



SAME Cybersecurity Presentation

BY RICHARD WATSON, US ARMY CORPS OF ENGINEERS
TULSA DISTRICT

How did I get involved in Cybersecurity?

- Background in process control and automation
- Worked for USACE in Hydropower
- Became DoD 8570 certified as IAT1 in 2015 (CompTIA Network + CE)
- System administrator on SCADA system in 2015

Dateline for Cybersecurity in DoD

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) was introduced in the 1990's
- DoD Information Assurance Certification and Accreditation Process (DIACAP) was introduced in 2006
- Risk Management Framework (RMF) was introduced in 2014

What is cybersecurity?

- Protecting of digital system to prevent unauthorized use, access, or interrupting operation
 - How is this accomplished
 - Have a framework that helps you deal with both attempted and successful cyber attacks
 - Risk Management Framework for DoD
 - Providing a hardened control system
 - Limiting the types of media that can be introduced
 - Closing unused ports
 - Password protection
 - Having policies in place for emergencies
 - Having trained personnel in place to handle emergencies

How does cybersecurity apply to military construction?

- New construction and renovations of facilities add facility-related controls systems that transmit and store digital information
- Designers of Record are not responsible for getting a system the Authority to Operate (ATO) that would be on the System Owner (SO)
- Designers of Record are responsible for providing the System Owner (SO) a system that can be hardened and meets as many of the criteria for cybersecurity as possible

What systems do cybersecurity principles apply?

- BAS (Building Automation Systems)
 - HVAC (Heating, Ventilation, and Air Conditioning)
 - Lighting Control
 - Fire Protection/Life Safety
 - UMCS (Utility Monitoring and Control System)
 - ESS (Electronic Security Systems)
 - Other systems
- SCADA (Supervisory Control and Data Acquisition)
- ICS (Industrial Control Systems)

Example of why cyber needed in BAS

NIST NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE **NVD**

VULNERABILITIES

CVE-2018-8880 Detail

Current Description

Lutron Quantum BACnet Integration 2.0 (firmware 3.2.243) doesn't check for correct user authentication before showing the /deviceIP information, which leads to internal network information disclosure.

Source: MITRE
[View Analysis Description](#)

Impact

| CVSS v3.0 Severity and Metrics: | CVSS v2.0 Severity and Metrics: |
|--|---|
| Base Score: 7.5 HIGH | Base Score: 5.0 MEDIUM |
| Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N |
| (V3.0 legend) | (V2 legend) |
| Impact Score: 3.6 | Impact Subscore: 2.9 |
| Exploitability Score: 3.9 | Exploitability Subscore: 10.0 |

| | |
|---------------------------------------|------------------------------------|
| Attack Vector (AV): Network | Access Vector (AV): Network |
| Attack Complexity (AC): Low | Access Complexity (AC): Low |
| Privileges Required (PR): None | Authentication (AU): None |
| User Interaction (UI): None | |

QUICK INFO

CVE Dictionary Entry: CVE-2018-8880

NVD Published Date: 04/23/2018

NVD Last Modified: 05/25/2018

Another Example

NIST

NVD MENU

[Information Technology Laboratory](#)

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2015-6471 Detail

Current Description

Eaton Cooper Power Systems ProView 4.x and 5.x before 5.1 on Form 6 controls and Idea and IdeaPLUS relays does not properly initialize padding fields in Ethernet packets, which allows remote attackers to obtain sensitive information by reading packet data.

Source: MITRE

[View Analysis Description](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2015-6471

NVD Published Date:

12/22/2015

NVD Last Modified:

12/23/2015

Impact

CVSS v3.0 Severity

and Metrics:

Base Score: 5.3 MEDIUM

Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A/N/AC:M/Au:N/C:P/I:N/A/N
(V3.0 legend)

Impact Score: 1.4

Exploitability Score: 3.9

CVSS v2.0 Severity

and Metrics:

Base Score: 4.3 MEDIUM

Vector:

AV:N/AC:M/Au:N/C:P/I:N/A/N
(V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.6

Attack Vector (AV): Network

Attack Complexity (AC):

Low

Privileges Required (PR):

Access Vector (AV):

Network

Access Complexity (AC):

Medium

Authentication (AU): None

What are the five steps of cybersecurity for designers?

- Work with the system owner to determine the C.I.A. impact rating of control systems in facility
- Use the C.I.A. impact ratings to select the proper list of security controls
- Use the DoD Master Control Correlation Identifier (CCI) list to create a list of relevant CCI's based on the C.I.A impact rating
- Categorize CCI's and identify the CCI's that require input from the designer or are the designer's responsibility
- Include cybersecurity requirements in project specifications and documents

Work with the system owner to determine the C.I.A. impact rating of control systems in facility

- What is C.I.A.
 - C – Confidentiality (restrictions of information access)
 - I – Integrity (guarding against information modification or destruction)
 - A – Availability (ensuring timely and reliable access)
- Prepare a list of control systems that are going to be incorporated in the building including any communication protocols used.
- Ask the system owner to provide an impact rating for each control system on the project.

Use the C.I.A. impact ratings to select the proper list of security controls

- What are examples of controls
 - AC – Access control
 - AU – Audit and Accountability
 - SC – System and Communications Protection
 - There are a total of 18 families of security controls
- Where can these be found NIST SP 800-82r2 and UFC 4-010-06
- What is meant by families
 - Access control is broken down farther
 - AC-2 Account Management
 - AC-3 Access Enforcement
 - Etc.

Security Control Example from UFC

UFC 4-010-06

19 September 2016

Change 1, 18 January 2017

Table G-1 Access Control (AC) Control Family

| Security Control ID | Security Control Name and Design Guidance |
|---------------------|---|
| AC-2 | <p>Account Management: Specify what account types provide which permissions in the control system (e.g. “view only”, “acknowledge alarms”, “change set-points”, etc.). Note that designer may need to explain these roles to the ISSM / ISSO so they can perform their DoD-defined duties under this control. Note that “accounts” (and particularly “temporary” or “emergency” accounts) likely exist at Level 4 and may or may not exist at Levels 1 or 2, depending on the control system type. (For example, many building control systems won’t have user accounts at these levels, but many utility control systems do). Designer may need to explain lack of “accounts” at Levels 1 and 2. Specifications should require that account activities be audited (logged), but auditing may be limited to software applications, and require notification be supported. Note that notification (e.g. email, rollup to another system) will generally require Platform Enclave or other Level 4 and Level 5 support for actual execution.</p> |
| AC-3 | <p>Access Enforcement: AC-3 is met by requiring the contractor to configure any control system component which has a STIG or SRG in accordance with that STIG or SRG”</p> |

Use the DoD Master Control Correlation Identifier (CCI) list to create a list of relevant CCI's based on the C.I.A impact rating

- Use the C.I.A. impact rating to list all of the CCI's that are included
- Is the CCI the responsibility of the Designer or someone/something else?
 - DoD Defined
 - Non-Designer (System Owner)
 - Platform Enclave (Standard IT equipment)
 - Impractical
- Is the CCI applicable to a control system

Who or What is Responsible

- DoD Defined
 - Provided by DoD either in a policy or a prescribed value
- Designer
 - Designer has some role in addressing this CCI
- Non-Designer
 - Designer does not have responsibility in this CCI
- Platform Enclave
 - Standard IT device implements this CCI
- Impractical
 - The control system is not capable of implementing this CCI

CCI Example from UFC

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

H-5 CCI TABLES

Table H-1 Summary of CCIs for LOW and MODERATE Impact Systems

| CCI # | 800-53 Control Text Indicator | Applies At Or Above Impact | Table Reference | Applicable to a Control System? |
|------------|-------------------------------|----------------------------|---|---------------------------------|
| CCI-002107 | AC-1 (a) | LOW | None (Non-Designer) | TRUE |
| CCI-002108 | AC-1 (a) | LOW | None (Non-Designer) | TRUE |
| CCI-000001 | AC-1 (a) (1) | LOW | None (Non-Designer) | TRUE |
| CCI-000002 | AC-1 (a) (1) | LOW | None (Non-Designer) | TRUE |
| CCI-002106 | AC-1 (a) (1) | LOW | None (Non-Designer) | TRUE |
| CCI-000004 | AC-1 (a) (2) | LOW | None (Non-Designer) | TRUE |
| CCI-000005 | AC-1 (a) (2) | LOW | None (Non-Designer) | TRUE |
| CCI-002109 | AC-1 (a) (2) | LOW | None (Non-Designer) | TRUE |
| CCI-000003 | AC-1 (b) (1) | LOW | None (Non-Designer) | TRUE |
| CCI-001545 | AC-1(b)(1) | LOW | | TRUE |
| CCI-000006 | AC-1(b)(2) | LOW | None (Non-Designer) | TRUE |
| CCI-001546 | AC-1(b)(2) | LOW | | TRUE |
| CCI-002110 | AC-2(a) | LOW | Table H-4 (Designer) | TRUE |
| CCI-002111 | AC-2(a) | LOW | None (Non-Designer) | TRUE |
| CCI-002112 | AC-2(b) | LOW | None (Non-Designer) | TRUE |
| CCI-000008 | AC-2(c) | LOW | None (Non-Designer) | TRUE |
| CCI-002113 | AC-2(c) | LOW | None (Non-Designer) | TRUE |
| CCI-002115 | AC-2(d) | LOW | None (Non-Designer) | TRUE |
| CCI-002116 | AC-2(d) | LOW | None (Non-Designer) | TRUE |
| CCI-002117 | AC-2(d) | LOW | None (Non-Designer) | TRUE |
| CCI-002118 | AC-2(d) | LOW | None (Non-Designer) | TRUE |
| CCI-002119 | AC-2(d) | LOW | None (Non-Designer) | TRUE |
| CCI-002120 | AC-2(e) | LOW | None (Non-Designer) | TRUE |
| CCI-000010 | AC-2(e) | LOW | None (Non-Designer) | TRUE |
| CCI-000011 | AC-2(f) | LOW | None (Non-Designer) | TRUE |
| CCI-002121 | AC-2(f) | LOW | None (Non-Designer) | TRUE |
| CCI-002122 | AC-2(g) | LOW | None (Non-Designer) | TRUE |
| CCI-002123 | AC-2(h)(1) | LOW | None (Non-Designer) | TRUE |
| CCI-002124 | AC-2(h)(2) | LOW | None (Non-Designer) | TRUE |
| CCI-002125 | AC-2(h)(3) | LOW | None (Non-Designer) | TRUE |
| CCI-002126 | AC-2(i)(1) | LOW | None (Non-Designer) | TRUE |
| CCI-002127 | AC-2(i)(2) | LOW | None (Non-Designer) | TRUE |
| CCI-002128 | AC-2(i)(3) | LOW | None (Non-Designer) | TRUE |
| CCI-000012 | AC-2(j) | LOW | None (Non-Designer) | TRUE |
| CCI-001547 | AC-2(j) | LOW | | TRUE |
| CCI-002129 | AC-2(k) | LOW | None (Non-Designer) | TRUE |
| CCI-000015 | AC-2(1) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001682 | AC-2(2) | MODERATE | Table H-5 (Designer) Table H-7 (Enclave) | TRUE |
| CCI-000016 | AC-2(2) | MODERATE | Table H-7 (Enclave) | TRUE |

Categorize CCI's and identify the CCI's that require input from the designer or are the designer's responsibility

- Can the control system do what is required in the CCI?
 - CCI-000048 states that the information system display's the organization use banner.
 - If the control system is capable of this include in UFGS specification
 - If the control system cannot do this, lists the reasons and state that it is impractical
- If the CCI states "The Information System..."
 - The Designer will need to address these
- If the CCI states "The Organization..."
 - The Designer may need to address this if STIGs or SRGs are involved

CCI example from UFC

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

| Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems | | | |
|---|-------------------------------|--|---|
| CCI # | 800-53 Control Text Indicator | CCI Definition | Responsibility |
| 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, policies, regulations, standards, and guidance. | Enclave Designer Impractical |
| 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-Defined Enclave Designer Impractical |
| 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. | DoD-Defined Enclave Designer Impractical |
| 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. | DoD-Defined Enclave Designer Impractical |
| 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. | DoD-Defined Enclave Designer Impractical |
| 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. | DoD-Defined Enclave Designer Impractical |
| CCI-000050 | AC-8(b) | 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. | Enclave Designer |

What are STIGs and SRGs

- Security Technical Implementation Guides (STIGs)
 - The actions needed to provide a hardened system for cybersecurity
 - Usually on a particular software or firmware (CISCO IOS, SEL, Windows, etc)
- Security Requirements Guides (SRGs)
 - The actions needed to provide a hardened system for cybersecurity
 - Usually on a generic system (Layer 2 switch, AAA)

Where do you get STIGs and SRGs

The screenshot shows a web browser window with the URL <https://public.cyber.mil>. The page features the DoD Cyber Exchange Public logo on the left and a navigation menu with items: Topics, Training, PKI/PKE, SRGs/STIGs, Resources, and Help. A search bar and a "Login with CAC" button are also visible. The main content area has a dark blue background with a network diagram. The heading "Cyber Awareness Challenge Version 2019" is prominently displayed. Below it, a paragraph of text describes the new version of the challenge, mentioning a major update, a new look and feel, and the addition of a Knowledge Check option, a Facilitator Guide, and a Facilitator Briefing. A yellow "LEARN MORE" button is centered below the text. At the bottom of the main content area, there are five small circles, with the second one from the left being filled, indicating the current slide in a sequence.

DoD CYBER EXCHANGE PUBLIC

Topics Training PKI/PKE SRGs/STIGs Resources Help

Cyber Awareness Challenge Version 2019

The new Cyber Awareness Challenge is now available. This version is a major update from previous versions, with a completely new look and feel. Return users will now have the option to opt out of the full course by taking the new Knowledge Check option. There is also an addition of a Facilitator Guide, and Facilitator Briefing all available under the Content Delivery Options.

LEARN MORE

Example STIG (Schweitzer Engineering Laboratories SEL-2740S)

Group ID (Valid): V-92263

Group Title: SRG-NET-000148-L2S-000015

Rule ID: SV-102363r1_rule

Severity: CAT I

Rule Version (STIG-ID): SELS-SW-000020

Rule Title: The SEL-2740S must uniquely identify all network-connected endpoint devices before establishing any connection.

Vulnerability Discussion: Controlling LAN access via identification of connecting hosts can assist in preventing a malicious user from connecting an unauthorized PC to a switch port to inject or receive data from the network without detection.

Check Content:

Review SEL-2740S flow rules to ensure they contain the proper match criteria (MAC, IP, Port, SRC, DST, etc.) for the connected hosts restricting all other access to the network.

If the SEL-2740S is configured with flows with wildcard or unnecessary packet forwarding rules, this is a finding.

Fix Text: For adding an SEL-2740S Flow Rule to forward traffic, do the following:

1. Log in to OTSDN Controller using Permission Level 3.
2. Click "Flow Entries" in Navigation Menu.
3. Click "Add Flow" button.
4. Enter General Setting values for "Switch", "Enable". Optional: Enter General Settings for "Table ID", "Priority", "Idle Timeout", and "Hard Timeout".
5. Depending on communication protocol behavior, enter appropriate Match Field values for "ARP Opcode" ("Request" or "Reply"), "ARP Source", "ARP Target", "Communication Service Type (CST) Match", "Ethernet Destination", "Ethernet Source", "Ethernet Type", "InPort", "IP Proto", "IPv4 Destination", "IPv4 Source", "TCP Destination", "TCP Source", "UDP Destination", "UDP Source", "VLAN Priority", and/or "VLAN Virtually ID".
6. Enter appropriate Write-Actions for "Pop VLAN ID", "Push VLAN ID", "Set VLAN ID", "Set VLAN Priority", "Set Queue", "Group by Alias or Value", and/or "Output by Alias or Value".
7. Click "Submit".
8. Repeat for every switch necessary.

CCI: CCI-000778

CCI-000778

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

Table H-1 Summary of CCIs for LOW and MODERATE Impact Systems

| CCI # | 800-53 Control Text Indicator | Applies At Or Above Impact | Table Reference | Applicable to a Control System? |
|------------|-------------------------------|----------------------------|---|---------------------------------|
| CCI-000552 | CP-10 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-000553 | CP-10(2) | MODERATE | Table H-5 (Designer) | TRUE |
| CCI-002855 | CP-12 | LOW | Table H-4 (Designer) | TRUE |
| CCI-002856 | CP-12 | LOW | Table H-4 (Designer) | TRUE |
| CCI-002857 | CP-12 | LOW | Table H-4 (Designer) | TRUE |
| CCI-001933 | IA-1(a) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-001934 | IA-1(a) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000756 | IA-1(a)(1) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000757 | IA-1(a)(1) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-001932 | IA-1(a)(1) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000760 | IA-1(a)(2) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000761 | IA-1(a)(2) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000758 | IA-1(b)(1) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000759 | IA-1(b)(1) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000762 | IA-1(b)(2) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000763 | IA-1(b)(2) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-000764 | IA-2 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-000765 | IA-2(1) | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-000766 | IA-2(2) | MODERATE | Table H-5 (Designer) Table H-7 (Enclave) | TRUE |
| CCI-000767 | IA-2(3) | MODERATE | Table H-5 (Designer) Table H-7 (Enclave) | TRUE |
| CCI-001949 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001951 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001952 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001948 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001950 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001947 | IA-2(11) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001953 | IA-2(12) | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-001954 | IA-2(12) | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-000777 | IA-3 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-000778 | IA-3 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-001958 | IA-3 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |

Example SRG (Layer 2 Switch SRG)

Group ID (Valid): V-62165

Group Title: SRG-NET-000235

Rule ID: SV-76655r2_rule

Severity: CAT II

Rule Version (STIG-ID): [SRG-NET-000235-L2S-000031](#)

Rule Title: The layer 2 switch must be configured to fail securely in the event of an operational failure.

Vulnerability Discussion: If the switch fails in an unsecure manner (open), unauthorized traffic originating externally to the enclave may enter or the device may permit unauthorized information release. Fail secure is a condition achieved by employing information system mechanisms to ensure, in the event of an operational failure of the switch, that it does not enter into an unsecure state where intended security properties no longer hold.

If the device fails, it must not fail in a manner that will allow unauthorized access. If the switch fails for any reason, it must stop forwarding traffic altogether or maintain the configured security policies. If the device stops forwarding traffic, maintaining network availability would be achieved through device redundancy.

An example is a firewall that blocks all traffic rather than allowing all traffic when a firewall component fails (e.g., fail closed and do not forward traffic). This prevents an attacker from forcing a failure of the system in order to obtain access. Abort refers to stopping a program or function before it has finished naturally. The term abort refers to both requested and unexpected terminations.

Check Content:

Review the vendor documentation to determine if the layer 2 switch will fail to a secure state in the event that the system initialization fails, shutdown fails, or abort fails.

If the layer 2 switch does not fail to a secure state in the event that the system initialization fails, shutdown fails, or abort fails, this is a finding.

Fix Text: Configure the layer 2 switch to fail to a secure state upon failure of initialization, shutdown, or abort actions.

CCI: CCI-001126

CCI-001126

UFC 4-010-06
19 September 2016
Change 1, 18 January 2017

Table H-1 Summary of CCIs for LOW and MODERATE Impact Systems

| CCI # | 800-53 Control Text Indicator | Applies At Or Above Impact | Table Reference | Applicable to a Control System? |
|------------|-------------------------------|----------------------------|---|---------------------------------|
| CCI-001093 | SC-5 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-002385 | SC-5 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-002386 | SC-5 | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-001097 | SC-7(a) | LOW | Table H-4 (Designer) Table H-6 (Enclave) | TRUE |
| CCI-002395 | SC-7(b) | LOW | | FALSE |
| CCI-001098 | SC-7(c) | LOW | Table H-6 (Enclave) | TRUE |
| CCI-001101 | SC-7(3) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001102 | SC-7(4)(a) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001103 | SC-7(4)(b) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-002396 | SC-7(4)(c) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001105 | SC-7(4)(d) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001106 | SC-7(4)(e) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001107 | SC-7(4)(e) | MODERATE | | TRUE |
| CCI-001108 | SC-7(4)(e) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001109 | SC-7(5) | MODERATE | Table H-5 (Designer) Table H-7 (Enclave) | TRUE |
| CCI-002397 | SC-7(7) | MODERATE | Table H-7 (Enclave) | TRUE |
| CCI-001126 | SC-7(18) | MODERATE | Table H-5 (Designer) | TRUE |
| CCI-002418 | SC-8 | MODERATE | Table H-5 (Designer) | TRUE |
| CCI-002419 | SC-8(1) | MODERATE | Table H-5 (Designer) | TRUE |
| CCI-002421 | SC-8(1) | MODERATE | Table H-5 (Designer) | TRUE |

Include cybersecurity requirements in project specifications and documents

- Create a UFGS 25 05 11 for each control system that is included in the design
- Have a write up in the Design Analysis for each control system
 - How was the C.I.A. impact rating was determined
 - Description of the control system including any protocols used and whether it connects to a base wide system or not
- Attach list of CCI's to the Design Analysis
- Attach checklist from ECB to Design Analysis (Optional)

What are the deliverables at each stage of design?

- ECB 2018-11 has a design checklist with items that are required at each level of design
- UFC 4-010-06 chapter 5 also lists additional deliverables

What is ECB 2018-11?

- ECB 2018-11 was released in August of 2018
- It mandates the use of Mandatory Centers of Expertise (MCX) for USACE projects
- The Mandatory Centers of Expertise for Cybersecurity are
 - Civil Works CICS-MCX in Little Rock District
 - Military CSC-MCX in Huntsville

References

- DoDI 8500.01 Cybersecurity
- DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)
- UFC 4-010-06 Cybersecurity of Facility-Related Control Systems
- ECB 2018-11 Control System Cybersecurity Coordination Requirement
- Component level Cybersecurity Directives (Example AFI 17-130)
- NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-82r2 Guide to Industrial Control Systems (ICS) Security

Questions