SECTION 25 05 11

CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS
11/17

PART 1 GENERAL

1.1 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.

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

ASHRAE 135	(2016) BACnet—A Data Communication Protocol for Building Automation and Control Networks

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 201-2	(2013) Personal Identity Verification (PIV) of Federal Employees and Contractors

U.S. DEPARTMENT OF DEFENSE (DOD)

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

1.2 SUBMITTALS

Government approval is required for submittals with a "G" designation; submittals not having a "G" designation are [for Contractor Quality Control approval.][for information only. When used, a designation following the "G" designation identifies the office that will review the submittal for the Government.] 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[, [_____]]

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; G[, [_____]]

SD-11 Closeout Submittals

Password Summary Report; G[, [_____]]

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

1.3 CYBERSECURITY DOCUMENTATION

[1.3.1 Cybersecurity Interconnection Schedule

Provide a completed Cybersecurity Interconnection Schedule documenting connections between the installed system and other systems. See Attachment 25 05 11-A.

]1.3.2 Network Communication Report

Provide a network communication report. See Attachment 25 05 11-B.

1.3.3 Control System Inventory Report

Provide a Control System Inventory report. See Attachment 25 05 11-C.

1.3.4 Cybersecurity Riser Diagram

Provide a Cybersecurity Riser Diagram.

1.4 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.

1.5 CYBERSECURITY DURING CONSTRUCTION

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

1.5.1 Contractor Computer Equipment

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

1.5.1.1 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.

1.5.1.2 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.

1.5.1.3 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.

1.5.1.4 Contractor Computer Cybersecurity Compliance Statements

Provide a single submittal containing completed Contractor Computer Cybersecurity Compliance Statements for each company using contractor owned computers that will be connected to network controllers during construction. See Attachment 25 05 11-D.

1.5.2 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:

1.5.2.1 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.

1.5.3 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

1.5.4 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.

1.5.5 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.

1.5.6 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. If no temporary IP networks will be used, provide a single copy of the Statement indicating this. See Attachment 25 05 11-E.

1.6 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

[3.1.1.1 [_____] Control System Devices

[_____]

]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 support user accounts (such as "admin", "user 1", "user 2")or have their web interface disabled.

3.1.2 Unsuccessful Logon Attempts

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

3.1.2.1 Devices Supporting Accounts

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

3.1.2.2 Devices

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

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

b. Once an account is locked, the account must stay locked until unlocked by an administrator.

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

3.1.2.3 High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

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

High Availability Interfaces Exempt from Unsuccessful Logon Attempts Requirements

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

]

3.1.3 System Use Notification

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

Devices which are connected to a network and have a user interface must display a warning banner meeting the requirements of DTM 08-060 if capable of doing so. Devices which are connected to a network and have a user interface but are not capable of displaying a banner must have a permanently affixed label displaying an approved banner from DTM 08-060.Labels must be machine printed or engraved, plastic or metal, designed for permanent installation, must use a font no smaller than 14 point, and must provide a high contract between font and background colors.

3.1.3.1 User Interface Banner Schedule

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

User Interface Schedule Format
(with sample entries)

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

3.1.4 Permitted Actions Without Identification or Authentication

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

3.1.5 Wireless Access

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

3.1.5.1 Wireless IP Communications

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

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

3.1.5.2 Non-IP Wireless Communication

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

3.1.5.3 Wireless Communication Request

Provide a report documenting the proposed use of wireless communication prior to beginning construction using the Wireless Communication Request Schedule. See Attachment 25 05 11-F.

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)

a. Successful and unsuccessful logon attempts

b. Privileged activities or other system level access

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

d. Concurrent logons from different workstations

e. Successful and unsuccessful accesses to objects

f. All program initiations

g. All direct access to the information system

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

i. All kernel module load, unload, and restart

3.2.1.1.2 Audit Event Information To Record

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

a. What type of event occurred

b. When the event occurred

c. Where the event occurred

d. The source of the event

e. The outcome of the event

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

3.2.1.2 For HVAC Control System Devices

3.2.1.2.1 HVAC Control System Devices FULLY Supporting User Accounts

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

a. Successful and unsuccessful logon attempts to the device

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

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

d. All device shutdown and startup

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

3.2.1.2.2 Other HVAC Control System Devices

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

[3.2.1.3 [_____] Control System Devices

[_____]

]3.2.1.4 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:

3.2.1.4.1 Devices Which FULLY Support Accounts

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

3.2.1.4.1.1 Audited Events

Configure each device to audit the following events:

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

a. Successful and unsuccessful logon attempts

b. Privileged activities or other system level access

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

d. Concurrent logons from different workstations

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

f. All kernel module load, unload, and restart

3.2.1.4.1.2 Audit Event Information To Record

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

a. what type of event occurred

b. when the event occurred

c. where the event occurred

d. the source of the event

e. the outcome of the event

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

3.2.1.4.2 Devices Which Do Not FULLY Support Accounts

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

3.2.2 Audit Storage Capacity and Audit Upload

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

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

b. For non-computer control system devices capable of generating audit records, provide [60][_____] days worth of secure local storage, assuming [10][_____] auditable events per day.[

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

3.2.2.1 Device Audit Record Upload Software

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

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

3.2.3 Response to Audit Processing Failures

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

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

3.2.4 Time Stamps

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

[3.2.4.3 [_____] Control System Devices

[_____][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

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

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

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

3.5.1.1 HVAC Control Systems Devices

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

3.5.1.2 Electronic Security System Devices

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

[3.5.1.3 [_____] Control System Devices

[_____]

]3.5.1.4 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][or][_____].

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][password-based authentication][hardware token-based authentication].

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

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

[3.5.2.1.2 [_____] Control System Devices

[_____]

]3.5.2.1.3 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][password-based authentication][hardware token-based authentication].

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

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

3.5.2.2 Password-Based Authentication Requirements

3.5.2.2.1 Passwords for Computers
All computers supporting password-based authentication must enforce the

following requirements:

a. Minimum password length of 12 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character.

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

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

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

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

3.5.2.2.2 Passwords for Non-Computer Devices FULLY Supporting Accounts

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

a. Minimum password length of twelve (12) characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character.

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

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

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

3.5.2.2.3 Passwords for Web Interfaces

Passwords for connecting to a web interface supporting password-based authentication must enforce the following requirements:

a. Minimum password length of 12 characters

b. Password must contain at least one uppercase character.

c. Password must contain at least one lowercase character.

d. Password must contain at least one numeric character.

e. Password must contain at least one special character.

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

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

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

3.5.2.2.4 Passwords for Devices Minimally Supporting Accounts

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 [_____]. Do not use the same password for more than one device unless specifically instructed to do so. Provide a Password Summary Report documenting the password for each device and describing the procedure to change the password for each device.

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

3.5.2.3 Hardware Token-Based Authentication Requirements

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

3.5.3 Authenticator Feedback

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

Devices must never show authentication information, including passwords, on a display. Devices that momentarily display a character as it is entered, and then obscure the character, are acceptable. For devices that have STIGs or SRGs related to obscuring of authenticator feedback (CCI-000206), comply with the requirements of those STIGS/SRGs.

3.5.4 Device Identification and Authentication

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

3.5.4.1 For HVAC Control System Devices

Devices using Fox Protocol must use HTTPS[using a web server certificate obtained from [_____]]. [Devices using Fox Protocol must support IEEE 802.1x.][Devices using Ethernet must support IEEE 802.1x.

][Devices using BACnet must support Network Security as specified in Clause 24 of ASHRAE 135.]

[3.5.4.2 [_____] Control System Devices

[_____]

]3.5.4.3 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 [_____]] instead.

3.5.5 Cryptographic Module Authentication

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

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

3.6 EMERGENCY POWER

[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 [_____] by responding with a [_____].]For control system devices other than computers:

3.7.1 HVAC Control System Devices Other Than Computers

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

[3.7.2 [_____] Control System Devices Other Than Computers

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

]3.7.3 Default Requirements for Control System Devices

Non-computer control system devices where Durability to Vulnerability Scanning requirements are not otherwise indicated in this Section [must respond to scans from [_____] by responding with a [_____]][are not required to respond to scans].

3.8 FIPS 201-2 REQUIREMENT

{For Reference Only: This subpart (and its subparts) relates to SA-4

(10); CCI-003116}

Devices in the following systems which implement PIV must be on the NIST FIPS 201-2 approved product list: [NONE][electronic security systems(ESS)][_____].

3.9 DEVICES WITH CONNECTION TO MULTIPLE IP NETWORKS

Except for Ethernet switches, do not use more than one physical connection to IP networks on the same device unless doing so is both required by the project specifications and the specific application is approved. If a device with multiple IP connections is required, provide a Multiple IP Connection Device Request using the Multiple IP Connection Device Request Schedule 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.

[3.10.2 Cryptographic Protection

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

]3.11 SYSTEM AND INTEGRATION INTEGRITY

3.11.1 Malicious Code Protection

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

[3.11.2 Information System Monitoring

[_____]

]3.12 FIELD QUALITY CONTROL

3.12.1 Tests

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

-- End of Section --