	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	Definition of the security safeguard to be employed to protect the information system will be defined at the Network Provider level for all devices on the Network Provider. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE
CCI-001097	SC-7(a)	The information system monitors and controls communications at the external	Monitoring and the controlling of communications at the external boundary of the system will be the responsibility of the Network Provider. The control system shall not be publicly accessible.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		boundary of the system and at key internal boundaries within the system.		
CCI-001109	SC-7(5)	The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception	The organization being inspected/assessed configures the information system to deny network communications traffic at managed interfaces by default and allows network communications traffic by exception (i.e., deny all, permit by exception). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE
CCI-001126	SC-7(18)	The information system fails securely in the event of an operational failure of a boundary protection device.	This control applies to network devices that control system is connected to.	APPLICABLE
CCI-002418	SC-8	The information system protects the confidentiality and/or integrity of transmitted information.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of transmitted information. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002419	SC-8(1)	The organization defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented to protect information during transmission.	DoD has defined the alternative physical safeguards as Protected Distribution System (PDS).	APPLICABLE
CCI-002421	SC-8(1)	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.	The organization being inspected/assessed configures the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Protected Distribution System (PDS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if control system can employ cryptographic mechanisms.
CCI-001133	SC-10	The information system terminates the network	The organization being inspected/assessed configures the information system to terminate the network connection associated	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity	with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001134	SC-10	The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.	DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	Impractical
CCI-001160; 001161; 001162; 001163; 001164; 001165	SC-18(a)(b)(c)	The organization controls the use of mobile code within the information system.	The organization being inspected/assessed documents and implements a process to control the use of mobile code within the information system.	N/A – There is no mobile code being used.
CCI-001184	SC-23	The information system protects the authenticity of communications sessions.	The organization being inspected/assessed configures the information system to protect the authenticity of communications sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001190; 001191; 001192; 001193; CCI-001665	SC-24	The information system preserves organization-defined system state information in the event of a system failure.	The organization being inspected/assessed configures the information system to preserve information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes in the event of a system failure. Control system must be configured to store information in the event of a failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE
CCI-001199	SC-28	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	The organization being inspected/assessed configures the information system to protect the confidentiality and/or integrity of organization-defined information at rest. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	N/A
CC-002472	SC-28	The organization defines the information at rest that is to be protected by the information system.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by the information system which must include, at a minimum, PII and classified information. DoD has determined the information at rest is not appropriate to define at the Enterprise level. This information is typically not stored on Control Systems.	N/A
CCI-002530	SC-39	The information system maintains a separate execution domain for each executing process.	To the greatest extent practical, the hardware performs control sequences without reliance on the network.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002544	SC-41	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed.	Define and document the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed. The control system has a specific purpose (not a general one) and its function (and limitations) are specified by the control system architecture and protocols. Specifications should require disabling any ports/protocols/services not specifically needed by the control system. Required software should be covered by specification, all other software should be prohibited.	APPLICABLE
CCI-002545	SC-41	The organization defines the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components.	Document the connection ports or input/output devices that are to be physically disabled or removed from organization-defined information systems or information system components. The control system has a specific purpose (not a general one) and its function (and limitations) are specified by the control system architecture and protocols. Specifications should require disabling any ports/protocols/services not specifically needed by the control system. Required software should be covered by specification, all other software should be prohibited.	APPLICABLE
CCI-002546	SC-41	The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined	Physically disable or remove connection ports or input/output devices.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information systems or information system components.		
CCI-001241	SI-3(c)(1)	The organization configures malicious code protection mechanisms to perform periodic scans of the information system on an organization-defined frequency.	The Network Provider will implement/configure security scanning for servers and workstations on their network. Servers and workstations installed under this project that are on a PRIVATE VLAN, the owning organization must install and configure malware protection software. Configure software to perform a full system scan every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	Impractical
CCI-002623	SI-3(c)(1)	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	Impractical
CCI-001253	SI-4(a)(1)	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	Network monitoring is conducted by the network provider for control system components on non-private (VLAN) side. Network monitoring cannot be implemented for field devices/components on the private network (VLAN).	Impractical
CCI-002703	SI-7	The organization defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes.	The organization being inspected/assessed defines and documents the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes. DoD has determined the software, firmware, and information are not appropriate to define at the Enterprise level.	Impractical
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed	The organization being inspected/assessed defines and documents the software on which integrity checks will be performed. DoD has determined the software is not appropriate to define at the Enterprise level.	Impractical
CCI-002706	SI-7(1)	The organization defines the firmware on which integrity checks will be performed.	The organization being inspected/assessed defines and documents the firmware on which integrity checks will be performed. DoD has determined the firmware is not appropriate to define at the Enterprise level.	Impractical
CCI-002707	SI-7(1)	The organization defines the information on which integrity checks will be performed.	The organization being inspected/assessed defines and documents the information on which integrity checks will be performed. DoD has determined the information is not appropriate to define at the Enterprise level.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002710	SI-7(1)	The information system performs an integrity check of organization-defined software at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	The organization being inspected/assessed configures the information system to perform an integrity check of software defined in SI-7 (1), CCI 2705 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2710. DoD has defined the frequency as annually.	APPLICABLE if capability exists
CCI-002711	SI-7(1)	The information system performs an integrity check of organization-defined firmware at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	The organization being inspected/assessed configures the information system to perform an integrity check of firmware defined in SI-7 (1), CCI 2706 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2711. DoD has defined the frequency as annually.	APPLICABLE if capability exists
CCI-002712	SI-7(1)	The information system performs an integrity check of organization-defined information at startup, at organization-defined transitional states	The organization being inspected/assessed configures the information system to perform an integrity check of information defined in SI-7 (1), CCI 2707 at startup, at transitional states or security-relevant events defined in SI-7 (1), CCI 2708, or annually. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		or security-relevant events, or on organization-defined frequency.	STIG/SRG guidance. DoD has defined the frequency as annually.	
CCI-001310	SI-10	The information system checks the validity of organization-defined inputs.	The organization being inspected/assessed configures the information system to check the validity of all inputs except those identified specifically by the organization. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical
CCI-002744	SI-10	The organization defines the inputs the information system is to conduct validity checks.	The organization being inspected/assessed defines and documents specific inputs which do not require validity checks. DoD has defined the information inputs as all inputs except those identified specifically by the organization.	N/A
CCI-001312	SI-11(a)	The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	The organization being inspected/assessed configures the information system to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE
CCI-002773	SI-17	The organization defines the fail-safe procedures to be implemented by the information system when	In many cases standard control system design of sequences and alarm requirements address these CCIs without any additional design requirements	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.21 Attachment A Fire and Life Safety LOW-LOW-MOD				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		organization-defined failure conditions occur.		
CCI-002774	SI-17	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	Failure conditions likely to be experienced by control system components are component failure and communications failure to components.	APPLICABLE
CCI-002775	SI-17	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	Configure the information system to implement fail-safe procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

SECTION 25 05 11.23 01

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC

PART 1 GENERAL

This section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

1.1 CONTROL SYSTEM APPLICABILITY

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: Utility Monitoring Control System to include HVAC.

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

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.

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

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

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. Submittals with an "S" are for inclusion in the Sustainability eNotebook, in conformance with Section 01 33 29 SUSTAINABILITY REPORTING. 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

Qualifications; 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 Cybersecurity Representative

Provide a Cybersecurity Representative as the key person to implement and manage the cybersecurity related control systems of the project. This individual must have a minimum of 2 years of cybersecurity control systems experience, including two projects of similar size and complexity. Submit the Cybersecurity Representative's certification of qualifications no later than 60 calendar days after Notice to Proceed. Submit one hard copy and an electronic copy.

1.7.1.1 Duties

The Cybersecurity Representative must lead and oversee the cybersecurity control systems work specified herein and be the primary point of contact for the Government regarding the cybersecurity work.

1.7.1.2 Qualifications

The individual must have a minimum of 2 years with Risk Management Framework implementation experience and experience with Facility Related Control System cybersecurity implementation such as a control system related training or certification.

1.7.2 Cybersecurity Kickoff Meeting

Within 60 calendar days after contract award, the Cybersecurity Representative must schedule a Cybersecurity Kickoff Meeting with the Contracting Officer, system owner, system program manager, and Information System Security Manager (ISSM). The meeting will be located at a specific time and place to be determined by the Contracting Officer.

1.8 CYBERSECURITY DOCUMENTATION

1.8.1 Cybersecurity Interconnection Schedule

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-graphics-tables.)

1.8.2 Network Communication Report

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.

1.8.3 Control System Inventory Report

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-graphics-tables documenting all 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.

1.8.4 Software Recovery and Reconstitution Images

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.

1.8.5 Cybersecurity Riser Diagram

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 overlayed on a facility schematic.

1.8.6 Control System Cybersecurity Documentation

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

1.8.6.1 Software Applications

For all software applications running on computers provide:

a. Administrator documentation that describes secure configuration of the software.

b. Administrator documentation that describes secure installation of the software.

c. Administrator documentation that describes secure operation of the software.

d. Administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software.

e. Administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software.

f. User documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms.

g. User documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner.

h. User documentation that describes user responsibilities in maintaining the security of the software.

1.8.6.2 For HVAC Control System Devices

1.8.6.2.1 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.

b. Documentation that describes secure operation of the device.

c. Documentation that describes effective use and maintenance of security functions or mechanisms for the device.

d. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device.

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.

f. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner.

1.8.6.2.2 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.

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.

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.

1.8.6.3 Default Requirements for Control System Devices

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.

b. Documentation that describes secure installation of the device.

c. Documentation that describes secure operation of the device.

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device.

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device.

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms.

g. Documentation that describes methods for user interaction which enables individuals to use the device in a more secure manner.

h. Documentation that describes user responsibilities in maintaining the security of the device.

1.9 SOFTWARE UPDATE LICENSING

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.

1.10 CYBERSECURITY DURING CONSTRUCTION

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

1.10.1 Contractor Computer Equipment

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

1.10.1.1 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.

1.10.1.2 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.

1.10.1.3 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.

1.10.1.4 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-graphics-tables. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.10.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks must meet the following requirements:

1.10.2.1 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.

1.10.3 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

1.10.4 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.

1.10.5 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.

1.10.6 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-graphics-tables. 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.

1.11 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

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.

Implement a warning banner on terminal interfaces that conforms to DoD warning banner guidelines. Configure each component of the product to operate using the principle of least privilege. This includes operating communications, and energy delivery system services.

Provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. Provide a system administration mechanism for changing user(s') role (e.g., group) associations.

Configure the product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side. Provide a method for protecting against unauthorized privilege escalation.

Document options for defining access and security permissions, user accounts, and applications with associated roles. Configure these options as specified.

Prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware and document if not feasible, provide mitigation recommendations.

Verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

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 Default Requirements for Control System Devices

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

a. Devices with web interfaces must either FULLY support user accounts or have their web interface disabled.

b. Field devices with full local user interfaces allowing modification of data must FULLY support user accounts.

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

3.1.2 Account Management

Document all accounts (including but not limited to, generic or default) that need to be active for proper operation of the product. Change default account settings to specific settings (e.g., length, complexity, history, and configurations) provided by government representative. Changed account information will not be published. All new account information will be provided by a protected mechanism. Remove or disable any accounts that are not needed for normal or maintenance operations of the control system. Accounts for emergency operations shall be placed in a highly secure configuration and documentation must be provided.

3.1.3 Unsuccessful Logon Attempts

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon

attempts.

3.1.3.1 Devices MINIMALLY Supporting Accounts

Devices which MINIMALLY support accounts must lock the user input after three unsuccessful logon attempts and must support unlocking of the user input when unlocked by an administrator.

3.1.3.2 Devices FULLY Supporting Accounts

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.

3.1.3.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

Contact local ISSM and System Owner/Program Manager for requirements for high availability interfaces that are exempt from unsuccessful logon attempts. Work with local ISSM and local CIO to complete the following:

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

3.1.4 System Use Notification

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.

3.1.4.1 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

3.1.5 Permitted Actions Without Identification or Authentication

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.

3.1.6 Wireless Access

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).

3.1.6.1 Wireless IP Communications

Do 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.

3.1.6.2 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.

3.1.6.3 Wireless Communication Request

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-graphics-tables.

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.

3.1.6.4 Wireless Communication Testing

As part of Performance Verification Testing (PVT), 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. 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

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

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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

f. Successful and unsuccessful accesses to objects

g. All program initiations

h. All direct access to the information system

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

j. 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 Default Requirements for Control System Devices

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

3.2.1.3.1 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

3.2.1.3.1.1 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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

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

g. All kernel module load, unload, and restart

3.2.1.3.1.2 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

3.2.1.3.2 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

a. For devices that have STIG/SRGs related to audit storage capacity 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 audit records in conformance with applicable STIG/SRGs.

3.2.2.1 Device Audit Record Upload Software

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 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.

Contact local ISSM and System Owner/Program Manager for device audit record upload software requirements. 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

Front end computers associated with auditing must, in the case of a failure in the auditing system, notify ISSM 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

3.2.4.1 Computers

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

Time stamp requirements for HVAC Control Systems are as indicated in the Control System specifications.

3.2.4.3 Control System Devices

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

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

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

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

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 Default Requirements for Control System Devices

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.

3.5.2 Authenticator Management

3.5.2.1 Authentication Type

3.5.2.1.1 For HVAC Control System Devices

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.

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 Default Requirements for Control System Devices

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.

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

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

Devices minimally supporting accounts must support passwords with a minimum length of four characters.

3.5.2.2.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with ISSM. 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 hard copies 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

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, comply with the requirements of those STIGS/SRGs.

3.5.4 Device Identification and Authentication

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 ISSM.

3.5.4.1 For HVAC Control System Devices

Contact local ISSM and System Owner/Program Manager for HVAC Device Protocol Requirements.

3.5.4.2 Default Requirements for Control System Devices

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 ISSM instead.

3.5.5 Cryptographic Module Authentication

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

3.6 EMERGENCY POWER

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

3.7 DURABILITY TO VULNERABILITY SCANNING

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 Assured Compliance Assessment Solution (ACAS) by responding with a valid credentialed scan. 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 Default Requirements for Control System Devices

Non-computer control system devices where Durability to Vulnerability Scanning requirements are not otherwise indicated in this Section are not required to respond to scans.

3.8 FIPS 201-2 REQUIREMENT

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list.

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-graphics-tables to request approval for each device.

3.10 SYSTEM AND COMMUNICATION PROTECTION

3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection

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

3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

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

3.12 FIELD QUALITY CONTROL

3.12.1 Tests

In addition to testing and testing support required by other sections, provide a minimum of 80 hours of technical support for cybersecurity testing of control systems.

-- End of Section --

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002110	AC-2 (a)	The organization defines the information system account types that support the organizational missions/business functions.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions.	N/A
CCI-000213	AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Any device supporting accounts (either fully or partially) must limit access to the device according to specified limitations for each account. Install and configure any device having a Security Technical Implementation Guide (STIG) or Security Requirements Guide (SRG) in accordance with that STIG or SRG.	Impractical
CCI-000043	AC-7(A)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	APPLICABLE if system has capability
CCI-000044	AC-7(a)	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-	The information system shall be set to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval. Devices which Partially support accounts shall implement the requirements of a FULLY supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined time period.	physical access to the device should limited to only authorized personnel. Document any device incapable of meeting the defined requirement and state actual implementation.	
CCI-001423	AC-7(a)	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occurs.	DOD policy requires the system to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval.	APPLICABLE if system has capability.
CCI-002236	AC-7(a)	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires for systems that once an account is locked, the account must stay locked until unlocked by an administrator. This may have safety implications in control system environment. Implement with caution.	APPLICABLE if system has capability.
CCI-002237	AC-7(a)	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires that once the indicated number of unsuccessful login attempts occurs, delay login prompts by **[5] seconds**. If the provided software cannot meet these requirements, document software capabilities to protest from subsequent unsuccessful login attempts and propose alternate protections. Do not implement alternate protection measures without explicit permission from the System Owner.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002238	AC-7(a)	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The information system shall be configured to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Devices which Partially support accounts shall implement the requirements of a Fully supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel.	APPLICABLE if system has capability.
CCI-000048	AC-8(a)	The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives,	All devices (PC's, BPOCs, Network switches, etc…) with a user interface supporting the use of a password or PIN, and capable of displaying 50 or more alphanumeric characters shall be configured to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. The DOD Consent Banner can be found on the RMF Knowledge Service site at	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		policies, regulations, standards, and guidance.	https://rmfks.osd.mil/rmf/Guidance/GoverningPolicy/Pages/ConsentBanner.aspx Devices connected to a network, with a user interface supporting use of a password or PIN, and **not capable** of displaying 50 or more alphanumeric characters must have a permanently affixed label displaying an approved banner from the policy listed above.	
CCI-002247	AC-8(a)	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-002243	AC-8(a)(1)	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002244	AC-8(a)(2)	The organization-defined information system use notification message or banner is to state that information system usage may	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		be monitored, recorded, and subject to audit.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	
CCI-002245	AC-8(a)(3)	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002246	AC-8(a)(4)	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-000050	AC-8(a)(4)	The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit	Configure the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		actions to log on to or further access.		
CCI-002248	AC-8(C)(1)	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-000061	AC-14(a)	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following: • Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by the System Owner.
CCI-000232	AC-14(b)	The organization documents and provides supporting rationale in the security plan for the information system, user actions not	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following:	Impractical unless required by the System Owner.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		requiring identification and authentication	• Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	
CCI-001438	AC-18(a)	The organization establishes usage restrictions for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001439	AC-18(a)	The organization establishes implementation guidance for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-002323	AC-18(a)	The organization establishes configuration/connection requirements for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001441	AC-18(b)	The organization authorizes wireless access to the information system prior to allowing such connections.	Required if System relies on RF connectivity.	APPLICABLE
CCI-000123	AU-2(a)	The organization determines the information system must be capable of	HW (workstations, servers, network switches/infrastructure, etc…) capable of auditing shall audit the following: • Successful and unsuccessful logon attempts	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		auditing an organization-defined list of auditable events.	• Privileged activities or other system level access • Starting and ending time for user access to the system • Concurrent logons from different workstations. • Successful and unsuccessful accesses to objects • All program initiators • All direct access to the information system • All account creations, modifications, disabling, and terminations • All kernel module load, unload, and restart	
CCI-001571	AU-2(a)	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	APPLICABLE only if capability exists
CCI-000125	AU-2(c)	The organization provides a rationale for why the list of auditable events is deemed to be adequate to	The organization documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		support after-the-fact investigations of security incidents.		
CCI-001485	AU-2(d)	The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	N/A
CCI-000130	AU-3	The information system generates audit records containing information that establishes what type of event occurred.	The information system shall be configured to generate audit records containing information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (FPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000131	AU-3	The information system generates audit records containing information that establishes when an event occurred.	The information system shall be configured to generate audit records containing information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000132	AU-3	The information system generates audit records containing information that establishes where the event occurred.	The information system shall be configured to generate audit records containing information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000133	AU-3	The information system generates audit records containing information that establishes the source of the event.	The information system shall be configured to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000134	AU-3	The information system generates audit records containing information that establishes the outcome of the event.	The information system shall be configured to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001487	AU-3	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The information system shall be configured to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance that pertains to CCI 1487. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-001848	AU-4	The organization defines the audit record storage requirements	Devices that have STIG/SRGs must comply with the requirements of those STIG/SRGs. For BPOCs and field devices (not front end computers) capable of generating audit records, the front end server shall be configured to retrieve audit records from the devices. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-001849	AU-4	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	The organization allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 001848. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	If the front end server can be configured to automatically archive full logs or write audit logs to an audit server (from all connected audit capable devices), then this control shall be considered not-applicable (NA). Otherwise, if email services are available, configure the workstations and servers to alert at a minimum, the system administrator (SA) and	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			or the designated Information System Security Officer/Manager in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. If email services are not available then the workstations and servers shall configure the system to provide an alert on the screen in the event of an audit processing failure.	
CCI-000140	AU-5(b)	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	In case of an audit failure, if possible, configure the system to continue to collect audit records by overwriting existing audit records starting with the oldest records first. Ideal configuration would be to configure the system to send audit records directly to an audit server, or automatically archive full logs and document as such with the ISSO. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	APPLICABLE if capability exists
CCI-001490	AU-5(b)	The organization defines actions to be taken by the information system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure as described in CCI-000139 and CCI-000140.	N/A
CCI-000159	AU-8(a)	The information system uses internal system clocks to generate	Workstations and servers on the domain shall be configured to synchronize with domain controllers. If an NTP server is configured it should synchronize with a secure, authorized	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		time stamps for audit records.	source. If not on a domain or NTP server, workstations, server or other components that generate audit records, the timing requirement inherent in the control system will be sufficient. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001889	AU-8(b)	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001890	AU-8(b)	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	All devices which provide audit capabilities, configure them to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000169	AU-12(a)	The information system provides audit record generation capability for the auditable events defined in AU-2(a) at organization defined information system components.	CCI-000123 defines auditable events for an information system. Level 4 devices (workstations, servers, network switches, routers, etc.) shall implement to the extent possible the requirements in CCI-000123 and AU-2(a). Requirements that cannot be implemented must be documented and justification provided. Other devices (non level 4) that provide auditing capabilities shall implement the requirements in CCI-000123 where the capability exists and the ISSM deems relevant. Example, for components.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	
CCI-001459	AU-12(a)	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components. Devices which ARE NOT capable of generating an audit log are exempt. System documentation should define which components are capable and are not capable of generating audit logs.	APPLICABLE if capability exists
CCI-000171	AU-12(b)	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system	Configure all capable devices to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM. System administrator personnel will inherently have the rights associated with their accounts to select auditable events, however, organizational policy shall only authorize the ISSM or individuals appointed by the ISSM to select and make those necessary changes.	N/A
CCI-001910	AU-12(b)	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	N/A
CCI-000172	AU-12(c)	The information system generates audit records for	Audit record requirements are defined in CCI-000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487 above. For	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		the events defined in AU-2(d) with the content defined in AU-3.	information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.	Interconnections to other systems WILL NOT be implemented. Front end servers and workstations may reside on the local Network Enterprise Center's (NECs) network allowing a connection into the control system (CS) components.	N/A No Interconnects
CCI-002102	CA-9(a)	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	Define and document the information system components or classes of components that that are authorized internal connections to the information system. (e.g. Network Controllers, switches, routers, etc…)	APPLICABLE
CCI-002103	CA-9(b)	The organization documents, for each internal connection, the interface characteristics.	The organization documents, for each internal connection (network controllers, etc…) the communication protocols used and a general description of what information is communicated over the network. This can be accomplished through a network communication report.	APPLICABLE
CCI-002104	CA-9(b)	The organization documents, for each internal connection, the security requirements.	The organization documents, for each internal connection, the security requirements.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002105	CA-9(b)	The organization documents, for each internal connection, the nature of the information communicated.	See CCI-002103	APPLICABLE
CCI-000293	CM-2	The organization develops and documents a current baseline configuration of the information system.	Develop and document a current baseline configuration of the information system to include, drawings, software licenses, source code, hardware, etc…	APPLICABLE
CCI-000363	CM-6(a)	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). Document in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components. Field Devices (BPOCs, etc…) that do not have STIGs, SRGs, etc…obtain vendor configuration guides.	N/A
CCI-000364	CM-6(a)	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		configuration checklists.		
CCI-000365	CM-6(a)	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001588	CM-6(a)	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001755	CM-6(c)	The organization defines the information system components for which any	DoD has defined the information system components as all configurable information system components.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		deviation from the established configuration settings are to be identified, documented and approved.		
CCI-000381	CM-7(a)	The organization configures the information system to provide only essential capabilities.	Disable all ports, protocols and services not specifically needed by any device or component within the Control system (server, workstations, field devices, BPOCS, switches, etc…) Remove all software not specifically needed for use in the control system.	APPLICABLE
CCI-000380	CM-7(b)	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.		APPLICABLE
CCI-000382	CM-7(b)	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.		APPLICABLE
CCI-001761	CM-7(1)(b)	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed	Define and document in the system security plan, the functions, ports, protocols and services within the control system that are to be disabled when deemed unnecessary.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		unnecessary and/or non-secure.		
CCI-001762	CM-7(1)(b)	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	Disable functions, ports, protocols, and services within the control system deemed to be unnecessary and/or nonsecure, nonsecure functions, ports, protocols, and services.	APPLICABLE
CCI-000389	CM-8(a)(1)	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	Provide a Control System inventory report covering all networked, including network infrastructure devices. Provide the following information (where applicable): • If the device has (in other project documentation) a unique identifier • Description, make, mode, serial number, location • Software/firmware version Network information: protocol, network address	APPLICABLE
CCI-000392	CM-8(a)(2)	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the	See CCI-000389	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information system.		
CCI-000398	CM-8(a)(4)	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	APPLICABLE
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization must develop a contingency plan (CP) addressing recovery and reconstitution of the control system to a known state after a disruption In essence, restoring the system to the appropriate operational state. The CP will be site specific and should be developed in conjunction with stakeholders of the system. Copies of required software, backup data, hardware list and baseline configurations should be identified in the CP. NOTE-known state shall also include the accepted “as-built” documentation and include any custom programming and configuration for controllers or workstations.	APPLICABLE
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan. See also CCI-000550	APPLICABLE
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system to a known state after a failure.	must identify the selected method in the contingency plan. See also CCI-000550	
CCI-002855	CP-12	The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	Configure the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 002857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	APPLICABLE
CCI-002856	CP-12	The organization defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	When the following conditions are detected, the control system shall enter a safe mode of operation. • Commercial Power Loss • Fire • Water	APPLICABLE
CCI-002857	CP-12	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	**Commercial Power Failure:** Upon loss of commercial power, the control system will switch to Generator power and only Mission Critical Infrastructure (deemed by the organization) will received continued control system service. All other infrastructure/areas services will cease until commercial power is restored. **Fire:** The system shall be integrated with fire detectors. Upon detection of fire, the system will ensure dampers and air handlers are shut	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			down to prevent the propagation of smoke, gasses and fire through the system. The system shall remain in a shutdown/closed state until manually restarted/rebooted by organization personnel. **Water:** Upon detection of water (sprinkler system), the servers shall perform a graceful shutdown in order to minimize component failure due to water.	
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	All components capable of user accounts will be configured to uniquely identify and authenticate users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.	Multifactor authentication shall be implemented for users that require privileged level accounts to servers and workstations residing on the network (not standalone or PRIVATE VLAN segregated systems). Multifactor authentication can be implemented with through common access card (CAC) authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000777	IA-3	The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system.	All network connected endpoint devices (including but not limited to: workstations, printers, servers) shall be identified and authenticated before establishing a connection to the information system. Any device incapable of being authenticated to the system shall be documented.	APPLICABLE if capability exists
CCI-000778	IA-3	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to identify all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001958	IA-3	The information system authenticates an organization defined list of specific and/or types of devices before	Configure the network infrastructure to authenticate all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		establishing a local, remote, or network connection.	inspected/assessed must comply with the STIG/SRG guidance.	
CCI-000176	IA-5(b)	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	N/A
CCI-001544	IA-5(c)	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	APPLICABLE if capability exists
CCI-001989	IA-5(e)	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	Document and implement procedures to change default authenticators (passwords, etc.) or apply authenticators to all capable components prior to system installation.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000182	IA-5(g)	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	Document and implement procedures for changing/refreshing authenticators in the following time periods: • Password: 60 days.	N/A
CCI-001610	IA-5(g)	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period of Password: 60 days. Biometrics: every 3 years.	N/A
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	APPLICABLE if capability exists
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	APPLICABLE if capability exists
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	APPLICABLE if capability exists
CCI-001611	IA-5(1)(a)	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	APPLICABLE if capability exists
CCI-001612	IA-5(1)(a)	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	APPLICABLE if capability exists
CCI-001613	IA-5(1)(a)	The organization defines the minimum number of lower case	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		characters for password complexity enforcement.		
CCI-001614	IA-5(1)(a)	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	APPLICABLE if capability exists
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	APPLICABLE if capability exists
CCI-000195	IA-5(1)(b)	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195.	APPLICABLE if capability exists
CCI-001615	IA-5(1)(b)	The organization defines the minimum number of characters that are changed when	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		new passwords are created.	of characters as 50% of the minimum password length.	
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-protected passwords.	Configure the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	APPLICABLE if capability exists
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	APPLICABLE if capability exists
CCI-000198	IA-5(1)(d)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	APPLICABLE if capability exists
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.	Configure the information system to enforce maximum password lifetime restrictions. For capable components, set maximum password age to 60 days or less (excluding “0”). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	APPLICABLE if capability exists
CCI-001616	IA-5(1)(d)	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001617	IA-5(1)(d)	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days and not being "0".	APPLICABLE if capability exists
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. All other components utilizing passwords, the password reuse should be set to 24. If the components are incapable of being set to 24 then implement the maximum possible.	APPLICABLE if capability exists
CCI-001618	IA-5(1)(e)	The organization defines the number of generations for which password reuse is prohibited.	Per the STIGs for Windows based systems, the DOD has defined this to be set at a minimum of 24.	APPLICABLE if capability exists
CCI-002041	IA-5(1)(f)	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	APPLICABLE if capability exists
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		token-based authentication.	hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.	
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	APPLICABLE if capability exists
CCI-000206	IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Configure the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206. Applicable to networked devices. Does not apply to devices that have NO feedback during password/PIN entry.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			Devices shall 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 CCI-000206, comply with the requirements of those STIGS/SRGs.	
CCI-000803	IA-7	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	For devices that have STIG/SRGs related to CCI-000803, comply with the requirements of those STIG/SRGs.	APPLICABLE if capability exists
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	Develop a diagram and explain within the system security plan (SSP) the authorization boundary for the complete control system including all networked devices and controller hardware.	N/A
CCI-003053	PL-2(a)(4)	The organization's security plan for the information system provides the security	The NIST SP800-60, Vol 2, Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		categorization of the information system including supporting rationale.	environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency. The recommended Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)} Therefore the system shall be categorized as a LOW-LOW-LOW system.	
CCI-000207	PM-5	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	APPLICABLE
CCI-000236	PM-11(b)	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	No additional protection needs are needed aside from what the network provider supplies. Control system components (not including servers and workstations) would generally be on a private PRIVATE VLAN without public access thereby further segregating the components from the cyber domain.	N/A
CCI-001048	RA-3(a)	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of	The conducting of a Risk Assessment will most likely be site specific. The owning organization will need to conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	The Designer can assist in identifying risk to the owing organization in order to complete the risk assessment.	
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	Servers, workstations and network infrastructure on the network will be scanned for vulnerabilities by the network provider. All other IP devices associated with the system (whether on the public or private side of the network) 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. The owning organization will need a service level agreement (SLA) with the network provider to perform scanning of IP devices on a private PRIVATE VLAN or dark fiber network, or have in-house personnel assigned to perform the vulnerability scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new	Conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		vulnerabilities potentially affecting the system/applications are identified and reported.		
CCI-001641	RA-5(a)	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001643	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	Servers, workstations and network infrastructure on the network will follow the process for random scans as defined by the Network Provider. The organization will conduct random vulnerability scans every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) for all other control system components on a PRIVATE VLAN or the portion not scannable by the Network Provider.. The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and	The organization whether through the Network Provider or otherwise, employs the DoD Enterprise scanning tool.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.		
CCI-001058	RA-5(c)	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	N/A
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-003116	SA-4(10)	The organization employs only information technology products on the FIPS PUB 201-2-approved	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.		
CCI-003124	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	APPLICABLE
CCI-003125	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-003126	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	APPLICABLE
CCI-003127	SA-5(a)(2)	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003128	SA-5(a)(3)	The organization obtains administrator documentation for the information system, system component, or information system services that describes known	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.		
CCI-003129	SA-5(b)(1)	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003130	SA-5(b)(2)	The organization obtains user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner. To the extent possible this should also apply to Control System software applications.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		service in a more secure manner.		
CCI-003131	SA-5(b)(3)	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-001093	SC-5	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	Definition of the types of denial of service attacks will be defined at the Network Provider level.	APPLICABLE
CCI-002385	SC-5	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-	For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined security safeguards.		
CCI-002386	SC-5	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	Definition of the security safeguard to be employed to protect the information system will be defined at the Network Provider level for all devices on the Network Provider. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE
CCI-001097	SC-7(a)	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	Monitoring and the controlling of communications at the external boundary of the system will be the responsibility of the Network Provider. The control system shall not be publicly accessible.	N/A
CCI-001133	SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity	The organization being inspected/assessed configures the information system to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001134	SC-10	The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.	DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	Impractical
CCI-002530	SC-39	The information system maintains a separate execution domain for each executing process.	To the greatest extent practical, the hardware performs control sequences without reliance on the network.	APPLICABLE
CCI-002544; 002545;002546	SC-41	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed	Physically disable or remove connection ports or input/output devices.	APPLICABLE
CCI-001241	SI-3(c)(1)	The organization configures malicious code protection mechanisms to perform periodic scans of the	The Network Provider will implement/configure security scanning for servers and workstations on their network. Servers and workstations installed under this project that are on a PRIVATE VLAN, the owning organization must install and configure malware protection software.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information system on an organization-defined frequency.	Configure software to perform a full system scan every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	
CCI-002623	SI-3(c)(1)	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	Impractical
CCI-001253	SI-4(a)(1)	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	Impractical
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	Network monitoring is conducted by the network provider for control system components on non-private (VLAN) side. Network monitoring cannot be implemented for field devices/components on the private network (VLAN).	Impractical
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed	The organization being inspected/assessed defines and documents the software on which integrity checks will be performed. DoD has determined the software is not appropriate to	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.23 01 Attachment A UTILITY MONITORING CONTROL SYSTEM (UMCS) TO INCLUDE HVAC LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			define at the Enterprise level.	
CCI-002773	SI-17	The organization defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur.	In many cases standard control system design of sequences and alarm requirements address these CCIs without any additional design requirements	APPLICABLE
CCI-002774	SI-17	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	Failure conditions likely to be experienced by control system components are component failure and communications failure to components.	APPLICABLE
CCI-002775	SI-17	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	Configure the information system to implement fail-safe procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION 25 05 11.26 01

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)

PART 1 GENERAL

This section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

1.1 CONTROL SYSTEM APPLICABILITY

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: Utility Control Systems including Electrical Transmission and Distribution and Uninterruptible Power Supply (UPS).

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

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.

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

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

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. Submittals with an "S" are for inclusion in the Sustainability eNotebook, in conformance with Section 01 33 29 SUSTAINABILITY REPORTING. 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

Qualifications; 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 Cybersecurity Representative

Provide a Cybersecurity Representative as the key person to implement and manage the cybersecurity related control systems of the project. This individual must have a minimum of 2 years of cybersecurity control systems experience, including two projects of similar size and complexity. Submit the Cybersecurity Representative's certification of qualifications no later than 60 calendar days after Notice to Proceed. Submit one hard copy and an electronic copy.

1.7.1.1 Duties

The Cybersecurity Representative must lead and oversee the cybersecurity control systems work specified herein and be the primary point of contact for the Government regarding the cybersecurity work.

1.7.1.2 Qualifications

The individual must have a minimum of 2 years with Risk Management Framework implementation experience and experience with Facility Related Control System cybersecurity implementation such as a control system related training or certification.

1.7.2 Cybersecurity Kickoff Meeting

Within 60 calendar days after contract award, the Cybersecurity Representative must schedule a Cybersecurity Kickoff Meeting with the Contracting Officer, system owner, system program manager, and Information System Security Manager (ISSM). The meeting will be located at a specific time and place to be determined by the Contracting Officer.

1.8 CYBERSECURITY DOCUMENTATION

1.8.1 Cybersecurity Interconnection Schedule

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-graphics-tables.)

1.8.2 Network Communication Report

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 requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide Network Communication Report as an editable Microsoft Excel file.

1.8.3 Control System Inventory Report

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-graphics-tables documenting all 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 requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide Control System Inventory Report as an editable Microsoft Excel file.

1.8.4 Software Recovery and Reconstitution Images

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.

1.8.5 Cybersecurity Riser Diagram

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 overlayed on a facility schematic.

1.8.6 Control System Cybersecurity Documentation

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

1.8.6.1 Software Applications

For all software applications running on computers provide:

a. Administrator documentation that describes secure configuration of the software.

b. Administrator documentation that describes secure installation of the software.

c. Administrator documentation that describes secure operation of the software.

d. Administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software.

e. Administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software.

f. User documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms.

g. User documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner.

h. User documentation that describes user responsibilities in maintaining the security of the software.

1.8.6.2 Default Requirements for Control System Devices

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.

b. Documentation that describes secure installation of the device.

c. Documentation that describes secure operation of the device.

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device.

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device.

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms.

g. Documentation that describes methods for user interaction which

enables individuals to use the device in a more secure manner.

h. Documentation that describes user responsibilities in maintaining the security of the device.

1.9 SOFTWARE UPDATE LICENSING

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.

1.10 CYBERSECURITY DURING CONSTRUCTION

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

1.10.1 Contractor Computer Equipment

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

1.10.1.1 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.

1.10.1.2 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.

1.10.1.3 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.

1.10.1.4 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-graphics-tables. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.10.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks must meet the following requirements:

1.10.2.1 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.

1.10.3 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.

1.10.4 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.

1.10.5 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.

1.10.6 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-graphics-tables. 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.

1.11 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

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.

Implement a warning banner on terminal interfaces that conforms to DoD warning banner guidelines. Configure each component of the product to operate using the principle of least privilege. This includes operating communications, and energy delivery system services.

Provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. Provide a system administration mechanism for changing user(s') role (e.g., group) associations.

Configure the product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side. Provide a method for protecting against unauthorized privilege escalation.

Document options for defining access and security permissions, user accounts, and applications with associated roles. Configure these options as specified.

Prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware and document if not feasible, provide mitigation recommendations.

Verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

3.1.1.1 Computers

All computers must FULLY support user accounts.

3.1.1.2 Default Requirements for Control System Devices

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

a. Devices with web interfaces must either FULLY support user accounts or have their web interface disabled.

b. Field devices with full local user interfaces allowing modification of data must FULLY support user accounts.

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

3.1.2 Account Management

Document all accounts (including but not limited to, generic or default)

that need to be active for proper operation of the product. Change default account settings to specific settings (e.g., length, complexity, history, and configurations) provided by government representative. Changed account information will not be published. All new account information will be provided by a protected mechanism. Remove or disable any accounts that are not needed for normal or maintenance operations of the control system. Accounts for emergency operations shall be placed in a highly secure configuration and documentation must be provided.

3.1.3 Unsuccessful Logon Attempts

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts.

3.1.3.1 Devices MINIMALLY Supporting Accounts

Devices which MINIMALLY support accounts must lock the user input after three unsuccessful logon attempts and must support unlocking of the user input when unlocked by an administrator.

3.1.3.2 Devices FULLY Supporting Accounts

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.

3.1.3.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

Contact local ISSM and System Owner/Program Manager for requirements for high availability interfaces that are exempt from unsuccessful logon attempts. Work with local ISSM and local CIO to complete the following:

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

3.1.4 System Use Notification

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.

3.1.4.1 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

3.1.5 Permitted Actions Without Identification or Authentication

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.

3.1.6 Wireless Access

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).

3.1.6.1 Wireless IP Communications

Do 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.

3.1.6.2 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.

3.1.6.3 Wireless Communication Request

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-graphics-tables.

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.

3.1.6.4 Wireless Communication Testing

As part of Performance Verification Testing (PVT), 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. 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

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

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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

f. Successful and unsuccessful accesses to objects

g. All program initiations

h. All direct access to the information system

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

j. 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 Default Requirements for Control System Devices

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

3.2.1.2.1 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

3.2.1.2.1.1 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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

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

g. All kernel module load, unload, and restart

3.2.1.2.1.2 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

3.2.1.2.2 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

a. For devices that have STIG/SRGs related to audit storage capacity 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 audit records in conformance with applicable STIG/SRGs.

3.2.2.1 Device Audit Record Upload Software

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 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.

Contact local ISSM and System Owner/Program Manager for device audit record upload software requirements. 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

Front end computers associated with auditing must, in the case of a failure in the auditing system, notify ISSM 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

3.2.4.1 Computers

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 Control System Devices

Time stamp requirements for Control Systems are as indicated in 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 system so that each device generating audit records maintains accurate time to within 1 second.

3.2.4.3 Default Requirements for Control System Devices

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

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 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

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

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 Default Requirements for Control System Devices

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.

3.5.2 Authenticator Management

3.5.2.1 Authentication Type

3.5.2.1.1 Default Requirements for Control System Devices

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.

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

c. Devices MINIMALLY supporting accounts must use either password-based authentication or 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 not lock accounts due to expired passwords.

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

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 not 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 not lock accounts due to expired passwords.

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

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

3.5.2.2.4 Passwords for Devices Minimally Supporting Accounts

Devices minimally supporting accounts must support passwords with a minimum length of four characters.

3.5.2.2.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with ISSM. 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 Password Summary Report in electronic format. Provide two hard copies of 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

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, comply with the requirements of those STIGS/SRGs.

3.5.4 Device Identification and Authentication

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 ISSM.

3.5.4.1 Default Requirements for Control System Devices

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 ISSM instead.

3.5.5 Cryptographic Module Authentication

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

3.6 EMERGENCY POWER

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

3.7 DURABILITY TO VULNERABILITY SCANNING

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 Assured Compliance Assessment Solution (ACAS) by responding with a valid credentialed scan. For control system devices other than computers:

3.7.1 Default Requirements for Control System Devices

Non-computer control system devices where Durability to Vulnerability Scanning requirements are not otherwise indicated in this Section are not required to respond to scans.

3.8 FIPS 201-2 REQUIREMENT

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list.

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-graphics-tables to request approval for each device.

3.10 SYSTEM AND COMMUNICATION PROTECTION

3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection

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

3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

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

3.12 FIELD QUALITY CONTROL

3.12.1 Tests

In addition to testing and testing support required by other Sections, provide a minimum of 80 hours of technical support for cybersecurity testing of control systems.

-- End of Section --

THIS PAGE INTENTIONALLY LEFT BLANK

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-002110	AC-2 (a)	The organization defines the information system account types that support the organizational missions/business functions.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions.	N/A
CCI-000213	AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Any device supporting accounts (either fully or partially) must limit access to the device according to specified limitations for each account. Install and configure any device having a Security Technical Implementation Guide (STIG) or Security Requirements Guide (SRG) in accordance with that STIG or SRG.	Impractical
CCI-000043	AC-7(A)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	APPLICABLE if system has capability
CCI-000044	AC-7(a)	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the	The information system shall be set to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval. Devices which Partially support accounts shall implement the requirements of a FULLY supported account when possible. If unsuccessful login attempts and accounts	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		organization-defined time period.	lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel. Document any device incapable of meeting the defined requirement and state actual implementation.	
CCI-001423	AC-7(a)	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occurs.	DOD policy requires the system to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval.	APPLICABLE if system has capability.
CCI-002236	AC-7(a)	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires for systems that once an account is locked, the account must stay locked until unlocked by an administrator. This may have safety implications in control system environment. Implement with caution.	APPLICABLE if system has capability.
CCI-002237	AC-7(a)	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful	DOD policy requires that once the indicated number of unsuccessful login attempts occurs, delay login prompts by **[5] seconds**. If the provided software cannot meet these requirements, document software capabilities to protest from subsequent unsuccessful login attempts and propose alternate protections. Do not implement alternate protection measures without explicit permission from the System Owner.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		attempts is exceeded.		
CCI-002238	AC-7(a)	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The information system shall be configured to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Devices which Partially support accounts shall implement the requirements of a Fully supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel.	APPLICABLE if system has capability.
CCI-000048	AC-8(a)	The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent	All devices (PC's, BPOCs, Network switches, etc…) with a user interface supporting the use of a password or PIN, and capable of displaying 50 or more alphanumeric characters shall be configured to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. The DOD Consent Banner can be found on the RMF Knowledge Service site at https://rmfks.osd.mil/rmf/Guidance/GoverningPolicy/Pages/ConsentBanner.aspx Devices connected to a network, with a user interface supporting use of a password or PIN, and **not capable** of displaying 50 or more alphanumeric characters must have a permanently affixed label displaying an approved banner from the policy listed above.	
CCI-002247	AC-8(a)	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-002243	AC-8(a)(1)	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002244	AC-8(a)(2)	The organization-defined information system use	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD	APPLICABLE if system has capability.

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		notification message or banner is to state that information system usage may be monitored, recorded, and subject to audit.	requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	
CCI-002245	AC-8(a)(3)	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002246	AC-8(a)(4)	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-000050	AC-8(a)(4)	The information system retains the notification message or	Configure the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on	APPLICABLE if system has capability.

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access.	to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-002248	AC-8(C)(1)	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-000061	AC-14(a)	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following: • Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by the System Owner.
CCI-000232	AC-14(b)	The organization documents and provides	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually	Impractical unless required by

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		supporting rationale in the security plan for the information system, user actions not requiring identification and authentication	automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following: • Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	the System Owner.
CCI-001438	AC-18(a)	The organization establishes usage restrictions for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001439	AC-18(a)	The organization establishes implementation guidance for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-002323	AC-18(a)	The organization establishes configuration/connection requirements for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001441	AC-18(b)	The organization authorizes wireless access to the information system prior to allowing such connections.	Required if System relies on RF connectivity.	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-000123	AU-2(a)	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	HW (workstations, servers, network switches/infrastructure, etc…) capable of auditing shall audit the following: • Successful and unsuccessful logon attempts • Privileged activities or other system level access • Starting and ending time for user access to the system • Concurrent logons from different workstations. • Successful and unsuccessful accesses to objects • All program initiators • All direct access to the information system • All account creations, modifications, disabling, and terminations • All kernel module load, unload, and restart	APPLICABLE if capability exists
CCI-001571	AU-2(a)	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	APPLICABLE only if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-000125	AU-2(c)	The organization provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.	The organization documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	N/A
CCI-001485	AU-2(d)	The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	N/A
CCI-000130	AU-3	The information system generates audit records containing information that establishes what type of event occurred.	The information system shall be configured to generate audit records containing information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (FPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000131	AU-3	The information system generates audit records containing	The information system shall be configured to generate audit records containing information that establishes when an event occurred. For information system components that have	APPLICABLE if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		information that establishes when an event occurred.	applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	
CCI-000132	AU-3	The information system generates audit records containing information that establishes where the event occurred.	The information system shall be configured to generate audit records containing information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000133	AU-3	The information system generates audit records containing information that establishes the source of the event.	The information system shall be configured to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000134	AU-3	The information system generates audit records containing information that	The information system shall be configured to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		establishes the outcome of the event.	being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	
CCI-001487	AU-3	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The information system shall be configured to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance that pertains to CCI 1487. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-001848	AU-4	The organization defines the audit record storage requirements	Devices that have STIG/SRGs must comply with the requirements of those STIG/SRGs. For BPOCs and field devices (not front end computers) capable of generating audit records, the front end server shall be configured to retrieve audit records from the devices. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-001849	AU-4	The organization allocates audit record storage capacity in accordance with organization-defined audit	The organization allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 001848. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. Provide a secure mechanism of	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		record storage requirements.	uploading these audit records to a front end PC for storage and review.	
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	If the front end server can be configured to automatically archive full logs or write audit logs to an audit server (from all connected audit capable devices), then this control shall be considered not-applicable (NA). Otherwise, if email services are available, configure the workstations and servers to alert at a minimum, the system administrator (SA) and or the designated Information System Security Officer/Manager in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. If email services are not available then the workstations and servers shall configure the system to provide an alert on the screen in the event of an audit processing failure.	APPLICABLE if capability exists
CCI-000140	AU-5(b)	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	In case of an audit failure, if possible, configure the system to continue to collect audit records by overwriting existing audit records starting with the oldest records first. Ideal configuration would be to configure the system to send audit records directly to an audit server, or automatically archive full logs and document as such with the ISSO. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	APPLICABLE if capability exists
CCI-001490	AU-5(b)	The organization defines actions to be taken by the information	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure as described in CCI-000139 and CCI-000140.	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).		
CCI-000159	AU-8(a)	The information system uses internal system clocks to generate time stamps for audit records.	Workstations and servers on the domain shall be configured to synchronize with domain controllers. If an NTP server is configured it should synchronize with a secure, authorized source. If not on a domain or NTP server, workstations, server or other components that generate audit records, the timing requirement inherent in the control system will be sufficient. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001889	AU-8(b)	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001890	AU-8(b)	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or	All devices which provide audit capabilities, configure them to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		Greenwich Mean Time (GMT).	inspected/assessed must comply with the STIG/SRG guidance.	
CCI-000169	AU-12(a)	The information system provides audit record generation capability for the auditable events defined in AU-2(a) at organization defined information system components.	CCI-000123 defines auditable events for an information system. Level 4 devices (workstations, servers, network switches, routers, etc.) shall implement to the extent possible the requirements in CCI-000123 and AU-2(a). Requirements that cannot be implemented must be documented and justification provided. Other devices (non level 4) that provide auditing capabilities shall implement the requirements in CCI-000123 where the capability exists and the ISSM deems relevant. Example, for components. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	APPLICABLE if capability exists
CCI-001459	AU-12(a)	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components. Devices which ARE NOT capable of generating an audit log are exempt. System documentation should define which components are capable and are not capable of generating audit logs.	APPLICABLE if capability exists
CCI-000171	AU-12(b)	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system	Configure all capable devices to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM. System administrator personnel will inherently have the rights associated with their accounts to select auditable events, however, organizational policy shall only authorize the ISSM or	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
			individuals appointed by the ISSM to select and make those necessary changes.	
CCI-001910	AU-12(b)	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	N/A
CCI-000172	AU-12(c)	The information system generates audit records for the events defined in AU-2(d) with the content defined in AU-3.	Audit record requirements are defined in CCI-000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487 above. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	APPLICABLE if capability exists
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.	Interconnections to other systems WILL NOT be implemented. Front end servers and workstations may reside on the local Network Enterprise Center's (NECs) network allowing a connection into the control system (CS) components.	N/A No Interconnects
CCI-002102	CA-9(a)	The organization defines the information system components or classes of components that that are authorized internal connections to the	Define and document the information system components or classes of components that that are authorized internal connections to the information system. (e.g. Network Controllers, switches, routers, etc…)	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		information system.		
CCI-002103	CA-9(b)	The organization documents, for each internal connection, the interface characteristics.	The organization documents, for each internal connection (network controllers, etc…) the communication protocols used and a general description of what information is communicated over the network. This can be accomplished through a network communication report.	APPLICABLE
CCI-002104	CA-9(b)	The organization documents, for each internal connection, the security requirements.	The organization documents, for each internal connection, the security requirements.	N/A
CCI-002105	CA-9(b)	The organization documents, for each internal connection, the nature of the information communicated.	See CCI-002103	APPLICABLE
CCI-000293	CM-2	The organization develops and documents a current baseline configuration of the information system.	Develop and document a current baseline configuration of the information system to include, drawings, software licenses, source code, hardware, etc…	APPLICABLE
CCI-000363	CM-6(a)	The organization defines security configuration checklists to be used to establish and document configuration settings for the	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). Document in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		information system technology products employed.	apply to their information system components. Field Devices (BPOCs, etc…) that do not have STIGs, SRGs, etc…obtain vendor configuration guides.	
CCI-000364	CM-6(a)	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security configuration checklists.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	N/A
CCI-000365	CM-6(a)	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-001588	CM-6(a)	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001755	CM-6(c)	The organization defines the information system components for which any deviation from the established configuration settings are to be identified, documented and approved.	DoD has defined the information system components as all configurable information system components.	N/A
CCI-000381	CM-7(a)	The organization configures the information system to provide only essential capabilities.	Disable all ports, protocols and services not specifically needed by any device or component within the Control system (server, workstations, field devices, BPOCS, switches, etc…) Remove all software not specifically needed for use in the control system.	APPLICABLE
CCI-000380	CM-7(b)	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.		APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-000382	CM-7(b)	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.		APPLICABLE
CCI-001761	CM-7(1)(b)	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed unnecessary and/or non-secure.	Define and document in the system security plan, the functions, ports, protocols and services within the control system that are to be disabled when deemed unnecessary.	APPLICABLE
CCI-001762	CM-7(1)(b)	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	Disable functions, ports, protocols, and services within the control system deemed to be unnecessary and/or nonsecure, nonsecure functions, ports, protocols, and services.	APPLICABLE
CCI-000389	CM-8(a)(1)	The organization develops and documents an inventory of information system	Provide a Control System inventory report covering all networked, including network infrastructure devices. Provide the following information (where applicable):	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		components that accurately reflects the current information system.	• If the device has (in other project documentation) a unique identifier • Description, make, mode, serial number, location • Software/firmware version Network information: protocol, network address	
CCI-000392	CM-8(a)(2)	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.	See CCI-000389	APPLICABLE
CCI-000398	CM-8(a)(4)	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	APPLICABLE
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known	The organization must develop a contingency plan (CP) addressing recovery and reconstitution of the control system to a known state after a disruption In essence, restoring the system to the appropriate operational state. The CP will be site specific and should be developed in conjunction with	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		state after a disruption.	stakeholders of the system. Copies of required software, backup data, hardware list and baseline configurations should be identified in the CP. NOTE-known state shall also include the accepted "as-built" documentation and include any custom programming and configuration for controllers or workstations.	
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan. See also CCI-000550	N/A
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization must identify the selected method in the contingency plan. See also CCI-000550	N/A
CCI-002855	CP-12	The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	Configure the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 002857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	APPLICABLE
CCI-002856	CP-12	The organization defines the conditions, that	When the following conditions are detected, the control system shall enter a safe mode of operation.	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	• Commercial Power Loss • Fire • Water	
CCI-002857	CP-12	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	**Commercial Power Failure:** Upon loss of commercial power, the control system will switch to Generator power and only Mission Critical Infrastructure (deemed by the organization) will received continued control system service. All other infrastructure/areas services will cease until commercial power is restored. **Fire:** The system shall be integrated with fire detectors. Upon detection of fire, the system will ensure dampers and air handlers are shut down to prevent the propagation of smoke, gasses and fire through the system. The system shall remain in a shutdown/closed state until manually restarted/rebooted by organization personnel. **Water:** Upon detection of water (sprinkler system), the servers shall perform a graceful shutdown in order to minimize component failure due to water.	APPLICABLE
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting	All components capable of user accounts will be configured to uniquely identify and authenticate users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		on behalf of organizational users).	being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.	Multifactor authentication shall be implemented for users that require privileged level accounts to servers and workstations residing on the network (not standalone or PRIVATE VLAN segregated systems). Multifactor authentication can be implemented with through common access card (CAC) authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000777	IA-3	The organization defines a list of specific and/or types of devices for which identification and authentication is	All network connected endpoint devices (including but not limited to: workstations, printers, servers) shall be identified and authenticated before establishing a connection to the information system. Any device incapable of being authenticated to the system shall be documented.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		required before establishing a connection to the information system.		
CCI-000778	IA-3	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to identify all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001958	IA-3	The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to authenticate all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000176	IA-5(b)	The organization manages information system authenticators by establishing initial authenticator content for authenticators	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		defined by the organization.		
CCI-001544	IA-5(c)	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	APPLICABLE if capability exists
CCI-001989	IA-5(e)	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	Document and implement procedures to change default authenticators (passwords, etc.) or apply authenticators to all capable components prior to system installation.	N/A
CCI-000182	IA-5(g)	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	Document and implement procedures for changing/refreshing authenticators in the following time periods: • Password: 60 days.	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-001610	IA-5(g)	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period of Password: 60 days. Biometrics: every 3 years.	N/A
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	APPLICABLE if capability exists
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	APPLICABLE if capability exists
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	APPLICABLE if capability exists
CCI-001611	IA-5(1)(a)	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	APPLICABLE if capability exists
CCI-001612	IA-5(1)(a)	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	APPLICABLE if capability exists
CCI-001613	IA-5(1)(a)	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	APPLICABLE if capability exists
CCI-001614	IA-5(1)(a)	The organization defines the minimum number of numeric characters for	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		password complexity enforcement.		
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	APPLICABLE if capability exists
CCI-000195	IA-5(1)(b)	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195.	APPLICABLE if capability exists
CCI-001615	IA-5(1)(b)	The organization defines the minimum number of characters that are changed when new passwords are created.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number of characters as 50% of the minimum password length.	APPLICABLE if capability exists
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-	Configure the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with	APPLICABLE if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		protected passwords.	the STIG/SRG guidance that pertains to CCI 196.	
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	APPLICABLE if capability exists
CCI-000198	IA-5(1)(d)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	APPLICABLE if capability exists
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.	Configure the information system to enforce maximum password lifetime restrictions. For capable components, set maximum password age to 60 days or less (excluding “0”). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	APPLICABLE if capability exists
CCI-001616	IA-5(1)(d)	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	APPLICABLE if capability exists
CCI-001617	IA-5(1)(d)	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days and not being “0”.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. All other components utilizing passwords, the password reuse should be set to 24. If the components are incapable of being set to 24 then implement the maximum possible.	APPLICABLE if capability exists
CCI-001618	IA-5(1)(e)	The organization defines the number of generations for which password reuse is prohibited.	Per the STIGs for Windows based systems, the DOD has defined this to be set at a minimum of 24.	APPLICABLE if capability exists
CCI-002041	IA-5(1)(f)	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	APPLICABLE if capability exists
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.	APPLICABLE if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	APPLICABLE if capability exists
CCI-000206	IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Configure the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206. Applicable to networked devices. Does not apply to devices that have NO feedback during password/PIN entry. Devices shall never show authentication information, including passwords, on a	APPLICABLE if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
			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 CCI-000206, comply with the requirements of those STIGS/SRGs.	
CCI-000803	IA-7	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	For devices that have STIG/SRGs related to CCI-000803, comply with the requirements of those STIG/SRGs.	APPLICABLE if capability exists
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	Develop a diagram and explain within the system security plan (SSP) the authorization boundary for the complete control system including all networked devices and controller hardware.	N/A
CCI-003053	PL-2(a)(4)	The organization's security plan for the information system provides the security categorization of the information	The NIST SP800-60, Vol 2, Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This mission also includes measures taken to ensure the	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		system including supporting rationale.	provision of energy in the event of an emergency. The recommended Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)} Therefore the system shall be categorized as a LOW-LOW-LOW system.	
CCI-000207	PM-5	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	APPLICABLE
CCI-000236	PM-11(b)	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	No additional protection needs are needed aside from what the network provider supplies. Control system components (not including servers and workstations) would generally be on a private PRIVATE VLAN without public access thereby further segregating the components from the cyber domain.	N/A
CCI-001048	RA-3(a)	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the	The conducting of a Risk Assessment will most likely be site specific. The owning organization will need to conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction. The Designer can assist in identifying risk to the owing organization in order to complete the risk assessment.	N/A

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		unauthorized access, use, disclosure, disruption, modification, or destruction.		
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	Servers, workstations and network infrastructure on the network will be scanned for vulnerabilities by the network provider. All other IP devices associated with the system (whether on the public or private side of the network) 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. The owning organization will need a service level agreement (SLA) with the network provider to perform scanning of IP devices on a private PRIVATE VLAN or dark fiber network, or have in-house personnel assigned to perform the vulnerability scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new	Conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	Impractical

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		vulnerabilities potentially affecting the system/applications are identified and reported.		
CCI-001641	RA-5(a)	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001643	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	Servers, workstations and network infrastructure on the network will follow the process for random scans as defined by the Network Provider. The organization will conduct random vulnerability scans every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) for all other control system components on a PRIVATE VLAN or the portion not scannable by the Network Provider.. The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability	The organization whether through the Network Provider or otherwise, employs the DoD Enterprise scanning tool.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.		
CCI-001058	RA-5(c)	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	N/A
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-003116	SA-4(10)	The organization employs only information technology products on the	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		FIPS PUB 201-2-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.		
CCI-003124	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	APPLICABLE
CCI-003125	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system,	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		component, or service.		
CCI-003126	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	APPLICABLE
CCI-003127	SA-5(a)(2)	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003128	SA-5(a)(3)	The organization obtains administrator documentation for the information system, system component, or	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities of the system, component, or service.	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		information system services that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.	To the extent possible this should also apply to Control System software applications.	
CCI-003129	SA-5(b)(1)	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003130	SA-5(b)(2)	The organization obtains user documentation for the information system, system component or information system service that describes methods for user interaction which	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner. To the extent possible this should also apply to Control System software applications.	APPLICABLE

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		enables individuals to use the system, component, or service in a more secure manner.		
CCI-003131	SA-5(b)(3)	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-001093	SC-5	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	Definition of the types of denial of service attacks will be defined at the Network Provider level.	APPLICABLE
CCI-002385	SC-5	The information system protects against or limits the effects of organization-defined types of	For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		denial of service attacks by employing organization-defined security safeguards.	To the greatest extent practical, the hardware performs control logic without reliance on the network.	
CCI-002386	SC-5	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	Definition of the security safeguard to be employed to protect the information system will be defined at the Network Provider level for all devices on the Network Provider. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE
CCI-001097	SC-7(a)	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	Monitoring and the controlling of communications at the external boundary of the system will be the responsibility of the Network Provider. The control system shall not be publicly accessible.	N/A
CCI-001133	SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity	The organization being inspected/assessed configures the information system to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-001134	SC-10	The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.	DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	Impractical
CCI-002530	SC-39	The information system maintains a separate execution domain for each executing process.	To the greatest extent practical, the hardware performs control sequences without reliance on the network.	APPLICABLE
CCI-002544; 002545;002546	SC-41	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed	Physically disable or remove connection ports or input/output devices.	APPLICABLE
CCI-001241	SI-3(c)(1)	The organization configures	The Network Provider will implement/configure security scanning for	Impractical

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 01 Attachment A
UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS)
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
		malicious code protection mechanisms to perform periodic scans of the information system on an organization-defined frequency.	servers and workstations on their network. Servers and workstations installed under this project that are on a PRIVATE VLAN, the owning organization must install and configure malware protection software. Configure software to perform a full system scan every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	
CCI-002623	SI-3(c)(1)	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	Impractical
CCI-001253	SI-4(a)(1)	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	Impractical
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	Network monitoring is conducted by the network provider for control system components on non-private (VLAN) side. Network monitoring cannot be implemented for field devices/components on the private network (VLAN).	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 01 Attachment A UTILITY CONTROL SYSTEMS INCLUDING ELECTRICAL TRANSMISSION AND DISTRIBUTION AND UNINTERRUPTIBLE POWER SUPPLY (UPS) LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed	The organization being inspected/assessed defines and documents the software on which integrity checks will be performed. DoD has determined the software is not appropriate to define at the Enterprise level.	Impractical
CCI-002773	SI-17	The organization defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur.	In many cases standard control system design of sequences and alarm requirements address these CCIs without any additional design requirements	APPLICABLE
CCI-002774	SI-17	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	Failure conditions likely to be experienced by control system components are component failure and communications failure to components.	APPLICABLE
CCI-002775	SI-17	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	Configure the information system to implement fail-safe procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

SECTION 25 05 11.26 02

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS

PART 1 GENERAL

This section refers to Security Requirements Guide (SRGs) and Security Technical Implementation Guide (STIGs). STIGs and SRGs are available online at the Information Assurance Support Environment (IASE) website at http://iase.disa.mil/stigs/Pages/index.aspx. Not all control system components have applicable STIGs or SRGs.

1.1 CONTROL SYSTEM APPLICABILITY

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: Building Control Systems including Electrical and Lighting Controls.

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

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.

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

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

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are for Contractor Quality Control approval. Submittals with an "S" are for inclusion in the Sustainability eNotebook, in conformance with Section 01 33 29 SUSTAINABILITY REPORTING. 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

Qualifications; 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 Cybersecurity Representative

Provide a Cybersecurity Representative as the key person to implement and manage the cybersecurity related control systems of the project. This individual must have a minimum of 2 years of cybersecurity control systems experience, including two projects of similar size and complexity. Submit the Cybersecurity Representative's certification of qualifications no later than 60 calendar days after Notice to Proceed. Submit one hard copy and an electronic copy.

1.7.1.1 Duties

The Cybersecurity Representative must lead and oversee the cybersecurity control systems work specified herein and be the primary point of contact for the Government regarding the cybersecurity work.

1.7.1.2 Qualifications

The individual must have a minimum of 2 years with Risk Management Framework implementation experience and experience with Facility Related Control System cybersecurity implementation such as a control system related training or certification.

1.7.2 Cybersecurity Kickoff Meeting

Within 60 calendar days after contract award, the Cybersecurity Representative must schedule a Cybersecurity Kickoff Meeting with the Contracting Officer, system owner, system program manager, and Information System Security Manager (ISSM). The meeting will be located at a specific time and place to be determined by the Contracting Officer.

1.8 CYBERSECURITY DOCUMENTATION

1.8.1 Cybersecurity Interconnection Schedule

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-graphics-tables.)

1.8.2 Network Communication Report

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 requirements of Section 01 33 00 SUBMITTAL PROCEDURES provide Network Communication Report as an editable Microsoft Excel file.

1.8.3 Control System Inventory Report

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-graphics-tables documenting all 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 requirements of Section 01 33 00 SUBMITTAL PROCEDURES, provide Control System Inventory Report as an editable Microsoft Excel file.

1.8.4 Software Recovery and Reconstitution Images

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.

1.8.5 Cybersecurity Riser Diagram

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 overlayed on a facility schematic.

1.8.6 Control System Cybersecurity Documentation

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

1.8.6.1 Software Applications

For all software applications running on computers provide:

a. Administrator documentation that describes secure configuration of the software.

b. Administrator documentation that describes secure installation of the software.

c. Administrator documentation that describes secure operation of the software.

d. Administrator documentation that describes effective use and maintenance of security functions or mechanisms for the software.

e. Administrator documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the software.

f. User documentation that describes user-accessible security functions or mechanisms in the software and how to effectively use those security functions or mechanisms.

g. User documentation that describes methods for user interaction which enables individuals to use the software in a more secure manner.

h. User documentation that describes user responsibilities in maintaining the security of the software.

1.8.6.2 Default Requirements for Control System Devices

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.

b. Documentation that describes secure installation of the device.

c. Documentation that describes secure operation of the device.

d. Documentation that describes effective use and maintenance of security functions or mechanisms for the device.

e. Documentation that describes known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions for the device.

f. Documentation that describes user-accessible security functions or mechanisms in the device and how to effectively use those security functions or mechanisms.

g. Documentation that describes methods for user interaction which

enables individuals to use the device in a more secure manner.

h. Documentation that describes user responsibilities in maintaining the security of the device.

1.9 SOFTWARE UPDATE LICENSING

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.

1.10 CYBERSECURITY DURING CONSTRUCTION

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

1.10.1 Contractor Computer Equipment

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

1.10.1.1 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.

1.10.1.2 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.

1.10.1.3 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.

1.10.1.4 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-graphics-tables. Each Statement must be signed by a cybersecurity representative for the relevant company.

1.10.2 Temporary IP Networks

Temporary contractor-installed IP networks may be used during construction. When used, temporary contractor-installed IP networks must meet the following requirements:

1.10.2.1 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.

1.10.3 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

1.10.4 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.

1.10.5 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.

1.10.6 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-graphics-tables. 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.

1.11 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

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.

Implement a warning banner on terminal interfaces that conforms to DoD warning banner guidelines. Configure each component of the product to operate using the principle of least privilege. This includes operating communications, and energy delivery system services.

Provide user accounts with configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. Provide a system administration mechanism for changing user(s') role (e.g., group) associations.

Configure the product such that when a session or interprocess communication is initiated from a less privileged application, access shall be limited and enforced at the more critical side. Provide a method for protecting against unauthorized privilege escalation.

Document options for defining access and security permissions, user accounts, and applications with associated roles. Configure these options as specified.

Prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware and document if not feasible, provide mitigation recommendations.

Verify and provide documentation for the procured product, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

3.1.1.1 Computers

All computers must FULLY support user accounts.

3.1.1.2 Default Requirements for Control System Devices

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

a. Devices with web interfaces must either FULLY support user accounts or have their web interface disabled.

b. Field devices with full local user interfaces allowing modification of data must FULLY support user accounts.

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

3.1.2 Account Management

Document all accounts (including but not limited to, generic or default)

that need to be active for proper operation of the product. Change default account settings to specific settings (e.g., length, complexity, history, and configurations) provided by government representative. Changed account information will not be published. All new account information will be provided by a protected mechanism. Remove or disable any accounts that are not needed for normal or maintenance operations of the control system. Accounts for emergency operations shall be placed in a highly secure configuration and documentation must be provided.

3.1.3 Unsuccessful Logon Attempts

Except for high availability user interfaces indicated as exempt, devices must meet the indicated requirements for handling unsuccessful logon attempts.

3.1.3.1 Devices MINIMALLY Supporting Accounts

Devices which MINIMALLY support accounts must lock the user input after three unsuccessful logon attempts and must support unlocking of the user input when unlocked by an administrator.

3.1.3.2 Devices FULLY Supporting Accounts

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.

3.1.3.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

Contact local ISSM and System Owner/Program Manager for requirements for high availability interfaces that are exempt from unsuccessful logon attempts. Work with local ISSM and local CIO to complete the following:

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

3.1.4 System Use Notification

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.

3.1.4.1 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

3.1.5 Permitted Actions Without Identification or Authentication

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.

3.1.6 Wireless Access

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).

3.1.6.1 Wireless IP Communications

Do 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.

3.1.6.2 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.

3.1.6.3 Wireless Communication Request

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-graphics-tables.

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.

3.1.6.4 Wireless Communication Testing

As part of Performance Verification Testing (PVT), 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 wireless test boundary in vicinity of wireless device, and record whether a network connection can be established at each point. Wireless test boundary is the building exterior walls. If wireless testing is required, provide a Wireless Communication Test Report documenting testing points and results at each point for each wireless device.

3.2 CYBERSECURITY AUDITING

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

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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

f. Successful and unsuccessful accesses to objects

g. All program initiations

h. All direct access to the information system

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

j. 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 Default Requirements for Control System Devices

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

3.2.1.2.1 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.

3.2.1.2.1.1 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)

b. Successful and unsuccessful logon attempts

c. Privileged activities or other system level access

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

e. Concurrent logons from different workstations

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

g. All kernel module load, unload, and restart

3.2.1.2.1.2 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

3.2.1.2.2 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

a. For devices that have STIG/SRGs related to audit storage capacity 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 audit records in conformance with applicable STIG/SRGs.

3.2.2.1 Device Audit Record Upload Software

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 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.

Contact local ISSM and System Owner/Program Manager for device audit record upload software requirements. 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

Front end computers associated with auditing must, in the case of a failure in the auditing system, notify ISSM 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

3.2.4.1 Computers

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 Control System Devices

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 system so that each device generating audit records maintains accurate time to within 1 second.

3.2.4.3 Default Requirements for Control System Devices

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

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 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

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

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 Default Requirements for Control System Devices

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.

3.5.2 Authenticator Management

3.5.2.1 Authentication Type

3.5.2.1.1 Default Requirements for Control System Devices

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.

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

c. Devices MINIMALLY supporting accounts must use either password-based authentication or 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 not lock accounts due to expired passwords.

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

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 not 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 not lock accounts due to

expired passwords.

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

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

3.5.2.2.4 Passwords for Devices Minimally Supporting Accounts

Devices minimally supporting accounts must support passwords with a minimum length of four characters.

3.5.2.2.5 Password Configuration and Reporting

For all devices with a password, change the password from the default password. Coordinate selection of passwords with ISSM. 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 Password Summary Report in electronic format. Provide two hard copies of 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

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, comply with the requirements of those STIGS/SRGs.

3.5.4 Device Identification and Authentication

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 ISSM.

3.5.4.1 Default Requirements for Control System Devices

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 ISSM instead.

3.5.5 Cryptographic Module Authentication

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

3.6 EMERGENCY POWER

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

3.7 DURABILITY TO VULNERABILITY SCANNING

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 Assured Compliance Assessment Solution (ACAS) by responding with a valid credentialed scan. For control system devices other than computers:

3.7.1 Default Requirements for Control System Devices

Non-computer control system devices where Durability to Vulnerability Scanning requirements are not otherwise indicated in this Section are not required to respond to scans.

3.8 FIPS 201-2 REQUIREMENT

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list.

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-graphics-tables to request approval for each device.

3.10 SYSTEM AND COMMUNICATION PROTECTION

3.10.1 Denial of Service Protection, Process Isolation and Boundary Protection

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

3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

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

3.12 FIELD QUALITY CONTROL

3.12.1 Tests

In addition to testing and testing support required by other Sections, provide a minimum of 80 hours of technical support for cybersecurity testing of control systems.

-- End of Section --

THIS PAGE INTENTIONALLY LEFT BLANK

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002110	AC-2 (a)	The organization defines the information system account types that support the organizational missions/business functions.	The organization conducting the inspection/assessment obtains and examines the documented information system account types to ensure the organization being inspected/assessed defines the information system account types that support the organizational missions/business functions.	N/A
CCI-000213	AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Any device supporting accounts (either fully or partially) must limit access to the device according to specified limitations for each account. Install and configure any device having a Security Technical Implementation Guide (STIG) or Security Requirements Guide (SRG) in accordance with that STIG or SRG.	Impractical
CCI-000043	AC-7(A)	The organization defines the maximum number of consecutive invalid logon attempts to the information system by a user during an organization-defined time period.	DoD has defined the maximum number as three.	APPLICABLE if system has capability
CCI-000044	AC-7(a)	The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-	The information system shall be set to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval. Devices which Partially support accounts shall implement the requirements of a FULLY supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined time period.	physical access to the device should limited to only authorized personnel. Document any device incapable of meeting the defined requirement and state actual implementation.	
CCI-001423	AC-7(a)	The organization defines the time period in which the organization-defined maximum number of consecutive invalid logon attempts occurs.	DOD policy requires the system to Lock the user account when **[3]** unsuccessful login attempts occur within a **[60 minute]** interval.	APPLICABLE if system has capability.
CCI-002236	AC-7(a)	The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires for systems that once an account is locked, the account must stay locked until unlocked by an administrator. This may have safety implications in control system environment. Implement with caution.	APPLICABLE if system has capability.
CCI-002237	AC-7(a)	The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.	DOD policy requires that once the indicated number of unsuccessful login attempts occurs, delay login prompts by **[5] seconds**. If the provided software cannot meet these requirements, document software capabilities to protest from subsequent unsuccessful login attempts and propose alternate protections. Do not implement alternate protection measures without explicit permission from the System Owner.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002238	AC-7(a)	The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.	The information system shall be configured to automatically lock the account or node until the locked account is released by an administrator and delays the next login prompt for a minimum of 5 seconds when the maximum number of unsuccessful attempts is exceeded. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Devices which Partially support accounts shall implement the requirements of a Fully supported account when possible. If unsuccessful login attempts and accounts lockouts are not supported by the device, then physical access to the device should limited to only authorized personnel.	APPLICABLE if system has capability.
CCI-000048	AC-8(a)	The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives,	All devices (PC's, BPOCs, Network switches, etc…) with a user interface supporting the use of a password or PIN, and capable of displaying 50 or more alphanumeric characters shall be configured to display the DoD Information Systems – Standard Consent Banner and User Agreement before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. The DOD Consent Banner can be found on the RMF Knowledge Service site at	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		policies, regulations, standards, and guidance.	https://rmfks.osd.mil/rmf/Guidance/GoverningPolicy/Pages/ConsentBanner.aspx Devices connected to a network, with a user interface supporting use of a password or PIN, and **not capable** of displaying 50 or more alphanumeric characters must have a permanently affixed label displaying an approved banner from the policy listed above.	
CCI-002247	AC-8(a)	The organization defines the use notification message or banner the information system displays to users before granting access to the system.	DoD has defined the use notification message or banner as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-002243	AC-8(a)(1)	The organization-defined information system use notification message or banner is to state that users are accessing a U.S. Government information system.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002244	AC-8(a)(2)	The organization-defined information system use notification message or banner is to state that information system usage may	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		be monitored, recorded, and subject to audit.	DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	
CCI-002245	AC-8(a)(3)	The organization-defined information system use notification message or banner is to state that unauthorized use of the information system is prohibited and subject to criminal and civil penalties.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-002246	AC-8(a)(4)	The organization-defined information system use notification message or banner is to state that use of the information system indicates consent to monitoring and recording.	DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013 meets the DoD requirements the information system use notification message or banner. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policy, DTM 08-060.	APPLICABLE if system has capability.
CCI-000050	AC-8(a)(4)	The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit	Configure the information system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if system has capability.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		actions to log on to or further access.		
CCI-002248	AC-8(C)(1)	The organization defines the conditions of use which are to be displayed to users of the information system before granting further access.	DoD has defined the conditions as the content of DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," March 2013.	APPLICABLE if system has capability.
CCI-000061	AC-14(a)	The organization identifies and defines organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions.	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following: • Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner	Impractical unless required by the System Owner.
CCI-000232	AC-14(b)	The organization documents and provides supporting rationale in the security plan for the information system, user actions not	Workstations, Servers, Network Switches, etc., shall not allow any actions without identification or authentication. This is usually automatically met by authenticating (logging in) to a system. The control system must use identification and authentication except for the following:	Impractical unless required by the System Owner.

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		requiring identification and authentication	• Read only access via a user interface from other than a PC and via other than a web interface. • Interactions via devices other than user interfaces. Devices that do not support authentication should have physical security implemented by lockable enclosures, tamper switches, room access control, people trap, or paper access logs. Implementing this control has potential safety issues and should only be implemented if required by the System Owner.	
CCI-001438	AC-18(a)	The organization establishes usage restrictions for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001439	AC-18(a)	The organization establishes implementation guidance for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-002323	AC-18(a)	The organization establishes configuration/connection requirements for wireless access.	Required if System relies on RF connectivity.	APPLICABLE
CCI-001441	AC-18(b)	The organization authorizes wireless access to the information system prior to allowing such connections.	Required if System relies on RF connectivity.	APPLICABLE
CCI-000123	AU-2(a)	The organization determines the information system must be capable of	HW (workstations, servers, network switches/infrastructure, etc…) capable of auditing shall audit the following: • Successful and unsuccessful logon attempts	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		auditing an organization-defined list of auditable events.	• Privileged activities or other system level access • Starting and ending time for user access to the system • Concurrent logons from different workstations. • Successful and unsuccessful accesses to objects • All program initiators • All direct access to the information system • All account creations, modifications, disabling, and terminations • All kernel module load, unload, and restart	
CCI-001571	AU-2(a)	The organization defines the information system auditable events.	DoD has defined the information system auditable events as successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels). Successful and unsuccessful logon attempts, Privileged activities or other system level access, Starting and ending time for user access to the system, Concurrent logons from different workstations, Successful and unsuccessful accesses to objects, All program initiations, All direct access to the information system. All account creations, modifications, disabling, and terminations. All kernel module load, unload, and restart.	APPLICABLE only if capability exists
CCI-000125	AU-2(c)	The organization provides a rationale for why the list of auditable events is deemed to be adequate to	The organization documents in the audit and accountability policy the list of auditable system events, the organization provides clearly stated rationale for the selection of each system event. The rationale will support any after-action investigations of security event.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		support after-the-fact investigations of security incidents.		
CCI-001485	AU-2(d)	The organization defines the events which are to be audited on the information system on an organization-defined frequency of (or situation requiring) auditing for each identified event.	The organization being inspected/assessed defines and documents events which are to be audited on the information system. Events should be selected from the events the information system is capable of auditing as defined in AU-2 (a) and should be based on ongoing risk assessments of current threat information and environment. DoD has determined that the events are not appropriate to define at the Enterprise level.	N/A
CCI-000130	AU-3	The information system generates audit records containing information that establishes what type of event occurred.	The information system shall be configured to generate audit records containing information that establishes what type of event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (FPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000131	AU-3	The information system generates audit records containing information that establishes when an event occurred.	The information system shall be configured to generate audit records containing information that establishes when an event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000132	AU-3	The information system generates audit records containing information that establishes where the event occurred.	The information system shall be configured to generate audit records containing information that establishes where the event occurred. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 132. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000133	AU-3	The information system generates audit records containing information that establishes the source of the event.	The information system shall be configured to generate audit records containing information that establishes the source of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-000134	AU-3	The information system generates audit records containing information that establishes the outcome of the event.	The information system shall be configured to generate audit records containing information that establishes the outcome of the event. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists

CRH Simulator Facility ADAL
Designer Control Correlation Identifiers
25 05 11.26 02 Attachment A
BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS
LOW-LOW-LOW

CCI Number	800-53/82 Control Text Indicator	CCI Definition	Designer Implementation	Classification
CCI-001487	AU-3	The information system generates audit records containing information that establishes the identity of any individuals or subjects associated with the event.	The information system shall be configured to generate audit records containing information that establishes the identity of any individuals or subjects associated with the event. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance that pertains to CCI 1487. Other IP devices (BPOCs, other field devices) may not be able to generate audit records. Document if these components are incapable of implementing the requirements set forth in policy.	APPLICABLE if capability exists
CCI-001848	AU-4	The organization defines the audit record storage requirements	Devices that have STIG/SRGs must comply with the requirements of those STIG/SRGs. For BPOCs and field devices (not front end computers) capable of generating audit records, the front end server shall be configured to retrieve audit records from the devices. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-001849	AU-4	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	The organization allocates, and configures the information system to allocate audit record storage capacity as defined in AU-4, CCI 001848. For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. Provide a secure mechanism of uploading these audit records to a front end PC for storage and review.	N/A
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	If the front end server can be configured to automatically archive full logs or write audit logs to an audit server (from all connected audit capable devices), then this control shall be considered not-applicable (NA). Otherwise, if email services are available, configure the workstations and servers to alert at a minimum, the system administrator (SA) and	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			or the designated Information System Security Officer/Manager in the event of an audit processing failure. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 139. If email services are not available then the workstations and servers shall configure the system to provide an alert on the screen in the event of an audit processing failure.	
CCI-000140	AU-5(b)	The information system takes organization defined actions upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	In case of an audit failure, if possible, configure the system to continue to collect audit records by overwriting existing audit records starting with the oldest records first. Ideal configuration would be to configure the system to send audit records directly to an audit server, or automatically archive full logs and document as such with the ISSO. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	APPLICABLE if capability exists
CCI-001490	AU-5(b)	The organization defines actions to be taken by the information system upon audit failure (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).	The organization being inspected/assessed will define and document actions to be taken by the information system upon audit failure as described in CCI-000139 and CCI-000140.	N/A
CCI-000159	AU-8(a)	The information system uses internal system clocks to generate	Workstations and servers on the domain shall be configured to synchronize with domain controllers. If an NTP server is configured it should synchronize with a secure, authorized	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		time stamps for audit records.	source. If not on a domain or NTP server, workstations, server or other components that generate audit records, the timing requirement inherent in the control system will be sufficient. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	
CCI-001889	AU-8(b)	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	DoD has defined the granularity of time measurement as one second. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001890	AU-8(b)	The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	All devices which provide audit capabilities, configure them to generate time stamps for audit records that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000169	AU-12(a)	The information system provides audit record generation capability for the auditable events defined in AU-2(a) at organization defined information system components.	CCI-000123 defines auditable events for an information system. Level 4 devices (workstations, servers, network switches, routers, etc.) shall implement to the extent possible the requirements in CCI-000123 and AU-2(a). Requirements that cannot be implemented must be documented and justification provided. Other devices (non level 4) that provide auditing capabilities shall implement the requirements in CCI-000123 where the capability exists and the ISSM deems relevant. Example, for components.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance	
CCI-001459	AU-12(a)	The organization defines information system components that provide audit record generation capability.	DoD has defined the information system components as all information system and network components. Devices which ARE NOT capable of generating an audit log are exempt. System documentation should define which components are capable and are not capable of generating audit logs.	APPLICABLE if capability exists
CCI-000171	AU-12(b)	The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system	Configure all capable devices to ensure that only the ISSM or individuals appointed by the ISSM select which auditable events are to be audited by specific components of the information system. DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM. System administrator personnel will inherently have the rights associated with their accounts to select auditable events, however, organizational policy shall only authorize the ISSM or individuals appointed by the ISSM to select and make those necessary changes.	N/A
CCI-001910	AU-12(b)	The organization defines the personnel or roles allowed select which auditable events are to be audited by specific components of the information system.	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM.	N/A
CCI-000172	AU-12(c)	The information system generates audit records for	Audit record requirements are defined in CCI-000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487 above. For	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		the events defined in AU-2(d) with the content defined in AU-3.	information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 172.	
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.	Interconnections to other systems WILL NOT be implemented. Front end servers and workstations may reside on the local Network Enterprise Center's (NECs) network allowing a connection into the control system (CS) components.	N/A No Interconnects
CCI-002102	CA-9(a)	The organization defines the information system components or classes of components that that are authorized internal connections to the information system.	Define and document the information system components or classes of components that that are authorized internal connections to the information system. (e.g. Network Controllers, switches, routers, etc…)	APPLICABLE
CCI-002103	CA-9(b)	The organization documents, for each internal connection, the interface characteristics.	The organization documents, for each internal connection (network controllers, etc…) the communication protocols used and a general description of what information is communicated over the network. This can be accomplished through a network communication report.	APPLICABLE
CCI-002104	CA-9(b)	The organization documents, for each internal connection, the security requirements.	The organization documents, for each internal connection, the security requirements.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-002105	CA-9(b)	The organization documents, for each internal connection, the nature of the information communicated.	See CCI-002103	APPLICABLE
CCI-000293	CM-2	The organization develops and documents a current baseline configuration of the information system.	Develop and document a current baseline configuration of the information system to include, drawings, software licenses, source code, hardware, etc…	APPLICABLE
CCI-000363	CM-6(a)	The organization defines security configuration checklists to be used to establish and document configuration settings for the information system technology products employed.	DoD has defined the security configuration checklists as DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.). Document in the security plan, the configuration guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) which apply to their information system components. Field Devices (BPOCs, etc…) that do not have STIGs, SRGs, etc…obtain vendor configuration guides.	N/A
CCI-000364	CM-6(a)	The organization establishes configuration settings for information technology products employed within the information system using organization-defined security	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for establishing configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		configuration checklists.		
CCI-000365	CM-6(a)	The organization documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for documenting configuration settings. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001588	CM-6(a)	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.) meet the DoD requirement for ensuring security configuration checklists reflect the most restrictive mode consistent with operational requirements. DoD Components are automatically compliant with this control because they are covered by the DoD level security configuration or implementation guidance (e.g. STIGs, SRGs, NSA configuration guides, CTOs, DTMs etc.).	APPLICABLE
CCI-001755	CM-6(c)	The organization defines the information system components for which any	DoD has defined the information system components as all configurable information system components.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		deviation from the established configuration settings are to be identified, documented and approved.		
CCI-000381	CM-7(a)	The organization configures the information system to provide only essential capabilities.	Disable all ports, protocols and services not specifically needed by any device or component within the Control system (server, workstations, field devices, BPOCS, switches, etc…) Remove all software not specifically needed for use in the control system.	APPLICABLE
CCI-000380	CM-7(b)	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.		APPLICABLE
CCI-000382	CM-7(b)	The organization configures the information system to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services.		APPLICABLE
CCI-001761	CM-7(1)(b)	The organization defines the functions, ports, protocols and services within the information system that are to be disabled when deemed	Define and document in the system security plan, the functions, ports, protocols and services within the control system that are to be disabled when deemed unnecessary.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		unnecessary and/or non-secure.		
CCI-001762	CM-7(1)(b)	The organization disables organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.	Disable functions, ports, protocols, and services within the control system deemed to be unnecessary and/or nonsecure, nonsecure functions, ports, protocols, and services.	APPLICABLE
CCI-000389	CM-8(a)(1)	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	Provide a Control System inventory report covering all networked, including network infrastructure devices. Provide the following information (where applicable): • If the device has (in other project documentation) a unique identifier • Description, make, mode, serial number, location • Software/firmware version Network information: protocol, network address	APPLICABLE
CCI-000392	CM-8(a)(2)	The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the	See CCI-000389	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information system.		
CCI-000398	CM-8(a)(4)	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD has defined the information as hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name.	APPLICABLE
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	The organization must develop a contingency plan (CP) addressing recovery and reconstitution of the control system to a known state after a disruption In essence, restoring the system to the appropriate operational state. The CP will be site specific and should be developed in conjunction with stakeholders of the system. Copies of required software, backup data, hardware list and baseline configurations should be identified in the CP. NOTE-known state shall also include the accepted “as-built” documentation and include any custom programming and configuration for controllers or workstations.	N/A
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a compromise. The organization must identify the selected method in the contingency plan. See also CCI-000550	N/A
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information	The organization shall provide automated mechanisms or manual procedures, or a combination of the two, for the recovery and reconstitution of its information system to a known state after a failure. The organization	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		system to a known state after a failure.	must identify the selected method in the contingency plan. See also CCI-000550	
CCI-002855	CP-12	The information system, when organization-defined conditions are detected, enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	Configure the information system to enter a safe mode of operation with restrictions of safe mode of operation defined in CP-12, CCI 002857 when conditions defined in CP-12, CCI 2856 are detected. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2855.	APPLICABLE
CCI-002856	CP-12	The organization defines the conditions, that when detected, the information system enters a safe mode of operation with organization-defined restrictions of safe mode of operation.	When the following conditions are detected, the control system shall enter a safe mode of operation. • Commercial Power Loss • Fire • Water	APPLICABLE
CCI-002857	CP-12	The organization defines the restrictions of safe mode of operation that the information system will enter when organization-defined conditions are detected.	**Commercial Power Failure:** Upon loss of commercial power, the control system will switch to Generator power and only Mission Critical Infrastructure (deemed by the organization) will received continued control system service. All other infrastructure/areas services will cease until commercial power is restored. **Fire:** The system shall be integrated with fire detectors. Upon detection of fire, the system will ensure dampers and air handlers are shut	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			down to prevent the propagation of smoke, gasses and fire through the system. The system shall remain in a shutdown/closed state until manually restarted/rebooted by organization personnel. **Water:** Upon detection of water (sprinkler system), the servers shall perform a graceful shutdown in order to minimize component failure due to water.	
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	All components capable of user accounts will be configured to uniquely identify and authenticate users (or processes acting on behalf of organizational users). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.	Multifactor authentication shall be implemented for users that require privileged level accounts to servers and workstations residing on the network (not standalone or PRIVATE VLAN segregated systems). Multifactor authentication can be implemented with through common access card (CAC) authentication. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity Verification (PIV) credentials.	This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-000777	IA-3	The organization defines a list of specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system.	All network connected endpoint devices (including but not limited to: workstations, printers, servers) shall be identified and authenticated before establishing a connection to the information system. Any device incapable of being authenticated to the system shall be documented.	APPLICABLE if capability exists
CCI-000778	IA-3	The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.	Configure the network infrastructure to identify all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE if capability exists
CCI-001958	IA-3	The information system authenticates an organization defined list of specific and/or types of devices before	Configure the network infrastructure to authenticate all network connected endpoint devices (including but not limited to: workstations, printers, servers) before establishing a local, remote, network connection. For information system components that have applicable STIGs or SRGs, the organization being	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		establishing a local, remote, or network connection.	inspected/assessed must comply with the STIG/SRG guidance.	
CCI-000176	IA-5(b)	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	The organization being inspected/assessed defines and documents procedures for setting initial authenticator content.	N/A
CCI-001544	IA-5(c)	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	The organization being inspected/assessed documents and implements authenticator strength mechanisms sufficient for the intended use of the authenticators.	APPLICABLE if capability exists
CCI-001989	IA-5(e)	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	Document and implement procedures to change default authenticators (passwords, etc.) or apply authenticators to all capable components prior to system installation.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000182	IA-5(g)	The organization manages information system authenticators by changing/refreshing authenticators in accordance with the organization defined time period by authenticator type.	Document and implement procedures for changing/refreshing authenticators in the following time periods: • Password: 60 days.	N/A
CCI-001610	IA-5(g)	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD has defined the time period of Password: 60 days. Biometrics: every 3 years.	N/A
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of upper case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 192.	APPLICABLE if capability exists
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of lower case characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 193.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of numeric characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 194.	APPLICABLE if capability exists
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.	The organization being inspected/assessed configures the information system to enforce minimum password length. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 205.	APPLICABLE if capability exists
CCI-001611	IA-5(1)(a)	The organization defines the minimum number of special characters for password complexity enforcement.	DoD has defined the minimum number of special characters for password complexity enforcement as one special character.	APPLICABLE if capability exists
CCI-001612	IA-5(1)(a)	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD has defined the minimum number of upper case characters for password complexity enforcement as one upper-case character.	APPLICABLE if capability exists
CCI-001613	IA-5(1)(a)	The organization defines the minimum number of lower case	DoD has defined the minimum number of lower case characters for password complexity enforcement as one lower-case character.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		characters for password complexity enforcement.		
CCI-001614	IA-5(1)(a)	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD has defined the minimum number of numeric characters for password complexity enforcement as one numeric character.	APPLICABLE if capability exists
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the minimum number of special characters used.	The organization being inspected/assessed configures the information system to enforce password complexity by the minimum number of special characters used. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1619.	APPLICABLE if capability exists
CCI-000195	IA-5(1)(b)	The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195.	APPLICABLE if capability exists
CCI-001615	IA-5(1)(b)	The organization defines the minimum number of characters that are changed when	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 195. DoD has defined the minimum number	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		new passwords are created.	of characters as 50% of the minimum password length.	
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-protected passwords.	Configure the information system to store only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 196.	APPLICABLE if capability exists
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to transmit only encrypted representations of passwords. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 197.	APPLICABLE if capability exists
CCI-000198	IA-5(1)(d)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Configure the information system to enforce minimum password lifetime restrictions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 198.	APPLICABLE if capability exists
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.	Configure the information system to enforce maximum password lifetime restrictions. For capable components, set maximum password age to 60 days or less (excluding “0”). For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 199.	APPLICABLE if capability exists
CCI-001616	IA-5(1)(d)	The organization defines minimum password lifetime restrictions.	DoD has defined the minimum password lifetime restrictions as 24 hours.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001617	IA-5(1)(d)	The organization defines maximum password lifetime restrictions.	DoD has defined the maximum password lifetime restrictions as 60 days and not being "0".	APPLICABLE if capability exists
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.	For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 200. All other components utilizing passwords, the password reuse should be set to 24. If the components are incapable of being set to 24 then implement the maximum possible.	APPLICABLE if capability exists
CCI-001618	IA-5(1)(e)	The organization defines the number of generations for which password reuse is prohibited.	Per the STIGs for Windows based systems, the DOD has defined this to be set at a minimum of 24.	APPLICABLE if capability exists
CCI-002041	IA-5(1)(f)	The information system allows the use of a temporary password for system logons with an immediate change to a permanent password.	The organization being inspected/assessed configures the information system to allow the use of a temporary password for system logons with an immediate change to a permanent password. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 2041.	APPLICABLE if capability exists
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for	DoDI 8520.03 defines types of authentication credentials that are acceptable for authentication to different systems based on the systems' information sensitivity levels and the users' access environments. The definitions for credential strengths D, E and H found in DoDI 8520.03 Enclosure 3, Section 3 specifically deal with acceptable types of	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		token-based authentication.	hardware PKI credentials. DoD Components are automatically compliant with this control because they are covered by the DoD-level policy, DoDI 8520.03.	
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	The information system performing hardware token-based authentication must be configured to accept only DoD-approved PKI credentials in accordance with DoDI 8520.02 and DoDI 8520.03. For unclassified systems, DoD-approved PKI credentials include DoD PKI credentials, External Certification Authority (ECA) PKI credentials, and DoD-approved external PKI credentials. For SIPRNet, DoD-approved PKI credentials include DoD PKI credentials and NSS PKI credentials. If the information system accepts DoD-approved external PKI credentials, the information system must be configured to accept only certificates at approved assurance levels, as represented by the Certificate Policy Object Identifiers (OIDs) asserted in the certificate. The current list of DoD-approved external PKIs and acceptable Object Identifiers (OIDs) for each approved external PKI is available at http://iase.disa.mil/pki-pke/interoperability.	APPLICABLE if capability exists
CCI-000206	IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Configure the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 206. Applicable to networked devices. Does not apply to devices that have NO feedback during password/PIN entry.	APPLICABLE if capability exists

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			Devices shall 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 CCI-000206, comply with the requirements of those STIGS/SRGs.	
CCI-000803	IA-7	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	For devices that have STIG/SRGs related to CCI-000803, comply with the requirements of those STIG/SRGs.	APPLICABLE if capability exists
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	Develop a diagram and explain within the system security plan (SSP) the authorization boundary for the complete control system including all networked devices and controller hardware.	N/A
CCI-003053	PL-2(a)(4)	The organization's security plan for the information system provides the security	The NIST SP800-60, Vol 2, Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		categorization of the information system including supporting rationale.	environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency. The recommended Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)} Therefore the system shall be categorized as a LOW-LOW-LOW system.	
CCI-000207	PM-5	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being inspected/assessed must register and maintain their information systems in DITPR.	APPLICABLE
CCI-000236	PM-11(b)	The organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	No additional protection needs are needed aside from what the network provider supplies. Control system components (not including servers and workstations) would generally be on a private PRIVATE VLAN without public access thereby further segregating the components from the cyber domain.	N/A
CCI-001048	RA-3(a)	The organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of	The conducting of a Risk Assessment will most likely be site specific. The owning organization will need to conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	The Designer can assist in identifying risk to the owing organization in order to complete the risk assessment.	
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	Servers, workstations and network infrastructure on the network will be scanned for vulnerabilities by the network provider. All other IP devices associated with the system (whether on the public or private side of the network) 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. The owning organization will need a service level agreement (SLA) with the network provider to perform scanning of IP devices on a private PRIVATE VLAN or dark fiber network, or have in-house personnel assigned to perform the vulnerability scanning. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new	Conduct vulnerability scans of the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported via authoritative sources (e.g., IAVM, CTO, DTM, STIG, product vendor).	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		vulnerabilities potentially affecting the system/applications are identified and reported.		
CCI-001641	RA-5(a)	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	DoD has defined the requirement for vulnerability scanning periodicity of every 30 days. If the organization has determined a requirement for random scanning they must document that process. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001643	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined process for random scans.	Servers, workstations and network infrastructure on the network will follow the process for random scans as defined by the Network Provider. The organization will conduct random vulnerability scans every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs) for all other control system components on a PRIVATE VLAN or the portion not scannable by the Network Provider.. The organization will document the vulnerability scans as an audit trail for future reference. The audit trail must be maintained IAW DoD, CYBERCOM, or component policies. DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and	The organization whether through the Network Provider or otherwise, employs the DoD Enterprise scanning tool.	N/A

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.		
CCI-001058	RA-5(c)	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization analyzes vulnerability scan reports and security control assessment results with the intent of identifying legitimate vulnerabilities and the relationship between vulnerabilities and security controls.	N/A
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities identified in RA-5, CCI 001058 IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). Audit records of actions must be maintained IAW applicable DoD, CYBERCOM, and/or component policies. DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).	Impractical
CCI-003116	SA-4(10)	The organization employs only information technology products on the FIPS PUB 201-2-approved	The organization being inspected/assessed employs DoD approved PKI tokens for identity verification.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.		
CCI-003124	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure configuration of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure configuration of the system, component, or service.	APPLICABLE
CCI-003125	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure installation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure installation of the system, component, or service.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-003126	SA-5(a)(1)	The organization obtains administrator documentation for the information system, system component, or information system services that describes secure operation of the system, component, or service.	The organization being inspected/assessed documents within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe secure operation of the system, component, or service.	APPLICABLE
CCI-003127	SA-5(a)(2)	The organization obtains administrator documentation for the information system, system component, or information system services that describes effective use and maintenance of security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe effective use and maintenance of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003128	SA-5(a)(3)	The organization obtains administrator documentation for the information system, system component, or information system services that describes known	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe known vulnerabilities of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.		
CCI-003129	SA-5(b)(1)	The organization obtains user documentation for the information system, system component, or information system service that describes user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	Document within contracts/agreements, requirements that the developer provide administrator documentation for the information system, system component or information system service that describe user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-003130	SA-5(b)(2)	The organization obtains user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes methods for user interaction which enables individuals to use the system, component, or service in a more secure manner. To the extent possible this should also apply to Control System software applications.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		service in a more secure manner.		
CCI-003131	SA-5(b)(3)	The organization obtains user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service.	Document within contracts/agreements, requirements that the developer provide user documentation for the information system, system component or information system service that describes user responsibilities in maintaining the security of the system, component, or service. To the extent possible this should also apply to Control System software applications.	APPLICABLE
CCI-001093	SC-5	The organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system.	Definition of the types of denial of service attacks will be defined at the Network Provider level.	APPLICABLE
CCI-002385	SC-5	The information system protects against or limits the effects of organization-defined types of denial of service attacks by employing organization-	For information system components that have applicable STIGs or SRGs, the organization must comply with the STIG/SRG guidance. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		defined security safeguards.		
CCI-002386	SC-5	The organization defines the security safeguards to be employed to protect the information system against, or limit the effects of, denial of service attacks.	Definition of the security safeguard to be employed to protect the information system will be defined at the Network Provider level for all devices on the Network Provider. To the greatest extent practical, the hardware performs control logic without reliance on the network.	APPLICABLE
CCI-001097	SC-7(a)	The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.	Monitoring and the controlling of communications at the external boundary of the system will be the responsibility of the Network Provider. The control system shall not be publicly accessible.	N/A
CCI-001133	SC-10	The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity	The organization being inspected/assessed configures the information system to terminate the network connection associated with a communications session at the end of the session or after 10 minutes in band management and 15 minutes for user sessions. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
CCI-001134	SC-10	The organization defines the time period of inactivity after which the information system terminates a network connection associated with a communications session.	DoD has defined the time period as 10 minutes in band management and 15 minutes for user sessions.	Impractical
CCI-002530	SC-39	The information system maintains a separate execution domain for each executing process.	To the greatest extent practical, the hardware performs control sequences without reliance on the network.	APPLICABLE
CCI-002544; 002545;002546	SC-41	The organization defines the information systems or information system components on which organization-defined connection ports or input/output devices are to be physically disabled or removed	Physically disable or remove connection ports or input/output devices.	APPLICABLE
CCI-001241	SI-3(c)(1)	The organization configures malicious code protection mechanisms to perform periodic scans of the	The Network Provider will implement/configure security scanning for servers and workstations on their network. Servers and workstations installed under this project that are on a PRIVATE VLAN, the owning organization must install and configure malware protection software.	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
		information system on an organization-defined frequency.	Configure software to perform a full system scan every 7 days. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance that pertains to CCI 1241. DoD has defined the frequency as every 7 days.	
CCI-002623	SI-3(c)(1)	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD has defined the frequency as every 7 days.	Impractical
CCI-001253	SI-4(a)(1)	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.	DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	Impractical
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	Network monitoring is conducted by the network provider for control system components on non-private (VLAN) side. Network monitoring cannot be implemented for field devices/components on the private network (VLAN).	Impractical
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed	The organization being inspected/assessed defines and documents the software on which integrity checks will be performed. DoD has determined the software is not appropriate to	Impractical

CRH Simulator Facility ADAL Designer Control Correlation Identifiers 25 05 11.26 02 Attachment A BUILDING CONTROL SYSTEMS INCLUDING ELECTRICAL AND LIGHTING CONTROLS LOW-LOW-LOW				
CCI Number	**800-53/82 Control Text Indicator**	**CCI Definition**	**Designer Implementation**	**Classification**
			define at the Enterprise level.	
CCI-002773	SI-17	The organization defines the fail-safe procedures to be implemented by the information system when organization-defined failure conditions occur.	In many cases standard control system design of sequences and alarm requirements address these CCIs without any additional design requirements	APPLICABLE
CCI-002774	SI-17	The organization defines the failure conditions which, when they occur, will result in the information system implementing organization-defined fail-safe procedures.	Failure conditions likely to be experienced by control system components are component failure and communications failure to components.	APPLICABLE
CCI-002775	SI-17	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	Configure the information system to implement fail-safe procedures. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance.	APPLICABLE

THIS PAGE INTENTIONALLY LEFT BLANK