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

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

Record of Changes (changes are indicated by **1**\ ... /**1**/)

Change No.	**Date**	**Location**
1	01/19/2017	Revised paragraphs 3-3, 3-6 (second bullet), 3-6.2, 4-3 (second to last bullet), and 5-2.2.2.

FOREWORD

The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with USD (AT&L) Memorandum dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and in some instances, Bilateral Infrastructure Agreements (BIA.) Therefore, the acquisition team must ensure compliance with the most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

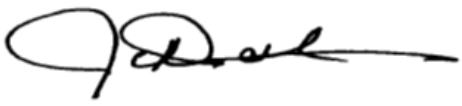
UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Services' responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Defense agencies should contact the preparing service for document interpretation and improvements. Technical content of UFC is the responsibility of the cognizant DoD working group. Recommended changes with supporting rationale should be sent to the respective service proponent office by the following electronic form: Criteria Change Request. The form is also accessible from the Internet sites listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide web site http://dod.wbdg.org/.

Hard copies of UFC printed from electronic media should be checked against the current electronic version prior to use to ensure that they are current.

AUTHORIZED BY:



JAMES C. DALTON, P.E.
Chief, Engineering and Construction
U.S. Army Corps of Engineers

JOSEPH E. GOTT, P.E.
Chief Engineer
Naval Facilities Engineering Command

EDWIN H. OSHIBA, SES, DAF
Deputy Director of Civil Engineers
DCS/Logistics, Engineering &
Force Protection

MICHAEL McANDREW
DASD (Facilities Investment and Management)
Office of the Assistant Secretary of Defense
(Energy, Installations, and Environment)

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

UNIFIED FACILITIES CRITERIA (UFC)
NEW DOCUMENT SUMMARY SHEET

Document: UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*

Superseding: None

Description: UFC 4-010-06 provides requirements for incorporating cybersecurity into the design of facility-related control systems.

Justification: DoDI 8500.01, Cybersecurity requires the implementation of a "multi-Leveled cybersecurity risk management process… as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 and the Committee on National Security Systems (CNSS) Policy 22." It further requires the use of NIST SP 800-37, and a transition to CNSSI No. 1253 and NIST SP 800-53. For control systems, NIST SP 800-82 R2 Appendix G is used as the overlay under CNSSI No. 1253.

This UFC provides criteria for the inclusion of cybersecurity in the design of control systems in order to address appropriate Risk Management Framework (RMF) security controls during design and subsequent construction.

Impact: While the inclusion of cybersecurity during the design and construction of control systems will increase the cost of both design and construction, it is more cost-effective to implement these security controls starting at design than to implement them on a designed and installed system. Historically, control systems have not included these cybersecurity requirements, so the addition of these cybersecurity requirements will increase both cost and security. The increase in cost will be lower than the increase in cost of applying these requirements after design.

Note: This UFC is based on NIST SP 800-53 R4 and NIST SP 800-82 R2. As new versions of NIST publications are issued, guidance will be posted on the RMF Knowledge Service (https://rmfks.osd.mil) and will be included in updates to this UFC.

TABLE OF CONTENTS

FIGURES

TABLES

CHAPTER 1 INTRODUCTION

1-1 BACKGROUND.

A control system (CS) typically consists of networked digital controllers and a user interface which are used to monitor, and generally also to control equipment. There are many types of control systems ranging from building control systems to manufacturing control systems to weapon control systems, all with different names and terminology. Facility-related control systems are a subset of control systems that are used to monitor and control equipment and systems related to DoD real property facilities (e.g., building control systems, utility control systems, electronic security systems, and fire and life safety systems).

The Risk Management Framework (RMF) is the DoD process for applying cybersecurity to information technology (IT), including control systems. The RMF categorizes systems by the impact the system can have on organizational mission using HIGH, MODERATE, and LOW impact levels. The RMF is further described in CHAPTER 2 and APPENDIX C.

1-2 PURPOSE AND SCOPE.

This UFC describes requirements for incorporating cybersecurity in the design of all facility-related control systems. It defines a process based on the Risk Management Framework suitable for control systems of any impact rating, and provides specific guidance suitable for control systems assigned LOW or MODERATE impact level.

1-3 APPLICABILITY.

This UFC applies to all planning, design and construction, renovation, and repair of new and existing facilities and installations that result in DoD real property assets, regardless of funding source. MODERATE and HIGH impact systems generally require more expertise and attention to detail than a UFC can provide. Design of MODERATE or HIGH impact systems will typically require additional customized requirements to achieve appropriate levels of cybersecurity and design of such systems should be coordinated with the points of contact provided in Paragraph 1-6.

In defining specific requirements for LOW or MODERATE systems, this UFC assumes the control system is being implemented on a DoD Installation. Systems not being implemented on a DoD Installation will require modifications to the requirements included in this UFC.

1-4 GENERAL BUILDING REQUIREMENTS.

Comply with UFC 1-200-01, DoD Building Code (General Building Requirements). UFC 1-200-01 provides applicability of model building codes and government unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, high performance and sustainability requirements, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-5 ORGANIZATION.

CHAPTER 2 provides an overview of the RMF as it applies to control systems, control system architecture and the cybersecurity approach to control systems. CHAPTER 3 defines a 5-step approach to incorporating cybersecurity into the design of control systems. CHAPTER 4 defines minimum design requirements for control systems to be implemented in addition to the specific requirements identified through the 5-step process described in CHAPTER 3. CHAPTER 5 defines the submittal requirements for documenting cybersecurity aspects of control system design.

APPENDIX C provides an overview of the Risk Management Framework as it pertains to control systems. 0 provides additional detail on the Platform Enclave concept. APPENDIX E describes the 5-Level architecture for control systems. APPENDIX F discusses considerations in the integration of critical building systems into a non-critical UMCS. 0 provides guidance for security control families, and individual security controls. APPENDIX H categorizes CCIs by impact and responsibility.

1-6 CYBERSECURITY POINTS OF CONTACT BY SERVICE.

Cybersecurity policies and approaches are evolving, and projects may have unique requirements. Assistance for control system cybersecurity is available from the following Service organizations:

- Army: ICS Cybersecurity Center of Expertise, Huntsville Engineering and Support Center
- Navy: Naval Facilities Engineering Command, Command Information Office (CIO)
- Air Force: Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) ICS Branch, Tyndall AFB
- Marine Corps: Contact Navy POC for Marine Corps POC information.

Note: All requests for support must be initiated by the Contracting Officer's Representative (COR) or, for government-designed projects, by the Project Lead.

1-7 REFERENCES.

APPENDIX A contains a list of references used in this document. The publication date or revision of the code or standard is not always included in this document. In general, when the publication date or revision is not included, the latest available issuance of the reference is used.

1-8 GLOSSARY.

APPENDIX B contains acronyms, abbreviations, and terms.

CHAPTER 2 CONTROL SYSTEM CYBERSECURITY OVERVIEW

2-1 RISK MANAGEMENT FRAMEWORK OVERVIEW.

A summary of key aspects of the Risk Management Framework (RMF) as it applies to control system design is provided here. APPENDIX C contains a more extensive summary of the RMF as it relates to this UFC. It is highly recommended that readers unfamiliar with the RMF review APPENDIX C before incorporating cybersecurity requirements into control system design.

2-1.1 Security Controls.

The RMF relies on the implementation of security controls, where a control is a specific action taken to secure a system. Note that this usage of the word ‘control’ is different from control engineering or control systems engineering, which is the engineering discipline that applies control theory to design systems with desired behaviors. To provide clarity of usage, this UFC will use the term “security control” to refer to cybersecurity controls.

2-1.2 RMF Goal.

The goal of the RMF is to reduce and mitigate vulnerabilities until the risk is acceptable to the System Owner (SO) and Authorizing Official (AO). Under the RMF, risk reduction is not "all or nothing", rather the security solution must reduce risk while considering the constraints of resources and mission requirements. For application of the RMF to control systems, the determination of cybersecurity risk reduction must also account for any additional risks to system functionality due to application of the security controls.

The decision of whether a level of risk is acceptable is made by the assigned government AO. The designer provides input into the risk analysis process by advising on the impact, or lack thereof, of applying security controls to the control system.

2-1.3 Platform Information Technology.

DoD Instructions 8500.01 and 8510.01 define the Risk Management Framework (RMF) for the DoD and establish a category for “special purpose” systems that are not traditional information technology or information systems, called Platform Information Technology (PIT) systems. These PIT systems, including control systems, use specifically tailored security controls sets and require the AO to have expertise in the system.

The selection of the set of security controls to implement for a given system is the responsibility of the AO. The designer provides input into security control selection by advising on the feasibility and potential impacts of applying a security control.

2-1.4 Inherited Security Controls.

An inherited security control is a security control that a system meets by virtue of someone else addressing it in such a way that it applies to the system. A control system will generally inherit security controls one of three ways: by existing within a physical security boundary, by being covered by policies and procedures already in place, or by connection to another system which addresses the security controls.

Since inheritance often requires the SO to coordinate with others, it's critical to document all security controls the control system expects to inherit. During control system design, the designer must identify and document any security controls which are expected to be inherited.

2-1.4.1 Physical Security Inheritance Example.

DoD installations implement physical security to manage risk to an acceptable level. For a control system on a DoD Installation, a security control requiring that members of the public not be allowed unrestricted physical access to components of a control system will be met by virtue of the control system existing within that physical security boundary. Although military installations are on occasion opened to the public for events such as boot camp graduations, the access is not unrestricted, and the level of access has been accepted by installation security. Since control systems are innately tied to and co-located with the physical systems they control, in most cases a control system will be able to inherit physical security from the installation or separately secured facilities.

2-1.4.2 Policy and Procedures Inheritance Example.

The DoD has polices in place governing many aspects of cybersecurity. A control system can therefore inherit a security control such as "the organization defines the frequency to review and update the current security planning policy".

2-1.4.3 Connection to another System Inheritance Example.

When a control system connects to another system, such as an Installation-wide network, inheritance may not be automatic but may require an agreement between the SOs of the systems. Such an agreement would cover acceptable behavior of the control system and explicitly define the security controls that will be inherited from the other system.

2-1.5 Applicability of RMF Security Controls to Design.

Security controls cover a wide range of requirements, many of which must be addressed by someone outside the control system design process. For example, a security control[1] that states "The organization protects the control system from unauthorized modification by members of the organization" is normally not addressed

[1] This is not an actual security control, but rather an illustrative example using a fictitious control.

by the designer; but rather is addressed through policies and procedures put in place by the organization that owns and operates the control system.

2-1.5.1 Applicability of RMF Security Controls to Design of Critical Systems.

The determination of whether a security control should be applied at design can become particularly complex for more critical (higher impact) systems. While it may be sufficient for a LOW impact system to assume a particular security control is addressed by another entity, the designer of a HIGH impact system may need to explicitly address a security control to ensure it is being implemented properly, to apply it at a higher standard, or to provide tools to the responsible parties to assist their implementation of the security control.

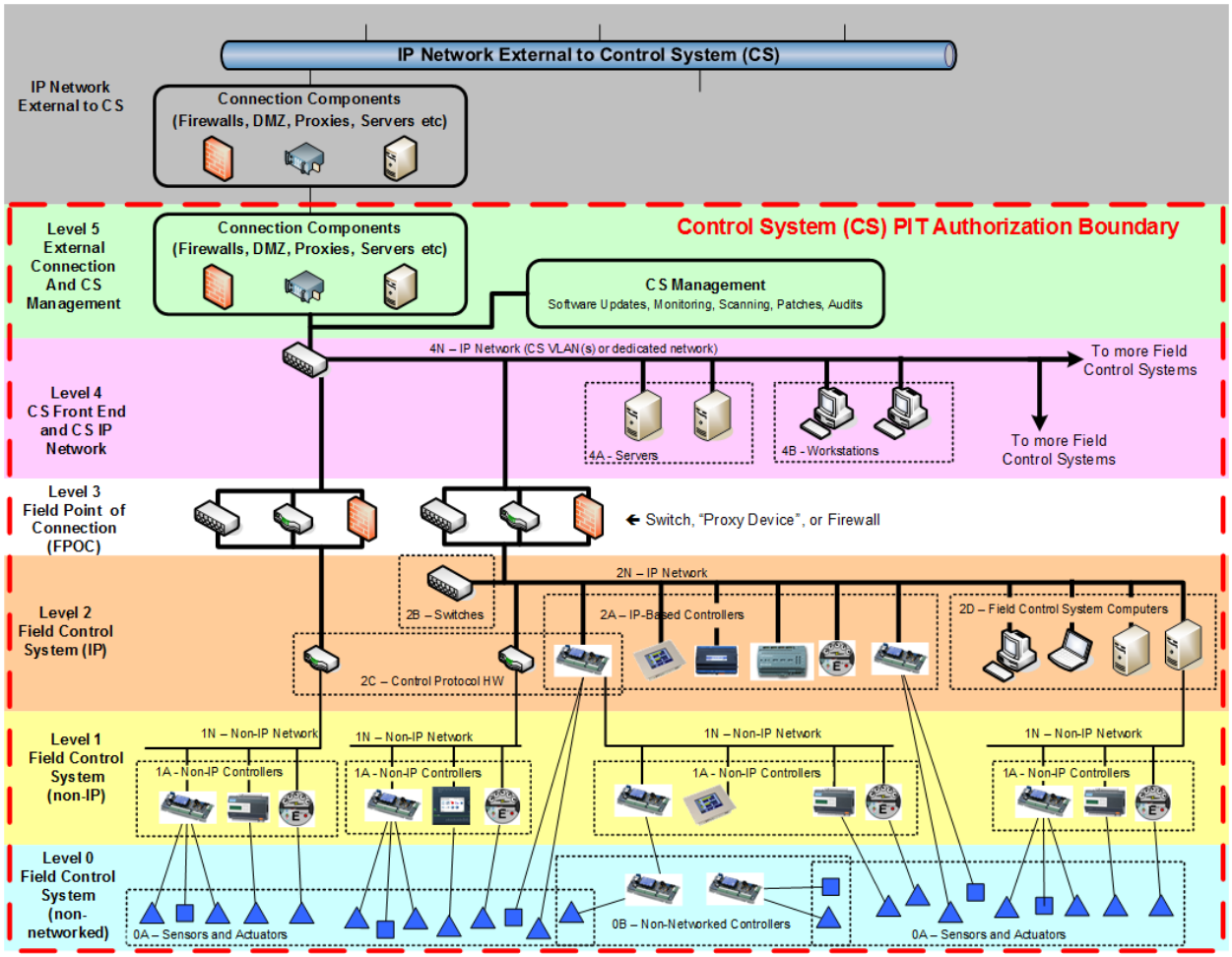
For example, while a security control stating “The organization protects the control system from unauthorized modification by members of the organization” might be addressed through policies and procedures for a LOW impact system, a higher impact system may require the designer to explicitly design in additional barriers to unauthorized modification, or to provide guidance to the organization concerning the importance of properly securing the control system against modification. In this case, however, it’s vital to consider the impact these restrictions may have on the ability to make necessary authorized changes. For this reason, designers of systems with HIGH mission impact should likely seek the assistance of a dedicated cybersecurity engineer. MODERATE systems may also require specialized attention depending on the particular circumstances of the design.

2-2 5-LEVEL CONTROL SYSTEM ARCHITECTURE.

Even though control systems are becoming more like standard IT systems, there remain major differences that must be recognized. The 5-Level control system architecture shown in Figure 2-1 is a framework for describing the system architecture of any control system. This architecture allows distinctions to be made between portions of the control system that look like standard IT, and portions that do not look like standard IT. This is important as many security controls can be applied in the normal fashion to the portion of the control system that looks like a standard IT system, but cannot be applied without modification (or sometimes at all) to the portion that does not look like a standard IT system.

APPENDIX E provides a more in-depth description of the 5-Level control system architecture.

Figure 2-1 5-Level Control System Architecture



2-2.1 "Standard IT" Parts of the Control System.

The parts of the control system that most resemble a standard or traditional IT system are referred to as the "Standard IT" parts:

- The IP Network portion of Level 4 (Level 4N).
- The IP Network portion of Level 2 (Levels 2N and 2B).
- The field point of connection (FPOC) at Level 3.
- The computer hardware for both servers and workstations (Levels 2D, 4A, 4B)
- The computer OS and other standard packages (e.g., antivirus) for both servers and workstations (desktops and laptops) (Levels 2D, 4A, 4B).
- External connections and control system management at Level 5.

The cybersecurity for the "standard IT" parts of the control system are largely addressed using standard cybersecurity practices and are generally outside the scope of control system design, and are not addressed by this UFC. The designer must address the IP

Network at Level 2N, which is generally procured and installed by the control system contractor, and the control system specific software used by the front end, which is generally not adequately covered by standard IT approaches.

2-2.2 "Non-Standard IT" Parts of the Control System.

What makes cybersecurity for a control system challenging is the parts of the control system that do not generally resemble a standard IT system: Level 0, Level 1, Level 2A, Level 2C and the control system applications at Level 2D, Level 4A and Level 4B. These parts of the control system are referred to as the "non-standard IT" parts in order to differentiate them from the "standard IT" parts. Traditional cybersecurity tools and requirements such as vulnerability management alerts, bulletins, Secure Technical Implementation Guides (STIGs) and DoD IT Policies are seldom applicable to these components, particularly to devices at Levels 0, 1 or 2. For example, a security control[2] requiring the screen to be locked when the user leaves the computer is not applicable to devices that do not have a screen or support user login. Different levels of the architecture have different issues related to the application of standard cybersecurity tools and requirements.

Cybersecurity for these portions of the control system must be addressed by the control system designer.

2-2.3 Platform Enclave.

Significant portions of the control system resemble a standard IT system which can be implemented in a standard manner for different control systems, regardless of the details of the control system itself. This has led to the creation of the Platform Enclave concept, which groups the "standard IT" portions of the control system, plus related standard policies and procedures, into an entity which can be handled separately from the rest of the control system. In some cases this Platform Enclave will be separately authorized and the overall control system will have two authorizations, one for the Platform Enclave and one for the Operational Architecture which primarily covers the "non-standard IT" components of the system. In other cases a single authorization will be used for the entire system. Even in cases where a single authorization is used, however, it's helpful to identify and categorize the "standard IT" portions of the control system. More information on the Platform Enclave approach is in 0.

2-3 CONTROL SYSTEM PROCUREMENT OVERVIEW.

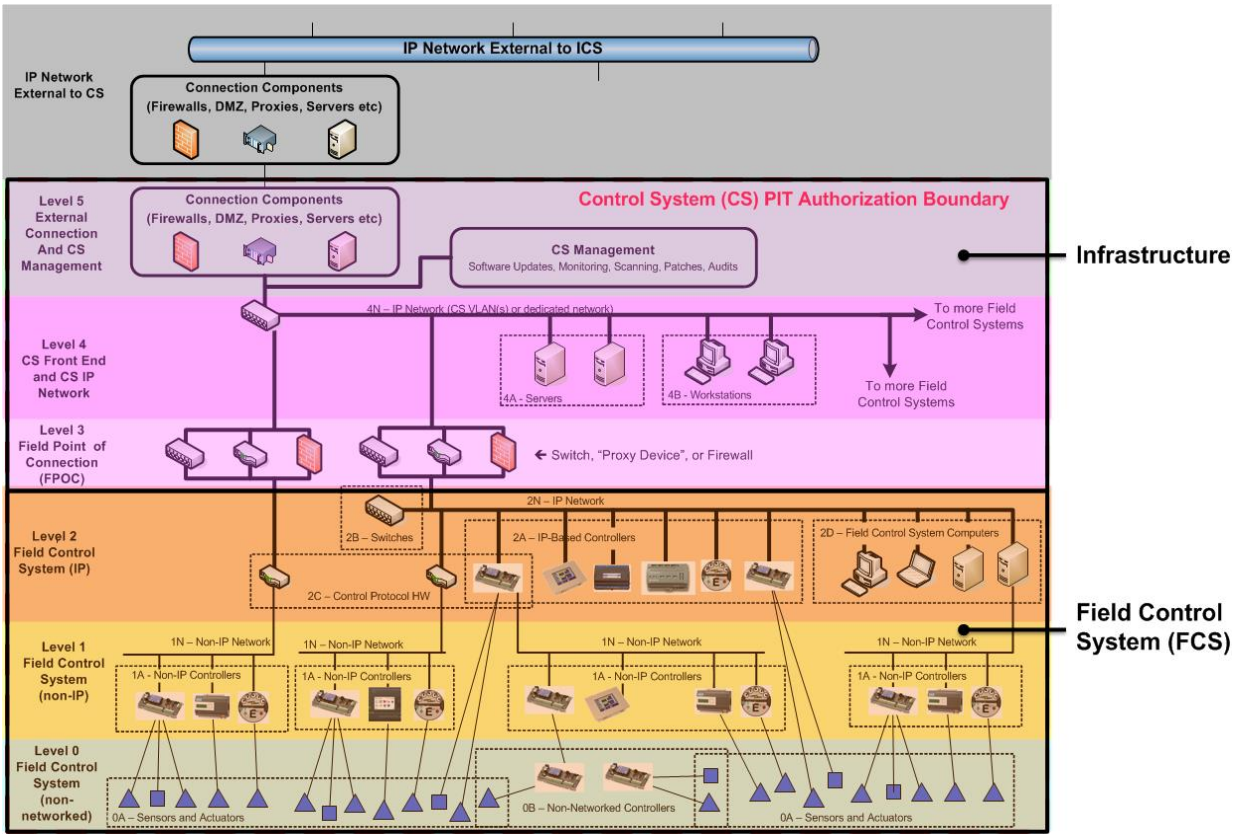
The DoD does not procure most installation-wide control systems as an entire 5-Level system as depicted in Figure 2-1. Typically, some Field Control Systems (FCS; architecture Levels 0, 1 and 2 – see Figure 2-2) are procured with a front end, and over time additional FCS are procured. These additional FCS are integrated with the existing front end, and added to the authorization to operate for the existing system to expand the installation-wide system. When designing a FCS that will be added to an existing system, there may be cybersecurity requirements specific to the authorization of the existing system which must be incorporated into the FCS design. This UFC cannot

[2] For reference – security control AC-11 deals with session lock requirements.

address site-specific requirements; when designing systems which will be added to an existing system authorization coordinate with the project site to obtain relevant requirements from the existing system.

Some control systems are procured to operate independently, with no integration to a larger system and without further significant expansion. Depending on the circumstances and architecture, treat these systems either as complete systems, containing all 4 or 5 Levels, or as a FCS (Level 0-2) with its own user interface at Levels 1 or 2. See Table E-3 in APPENDIX E for more information on the Level 2D computers.

Figure 2-2 Control System Architecture



CHAPTER 3 APPLYING CYBERSECURITY IN DESIGN

3-1 OVERVIEW.

The design of cybersecurity for facility-related control systems is a five step process. In some cases a specific step may be performed by someone other than the designer, but may still require input from the designer. Documentation of cybersecurity-related design decisions and input to others is described in CHAPTER 5.

In addition to requirements specific to Control Correlation Identifier (CCIs), design all control systems according to the minimum cybersecurity design requirements in CHAPTER 4 and cybersecurity requirements otherwise standard for the type of control system being designed.

3-1.1 Five Steps for Cybersecurity Design.

The five steps for cybersecurity design are:

Step 1: Based on the organizational mission and details of the control system, the System Owner (SO) and Authorizing Official (AO) determine the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) for the control system.

Step 2: Use the impact levels to select the proper list of controls from NIST SP 800-82.

Step 3: Using the DoD master Control Correlation Identifier (CCI) list, create a list of relevant CCIs based on the controls selected in Step 2.

Step 4: Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.

Step 5: Include cybersecurity requirements in the project specifications and provide input to others as required.

APPENDIX H contains tables covering steps 2 – 4 for LOW and MODERATE systems, assuming the existence of a Platform Enclave. These tables, with additional information in a filterable format, are also available in Excel format on the RMF Knowledge Service (https://rmfks.osd.mil). This website is CAC-enabled; designers without a CAC must request assistance from the Service if tables and information were not provided. 0 provides additional guidance on the implementation of specific controls.

3-1.2 Definition of "Organization".

Security controls often refer to the "organization" in identifying responsibilities and risk. Unless otherwise indicated, for the purposes of implementation of the RMF to control systems:

- For determining the impact level of a system, treat the “organization” as the relevant Service (e.g., Army, Navy, Air Force).
- For determining implementation requirements for specific controls, treat the “organization” as the Installation (garrison, post or base) or Region (for regional systems). Note that this doesn’t conflict with the above statement regarding the organization for determining impact, but rather indicates the portion of the Service that will have responsibility for implementation of the control.

3-2 STEP 1: DETERMINE CONTROL SYSTEM IMPACT RATING.

The SO, with concurrence from the AO, determines the impact levels of the control system. The SO may seek assistance from the control system designer in defining the functionality of the control system, the information the control system contains, and the impact of failure of the control system. For the DoD, impact levels are determined based on the mission of the relevant Service and in many cases can use the mission criticality rating of the facility (mission support, mission essential, mission critical) as a starting point to determining control system impact. It’s also important to note that while a traditional information system generally prioritizes Confidentiality, then Integrity and lastly Availability, control systems usually prioritize Availability first, then Integrity and lastly Confidentiality.

If impact ratings aren’t provided, request them from the Service. If the Service is unable to provide impact ratings then request direction from the Service and follow one of two courses of action as directed:

1. Use the “starting” impact ratings for the control system type and facility rating (mission support, mission essential, mission critical) from the Control System Master List available at the RMF Knowledge Service website (https://rmfks.osd.mil).

2. Do not proceed with the design until C-I-A Impact ratings are provided.

3-3 STEP 2: DETERMINATION OF SECURITY CONTROLS.

When the list of relevant controls is not provided by the Service, determine a starting list of controls based on the Confidentiality (C), Integrity (I) and Availability (A) impact ratings (or C-I-A ratings) provided by the **1**\Service/**1**/. The DoD uses NIST SP 800-82 as an overlay to determine the starting baseline security controls for control systems. The RMF Knowledge Service (https://rmfks.osd.mil) contains guidance on determining controls from C-I-A ratings, including an Excel Spreadsheet that generates a control list based on the impact ratings and the NIST SP 800-82 guidance. This website is CAC-enabled; designers without a CAC must request assistance from the Service if tables and information were not provided.

3-3.1 Recommend Security Controls to Tailor Out.

The standard security control baselines were developed for standard information systems and contain security controls that are entirely inapplicable to control systems (or other Platform Information Technology), or are prohibitive to implement due to technical or resource constraints. The RMF process allows these baselines to be tailored for the project by the removal or addition of specific controls. Review the list of controls and provide recommendations for controls to be tailored out from (or added to) the security control set as part of the cybersecurity documentation required by CHAPTER 5.

Note this tailoring can either be applied at the security control level during Step 2 or at the CCI level during Step 3 of the design process. For a LOW Impact system, Table H-2 and Table H-3 list recommended CCIs to be tailored out.

3-4 STEP 3: IDENTIFICATION OF CONTROL CORRELATION IDENTIFIERS.

Using the list of security controls from Step 2, create the list of corresponding control correlation identifiers (CCIs). This list of CCIs provides the starting point for identifying cybersecurity requirements to be included in control system design. The complete CCI list is available at the RMF Knowledge Service website via the “Export All Assessment Procedures to Spreadsheet" link at: https://rmfks.osd.mil/rmf/General/SecurityControls/Pages/ControlsExplorer.aspx. From the URL, select "All Control Families" from the "Choose Control Family" pull-down. After the page re-populates with the controls, click on "Export Implementation Guidance and Assessment Procedures" to download the CCIs into Excel.

Note: This website is CAC-enabled; designers without a CAC must request the CCI list from the Service if it was not provided.

3-5 STEP 4: CATEGORIZATION OF CONTROL CORRELATION IDENTIFIERS BY RESPONSIBILITY.

Categorize each CCI identified in Step 3 as one or more of the following categories:

- ***DoD-Defined:*** Either the DoD has provided a value for the “organization selected” values, or the DoD implementation guidance states that the CCI is already met by existing policy or regulation. These values are defined in the CCI list obtained from the RMF Knowledge Service. ***Note that definition or guidance provided may not be relevant for a control system – the organization definitions were determined from the perspective of a traditional information system, not for a control system.***
- ***Designer:*** The designer has a role to address for this CCI. Either the designer needs to provide design specifications to cover a requirement for the control system itself, or the designer must provide input to others regarding the implementation or lack of feasibility of the CCI (typically

because the CCI was written with an IT system, not a control system in mind).

- ***Non-Designer:*** The CCI is beyond the responsibility of the designer, and is the responsibility of someone else – typically the SO. This does not diminish the importance of these CCIs, but as these CCIs are not the responsibility of the designer they are beyond the scope of this UFC.
- ***Platform Enclave:*** The CCI contains a requirement which is expected to be implemented at the Platform Enclave and inherited by the control system, or is mostly implemented at the Platform Enclave but also needed within the field control system (in which case the CCI is also in the "Designer" category). For example, passwords are implemented at the Platform Enclave, but are also necessary at the control system user interface itself, local display panels and some controllers (those which support passwords). While implementation of the Platform Enclave is not the designer's responsibility (a key point of the Platform Enclave is that it is a standard approach that can be implemented across multiple control systems), it's important to document CCIs the control system expects to inherit from the Platform Enclave.

  The Platform Enclave category is in many ways a special case of the Non-Designer category, as it indicates a CCI that is addressed by others.
- ***Impractical:*** The CCI is impractical to fully implement in a control system, but may be applied in a limited manner to at least some part of the control system. In most cases, these are CCIs that can be implemented at Level 4 of the architecture, but would be prohibitively difficult to implement at Levels 0, 1, or 2.

Many CCIs will be assigned multiple categories. For example a security control related to passwords would be categorized in both Platform Enclave and Designer categories as it must be addressed at the Level 4 computers as well as at Level 1 and Level 2. If the DoD has selected a minimum password length for use with this control which cannot be met by all devices, it would also be categorized as Impractical and the designer must document how the security control was implemented for devices unable to meet the DoD selected value.

3-6 STEP 5: INCORPORATE CYBERSECURITY REQUIREMENTS.

In addition to requirements specific to CCIs, design all control systems according to the minimum cybersecurity design requirements in CHAPTER 4 and cybersecurity requirements otherwise standard for the type of control system being designed.

For each CCI identified as "designer", address the CCI in one or more of the following three ways:

- Incorporate a design requirement in the specifications for the control system.

- Select or identify required changes to standard CCI requirements which affect CCI implementation, such as the value of a specific parameter. Note that approval or rejection of these values by the**1**\Service (the AO or their designated representative)/**1**/ will impact control system design.
- Provide information about the design to others so they can implement a CCI. In particular, document CCIs that the system is expected to be inherited from another system or the Platform Enclave.

3-6.1 Addressing DoD Selected Values in CCIs.

Many CCIs have DoD standard values and are indicated in the Master CCI List as being automatically met or inherited based on the standard value. These CCIs have been derived from the general security controls in NIST SP 800-53, without regard to special consideration which might apply to a control system, such as the tailoring and supplemental guidance in NIST SP 800-82. Many of these CCIs cannot be applied to control systems using the approach identified by the DoD. In these cases, implement the CCI to the greatest extent practical, and document the incompatibilities.

3-6.2 Other "Organization Defined Values" in CCIs.

For CCIs which refer to "organization defined values" where the DoD has not defined value and one has not been provided, request appropriate values from the **1**\Service. If the Service/**1**/ is unable to provide values, propose reasonable values and document the proposed value with rationale.

3-6.3 Requirement Definition and Implementation CCIs.

Often, one CCI defines a requirement, and a second requires the implementation of that requirement. A hypothetical example[3] is:

- CCI #1 says "organization defines which components collect audit records". The implementation guidance for this CCI says "this is automatically met because the DoD has defined the components as ***'all components'***".
- CCI #2 says "the information system collects audit records at the defined components".

Together, these create an impossible requirement: if one accepts the definition in #1 (and that it's "automatically met"), then the system fails to meet #2 because, for example, Level 0 sensors can't collect audit records. In this case, both CCIs are "Designer" category; propose reasonable values for CCI #1, implement CCI #2 using this value and document the proposed values for CCI #1.

[3] This example uses simplified fictitious CCIs for illustrative purposes. The AU family of security controls deals with audit logs.

This Page Intentionally Left Blank

CHAPTER 4 MINIMUM CYBERSECURITY DESIGN REQUIREMENTS

4-1 DESIGN TO MINIMIZE FAILURE.

4-1.1 Reduce Dependency on the Network.

Avoid dependence on the network for the execution of control strategies. For example, a backup generator should always start based on a local measurement of utility availability, and not require a network "START" command. When dependence on the network is unavoidable, isolate that portion of the network as much as possible so that non-local network outages do not affect the required portions of the network. When a user interface is absolutely required for the functioning of a control strategy, consider a local interface (local display panel) or a dedicated front end (Level 2 front end) physically co-located with the equipment.

In some cases, it may be necessary to take additional steps to protect critical functions from modification over the network, for example a controller where critical parameters are exposed to network manipulation based on the controller design. In these cases, design barriers to manipulation into the control network architecture itself. See APPENDIX F for one possible approach.

4-1.2 Reduce Extraneous Functionality

Since additional capabilities often result in additional vulnerabilities, a key cybersecurity concept is “least functionality”, which means not adding capabilities which are not specifically needed. Design control system systems to minimize additional functionality which may create vulnerabilities in the control system, including but not limited to:

- Consider mission requirements before implementing remote adjustment of system parameters which are not expected or required to change. For example, a critical air conditioner serving a data center, a critical command and control building, or a UPS room which needs to maintain space temperature at 65 degrees Fahrenheit, 24 hours a day, 365 days a year should not have a network configurable operating schedule or set-point.
- Advanced or complex control strategies often require increased sensor inputs and a greater level of maintenance. Use care when requiring these strategies as the increased complexity results in increased probability of failure if the system is not properly maintained or if any specific parameter is compromised.

4-2 DESIGN TO MANAGE FAILURE.

4-2.1 Design for Graceful Failure.

4-2.1.1 Control Systems without Subsystems.

For control systems controlling a single process or piece of equipment, coordinate with the equipment designer to determine any additional redundancy and failure

requirements, and design the control system to match the requirements for the underlying equipment. In all cases design these systems to fail "safe" as defined by the criteria for the controlled system. For example, in cold climates, outside air intake dampers must fail closed based on the requirements of the heating, ventilation, and air conditioning UFC.

4-2.1.2 Control Systems with Independent Subsystems.

Many control systems are described as a single system but are actually composed of many (hundreds, even thousands) of essentially independent systems. A common example of this would be an installation-wide UMCS, where the air handler (AHU) controllers in one building have no dependence on the AHU in another building, and often no dependence on AHUs in the same building.

For control systems with independent subsystems, design each subsystem as required in paragraph 4-2.1.1, Control Systems without Subsystems, and also design the overall system such that loss of a single subsystem does not affect the operation of the rest of the system. Reduce information shared between subsystems and minimize dependence on the network. For subsystems which must rely on other subsystems define default ("fall back") behavior in the event that the other subsystem fails.

4-2.2 Degraded Operation.

After a system fails to a safe state, it may need to resume operation in a degraded capacity using some automated or manual method, recognizing there may be risk in this operation but that risk is manageable and outweighed by mission requirements.

Based on mission requirements, consider requiring means for manual operation including both monitoring instrumentation (e.g., thermometers, pressure gauges, meters), and manual control devices (such as "hand-off-auto" switches and actuators with manual actuation capability).

4-2.3 Redundancy.

If the criticality of the mission requires redundancy in the design of the control system, then the system must be designed to function without external intervention, and especially without human intervention. Design control strategies such that spare units start automatically when running units shut down, or have all units run and share load. Care must be taken when load-sharing to ensure that operators are notified when one unit of a redundant set fails since the remaining units will automatically pick up the load with no disruption in the load. Do not rely on an operator to start any backup unit; the odds of the operator not being available, or taking an incorrect action are too great. Provide alarms to alert operators of failures.

4-3 DO NOT IMPLEMENT STANDARD IT FUNCTIONS.

As a type of Platform IT, control systems are special purpose systems and must not be used as general computing resources. In particular:

- Do not share control system resources with other systems, particularly with non-PIT systems. Some exceptions such as separate virtual servers running on common hardware or shared Ethernet media with separate VLANs, may be permitted, but the overlap between control systems and other systems must be minimized.
- Do not allow control systems to provide, or share resources with, other applications that provide standard IT services. In particular, do not use control system components as Domain Name System (DNS) servers. (DNS servers may be implemented within the "Platform Enclave" at Level 5, but that is beyond the scope of the control system designer's responsibility and not addressed by this UFC.)
- Do not allow control systems to be publically accessible (i.e., they must require authentication prior to access).
- Prohibit the use of mobile code, except mobile code may be allowed at Level 4. Note that control systems may use mobile code technologies, Java in particular, within the control system, but must not download code without direct user approval.
- Do not use control system computers as standard computers for general applications.
- Do not implement Voice over Internet Protocol (VoIP) within the control system.
- Do not implement collaborative computing devices, technologies or protocols within the control system.
- Unless specifically authorized by the **1**\Service/**1**/ and required by the project site, do not allow control system components to access non-mil IP address space. Do not allow control system components to access social media. (Note that access to non-mil IP address space is generally not needed, and when needed will generally be a function of the front end, not the field control system.)
- Do not allow control systems to receive email (note that at Level 4 they may need a method of sending email for notifications).

4-4 DO NOT PROVIDE REMOTE ACCESS.

Do not provide remote access to the control system. If required, remote access to the Level 4 network should be provided by the Platform Enclave or the site IT organization. Coordinate remote access requirements with the project site IT organization and with the POCs listed in CHAPTER 1.

This Page Intentionally Left Blank

CHAPTER 5 CYBERSECURITY DOCUMENTATION

This chapter describes cybersecurity documentation that is required as part of the control system design package. This documentation is in addition to the documentation required by the relevant control system design criteria.

5-1 OVERVIEW.

Cybersecurity documentation for control system design documents the security controls and CCIs applied to the control system along with assumptions made regarding CCI implementation and information required by others.

5-2 REQUIREMENTS BY DESIGN PHASE.

Cybersecurity documentation requirements are indicated here by typical Design-Build or Design-Bid-Build design submittals. If the design is using a different submittal schedule, adjust accordingly.

The requirements here reference the five step cybersecurity design process defined in CHAPTER 3.

5-2.1 Basis of Design.

Provide a single submittal indicating the C-I-A impact level for the control system and listing the security controls generated during Step 2 along with recommendations and justifications for further tailoring of the security control set.

5-2.2 Design Submittals.

5-2.2.1 Concept Design Submittal (10-15%).

Provide a single submittal indicating the CCIs resulting from the approved tailored security control list (Step 3) and an initial classification for each CCI (Step 4).

5-2.2.2 Design Development Submittal (35-50%).

Provide a single submittal documenting the following:

- The final classification of each CCI (Step 4).
- The changes to standard CCI requirements identified in Step 5, along with an explanation of the changes.
- The CCIs which have been incorporated into the control system design (Step 5). Document changes from standard requirements, or selections made when multiple options are available. Otherwise, it is not necessary to document the details of the requirement, just whether a specific CCI has been incorporated.
- Information for others as required (Step 5)

The recommended format for this submittal is to use the format of **1**\0/**1**/ with the addition of a column to document the required information.

5-2.2.3 Pre-Final Design Submittal (90%).

Provide a submittal updating the Design Development Submittal with complete final information.

5-2.2.4 Final Design Submittal (100%).

Provide a submittal updating the Pre-Final Design Submittal with complete final information.

APPENDIX A REFERENCES

COMMITTEE ON NATIONAL SECURITY SYSTEMS

https://www.cnss.gov/CNSS/issuances/Instructions.cfm

CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*

CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary*

UNITED STATES DEPARTMENT OF DEFENSE

http://www.dtic.mil

Department of Defense Instruction 8500.01, *Cybersecurity*, March 2014

Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014

FEDERAL INFORMATION PROCESSING STANDARDS

http://csrc.nist.gov/publications/PubsFIPS.html

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*

FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

http://standards.ieee.org/findstds/standard/802.1X-2010.htm

IEEE 802.1X, *Port Based Network Access Control*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

http://www.nist.gov/

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015

UNIFIED FACILITIES CRITERIA (UFC)

http://www.wbdg.org/ccb/browse_cat.php?o=29&c=4

UFC 1-200-01, *DOD BUILDING CODE (GENERAL BUILDING REQUIREMENTS)*

UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS)

http://www.wbdg.org/ccb/browse_cat.php?o=29&c=3

UFGS 25 10 10, *UTILITY MONITORING AND CONTROL SYSTEM (UMCS) FRONT END AND INTEGRATION*

APPENDIX B GLOSSARY

B-1 ACRONYMS

B-1.1 General Acronyms

Acronym	Term
ACL	Access Control List
AO	Authorizing Official
BAS	Building Automation System
BCS	Building Control System
CCTV	Closed Circuit Television
CNSSI	Committee on National Security Systems Instruction
CCI	Control Correlation Identifier
COTS	Commercial Off The Shelf
CS	Control System
DoD	Department of Defense
ESS	Electronic Security System
EMCS	Energy Monitoring and Control System
FCN	Field Control Network
FCS	Field Control System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPOC	Field Point of Connection
GFE	Government Furnished Equipment
ICS	Industrial Control System
IDS	Intrusion Detection System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IP	Internet Protocol
IT	Information Technology
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
NIST	National Institute of Standards and Technology
OS	Operating System

Acronym	Term
PIT	Platform Information Technology
PKI	Public Key Infrastructure
SO	System Owner
UCS	Utility Control System
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guide Specification
UMCS	Utility Monitoring and Control System
UPS	Uninterruptible Power Supply
USACE	U.S. Army Corps of Engineers

B-1.2 Security Control Family Acronyms

Acronym	Term
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authorization
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SA	System and Information Integrity

B-2 DEFINITION OF TERMS

Term	Definition
Authorizing Official (CNSSI No. 4009)	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Building Automation System (BAS)	The system consisting of a UMCS Front End, connected Building Control Systems which control building electrical and mechanical systems, and user interfaces for building control supervision. The BAS is a subsystem of the Utility Monitoring and Control System. This term is being phased out in favor of UMCS.
Building Control System (BCS)	A system that controls building electrical and mechanical systems such as HVAC (including central plants), lighting, vertical transport systems, and irrigation systems. Building Control Systems generally do not have a full-featured user interface; they may have “local display panels” but typically rely on the UMCS front end for full user interface functionality. BCS is a subsystem of the Utility Monitoring and Control System, and is a class of Field Control System.
Closed Circuit Television System (CCTV)	An ESS that allows video assessment of alarm conditions via remote monitoring and recording of video events. Video monitoring may also be incorporated into other systems which are not CCTV.
Control Correlation Identifier (CCI)	The Control Correlation Identifier (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise a security control.
Control System (CS)	A system of digital controllers, communication architecture, and user interfaces that monitor, or monitor and control, infrastructure and equipment.
Controller	An electronic device – usually having internal programming logic and digital and analog input/output capability – which performs control functions. Two primary types of controller are equipment controller and supervisory controller.
Distributed Control System	This term is being phased out in preference of BCS, UCS, and/or UMCS.

Term	Definition
Electronic Security System (ESS)	The integrated electronic system that encompasses interior and exterior (physical) intrusion detection systems (IDS), CCTV systems for assessment of alarm conditions, access control systems, data transmission media, and alarm reporting systems for monitoring, control, and display.
Energy Monitoring Control System (EMCS)	Another name for a Utility Monitoring and Control System. See UMCS.
Engineering Tool Software	Software that is used to perform device or network management for a control system, including network configuration, controller configuration and controller programming.
Equipment Controller (EC)	A controller implementing control logic to control a piece of equipment. Note: a controller is defined by use, and many ECs also have the capability to act as supervisory controllers (SC). Some examples of equipment controllers are air handler controllers, protective relays, and pump controllers. Note that some devices, such as power meters or smart sensors, which only perform monitoring functions are still considered equipment controllers (despite not actually controlling anything).
Facility-Related Control System	A control system which controls equipment and infrastructure that is part of a DoD building, structure, or linear structure.
Field Control System (FCS)	A Building Control System, Utility Control System, Access Control System, etc. within the Facility and "downstream" of the FPOC.
Field Control Network (FCN)	The network used by the Building Control System, Utility Control System, etc., within a facility "downstream" of the FPOC. This includes IP, Ethernet, RS-485, TP/FT-10 and other network infrastructure that support control system(s) in a given facility.
Field Point of Connection (FPOC)	The FPOC is the point of connection between the control system IP network and the field control network (an IP network, a non-IP network, or both). The hardware which provides the connection at this location is an IT device such as a switch, IP router, or firewall.
[UMCS, ESS, etc.] Front End	The portion of the control system consisting primarily of IT equipment, such as computers and related equipment, intended to perform operational functions and run monitoring and control/engineering tool application software. The front end does not directly control physical systems; it interacts with them only through field control systems (FCS). The front end is a component of the [UMCS, ESS, etc.] infrastructure (see definition).

Term	Definition
Impact	The effect on organizational operations, organizational assets, or individuals due to a loss of Confidentiality, Integrity, or Availability in the control system. Impact is categorized as one of three levels: • LOW: limited adverse effect • MODERATE: serious adverse effect • HIGH: severe or catastrophic adverse effect The impact level of a system is generally written in ALL CAPS for clarity.
Incident (FIPS PUB 200)	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
Industrial Control System (ICS)	One type of control system. Most specifically a control system which controls an industrial (manufacturing) process. Sometimes also used to refer to other types of control systems, particularly utility control systems such as electrical, gas, or water distribution systems.
Information System (CNSSI No. 4009)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
[UMCS, ESS, ...] Infrastructure	The portion of a control system (such as a UMCS or ESS) which includes all components that are not part of a field control system. These components include the FPOC, the Platform Enclave, and the front end (i.e., its architecture Levels 3, 4 and 5)

Term	Definition
Intrusion Detection System (IDS) [Physical/ESS]	A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.
Intrusion Detection System (IDS) [Cyber]	A device or software application that monitors network or system activities for malicious activities or policy violations, and produces reports to management.
Least Privilege (CNSSI No. 4009)	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
Mobile Code (NIST SP 800-53r4)	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technology (NIST SP 800-53r4)	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript)
Non-Local Maintenance (NIST SP 800-53)	Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.
Operational Architecture (OA)	Those components of a control system that represent the purely operational components of the system such as controllers, Front End software, and other devices which support operational functions. When the “Platform Enclave” approach to authorizing a control system is used, the “non-standard IT” portions of the control system are authorized as the Operational Architecture and the overall system has two authorizations: Platform Enclave and Operational Architecture.
[UMCS, ESS, ...] Platform Enclave	Those components of the control system that are standard IT components and can be secured in a standard manner independent of the type of control system. These components serve only the control system and include the IP network, network management and security devices (e.g., switches, routers), software, computers and/or other devices which provide management and security of the network.
Platform IT (PIT)	IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Term	Definition
Remote Access (NIST SP 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet).
Risk (NIST SP 800-53)	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Management (NIST SP 800-53)	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Supervisory Control and Data Acquisition (SCADA)	This term has a variety of meanings depending on context, and is therefore not used in this UFC. BCS, UCS and UMCS are used instead, as they are more precise and less ambiguous.
Supervisory Controller	A controller that implements a combination of supervisory logic (global control or optimization strategies), scheduling, alarming, event management, trending, web services or network management. A supervisory controller may be located between the Platform Enclave and the field control system as the data aggregation conduit between the FCS and the front end. Note that this arrangement is defined by use; many supervisory controllers have the capability to also directly control equipment, and serve the role of both supervisory controller and equipment controller.
System Owner (SO) (CNSSI No. 4009)	Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

Term	Definition
Utility Control System (UCS)	A type of field control system used for control of utility systems such as electrical distribution and generation, sanitary sewer collection and treatment, water generation and pumping, etc. Building controls are excluded from a UCS, however it is possible to have a Utility Control System and a Building Control System in the same facility, and for those systems to share components such as the FPOC. A UCS is a subsystem of a Utility Monitoring and Control System (UMCS) and is a class of Field Control System (FCS).
Utility Monitoring and Control System (UMCS)	The system consisting of one or more building control systems and/or utility control systems and the associated UMCS Infrastructure. In other words, it is the complete utility monitoring system – from the front end to equipment controllers. At the highest level the UMCS is composed of a UMCS Platform Enclave and UMCS Front End (jointly referred to as UMCS Infrastructure), and connected Field Control System(s).
Vulnerability (NIST SP 800-53)	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX C RISK MANAGEMENT FRAMEWORK (RMF) OVERVIEW

C-1 RMF OVERVIEW

As defined by the National Institute of Standards and Technology (NIST), the RMF is "The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.". The RMF details how Risk Management is applied to Department of Defense (DoD) information technology in accordance with DoDI 8510.01.

C-2 RMF PROCESS

As shown in Figure C-3, the RMF is a six-step process:

1. Categorize the System: Categorization of the control system by Confidentiality, Integrity and Availability (C-I-A) Impact levels, taking into consideration both the importance of the mission and the importance of the control system to the mission. Determination of the C-I-A Impact levels will be made by the System Owner (SO) and is outside the scope of this UFC.

2. Select Security Controls: Based on the C-I-A level, a set of controls and an overlay to be implemented will be selected from CNSSI No. 1253 and NIST SP 800-82. In many cases, these controls will be further tailored based on the requirements of the Control System prior to implementation. While this UFC includes guidance concerning applicability of specific controls, the process of selecting security controls is generally outside the domain of the designer.

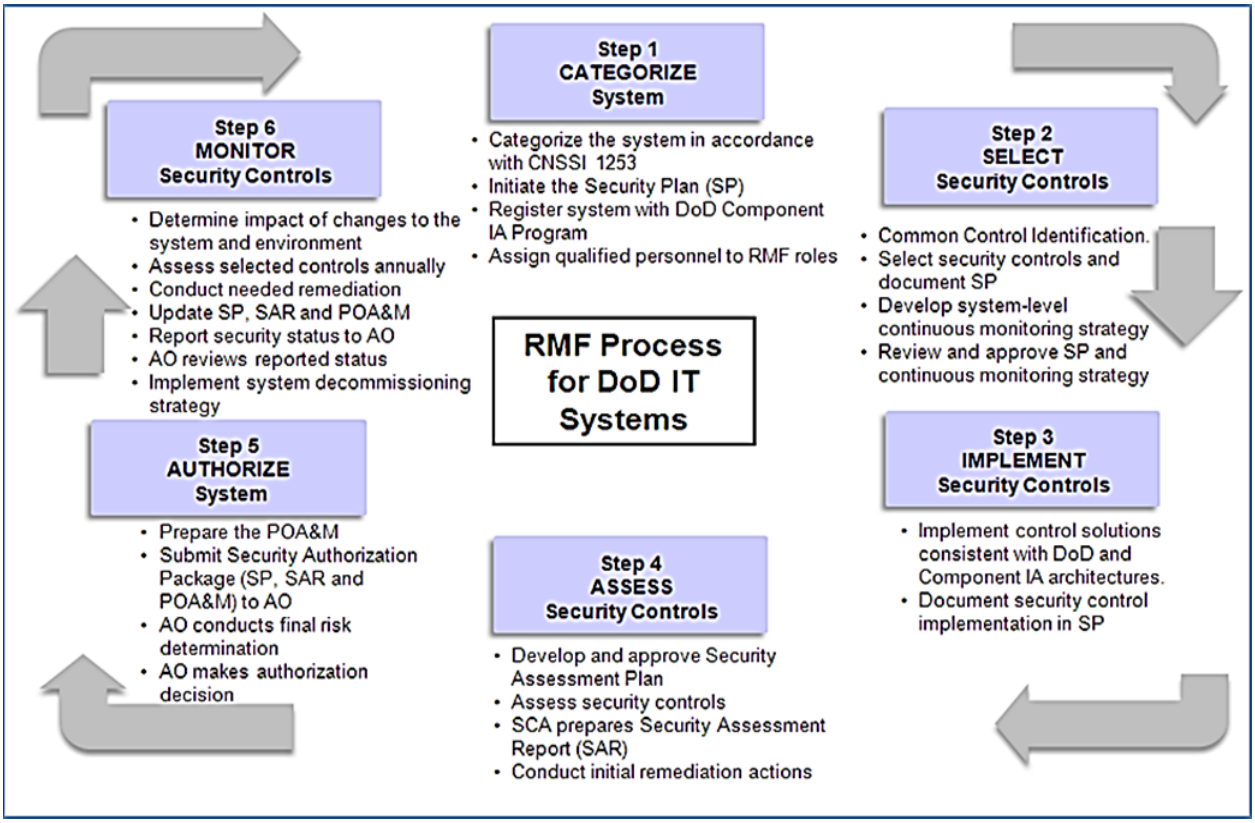
3. Implement Security Controls: Implementation of many security controls will be outside the scope of designer responsibilities. This UFC focuses on security controls which the designer must somehow address in design, generally through the incorporation of requirements into the plans and drawings, and on security controls which others may ask the designer to provide input on.

4. Assess Security Controls: After implementation, the effectiveness of the implementation is evaluated.

5. Authorize the System: Assuming a satisfactory evaluation, the Authorizing Official (AO) formally accepts the residual risk from the control system and authorizes operation of the system by issuing an authorization to operate.

6. Monitor Security Controls: The RMF enters a monitoring and evaluation phase, where the control system is monitored and periodically re-evaluated.

Figure C-3 NIST Risk Management Framework Steps



C-3 DEFINITION OF CONTROLS FROM NIST AND DODI 8510

C-3.1 Control Families

Since it is difficult to evaluate a performance requirement ("reduce risk below a specific level"), NIST provides a catalog of prescriptive requirements where meeting a particular requirement reduces the overall risk to the system. These requirements are broadly categorized into the following groupings (which are often referred to as "control families"):

- AC – Access Control
- AT – Awareness and Training
- AU – Audit and Accountability
- CA – Security Assessment and Authorization
- CM – Configuration Management
- CP – Contingency Planning

- IA – Identification and Authorization
- IR – Incident Response
- MA – Maintenance
- MP – Media Protection
- PE – Physical and Environmental Protection
- PL – Planning
- PM – Program Management
- PS – Personnel Security
- RA – Risk Assessment
- SA – System and Services Acquisition
- SC – System and Communications Protection
- SI – System and Information Integrity

C-3.2 Control Elements and Enhancements

Within each control family, there are numerous controls; most having multiple sub-elements. Many controls also have enhancements, additional actions that can be taken to enhance the effectiveness of the control. Individual controls are assigned a number within the control family, enhancements are sub-numbered, and elements of controls or enhancements are lettered. Enhancements and elements are written in parenthesis after the control number. An example of NIST SP 800-53 AC-2 is shown in

Figure C-4.

Figure C-4 NIST SP 800-53 Control AC-2

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:
Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
b. Assigns account managers for information system accounts;
c. Establishing conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
g. Monitors the use of information system accounts;
h. Notifying account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance: Information system account types include, for example, individual, shared,…[4]
Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, PL-4, SC-13.

Control Enhancements:

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT[4]
The organization employs automated mechanisms to support the management of information system accounts.

(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS[4]
The information system automatically [*Selection: removes; disables*] terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS
The information system automatically disables inactive accounts after [*Assignment: organization defined time period*].

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS[4]
The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies [*Assignment: organization-defined personnel or roles*].

(5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT[4]
The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

[4] For sake of brevity, complete 'Supplemental Guidance' text is not shown for AC-2 ACCOUNT MANAGEMENT.

(6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT[4]
The information system implements the following dynamic privilege management capabilities: [*Assignment: organization-defined list of dynamic privilege management capabilities*].

(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES[4]
The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
(b) Monitors privileged role assignments; and
(c) Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION[4]
The information system creates [*Assignment: organization-defined information system accounts*] dynamically.

(9) [4]ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS
The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

(10) ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION
The information system terminates shared/group account credentials when members leave the group.

(11) ACCOUNT MANAGEMENT | USAGE CONDITIONS[4]
The information system enforces [*Assignment: organization-defined circumstances and/or usage conditions*] for [*Assignment: organization-defined information system accounts*].

(12) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE[4]
The organization:
(a) Monitors information system accounts for [*Assignment: organization-defined atypical usage*]; and
(b) Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

(13) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS[4]
The organization disables accounts of users posing a significant risk within [*Assignment: organization-defined time period*] of discovery of the risk.

In this notation, AC-2 (5) is enhancement 5: "The organization requires that users log out when….".

C-3.3 Control Correlation Identifiers

The DoD implementation of the NIST controls for control systems is DoDI 8500. The DoD took the additional step of breaking down each control and control element into specific actions; each action is identified by a unique Control Correlation Identifier (CCI). For example, the above control, AC-2, is broken down into 61 separate CCIs, with 11 distinct CCIs for AC-2 (4) alone.

While this leads to a very fine level of implementation (the control system could audit account creation, but not audit account modification), it also leads to many dependencies between CCIs. For example, two of the CCIs associated with security control AC-2(4) found on the RMF Knowledge Service (Security Control Explorer) are:

- CCI-000018: “The information system automatically audits account creation actions.”
- CCI-001683: “The information system notifies organization-defined personnel or roles for account creation actions.”

Note: The RMF Knowledge Service website is https://rmfks.osd.mil.

While these are written as independent CCIs, they are clearly closely related and it is difficult to imagine a notification system that did not include an auditing capability.

C-4 REQUIREMENT DEFINITION VS IMPLEMENTATION

Broadly speaking, CCIs can be categorized into requirement definition and requirement implementation.

1. A CCI defines a requirement when the CCI is of the form “<someone> defines a <requirement>”. Examples of CCIs that define a requirement include those that state “The organization defines ….”

   a. “…a minimum level of detail for documentation”,

   b. “…a minimum frequency to review some criteria”,

   c. “…a list of events that raise a red flag for security”, or

   d. “…a policy or procedure for modifications to the control system”

2. A CCI implements a requirement when the CCI is of the form “<someone/something> meets a <requirement>”, where the requirement is typically defined in a related CCI. Examples of CCIs which implement a requirement defined in the previous example include CCIs that state “The organization ….”

   a. …obtains the required level of documentation”,

   b. …reviews a security plan annually”,

   c. …responds to breaches of physical security”, or

   d. …approves changes to the control system via a configuration management board”

C-4.1 CCIs Defining a Requirement

CCIs which define a requirement may be addressed by the designer, but are often addressed by the organization or already defined DoD-wide. In some cases, the final statement of the requirement may be by the organization, but with input from the designer based on knowledge of the control system and the specific vulnerability to be addressed. For example, the designer needs to provide input on password complexity

since not all control system components will support passwords, and those that do may support different complexities. In many cases, DoD-defined requirements are completely inappropriate for control systems and the designer must document deviations from the DoD definitions for these requirements in the design.

C-4.2 CCIs Requiring Implementing a Requirement

Implementation CCIs may further be classified by who/what does the implementation: the organization (or inherited from some other element) or the control system. "The organization conducts background checks" is an example of the former while "the control system logs users off after a period of inactivity" belongs to the latter. In some cases, this is not clear – a CCI that states "The organization enforces a minimum password length"[5] appears to create a requirement on the organization, but a moments consideration will make clear that this action must be implemented by the control system (since the control system either accepts or rejects a password entry), not the organization. CCIs that are implemented by the organization are not addressed by the designer and are outside the scope of this UFC. On the other hand, CCIs that are implemented by the control system must typically be addressed by the designer since implementing a CCI becomes a performance requirement in the specification of the control system.

C-5 PLATFORM INFORMATION TECHNOLOGY

The DoD implementation of the RMF defines Platform Information Technology (PIT) as "IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems", and differentiates PIT systems from standard information systems. Most specifically, DoDI 8500.01 indicates that PIT Systems "require uniquely tailored security control sets and control validation procedures and require security control assessors and AOs with specialized qualifications"

The Cybersecurity of PIT systems, such as control systems, requires not only the use of customized control baselines, but also further tailoring of controls as appropriate for the specific control system.

[5] This is not the text of an actual CCI, but rather a simple fictitious example used for illustrative purposes.

This Page Intentionally Left Blank

APPENDIX D PLATFORM ENCLAVE

D-1 PLATFORM ENCLAVE CONCEPT OVERVIEW

The fact that a significant portion of the control system resembles a standard IT system which can be implemented for different control system regardless of the details of the control system itself has led to the creation of the Platform Enclave concept. This concept groups the standard IT portions of the control system into a system which can be handled separately from the rest of the control system. In some cases this Platform Enclave will be separately authorized and the overall control system will have two authorizations, while in other cases a single authorization will be used for the entire system. Even in cases where a single authorization is used, however, it's helpful to identify and categorize the standard IT portions of the control system.

D-2 PLATFORM ENCLAVE USING TWO AUTHORIZATIONS

A primary reason to define to a Platform Enclave is to enable the approach where a control system is implemented using ***two*** Risk Management Framework authorizations, one for the Platform Enclave and one for the non-Platform Enclave portions of the control system, sometimes referred to as the "non-standard IT" portions. While this may seem to lead to a duplication of effort, in practice this generally isn't the case:

- While many controls, such as policies and procedures, will need to be done at both the Platform Enclave and "non-standard IT" portions, these policies and procedures can often be inherited by both from another Authorization, or implemented the same way in both the Platform Enclave and the "non-standard IT".
- Some controls can be applied at the Platform Enclave and then inherited by the "non-standard IT". For example, controls related to remote access can be defined independently of the "non-standard IT" by the Platform Enclave, and then inherited by the "non-standard IT" if necessary.
- While some controls will need to be addressed by both the Platform Enclave and the "non-standard IT", they will need to be addressed differently, and often to a different extent, in each.

D-3 PLATFORM ENCLAVE BENEFITS

The primary benefit of the Platform Enclave approach is that it allows for separation of the "standard IT" and "non-standard IT" components of the control system, and allows for a single authorization for the IT portion to cover multiple control system types. This approach is most beneficial when there is an existing network and cybersecurity infrastructure on which to establish the Platform Enclave, such as those that exist on the majority of DoD installations. Ideally, the Platform Enclave will be a standard established and authorized by each Service for implementation at every installation, in contrast to the authorization for the "non-standard IT" portion of the control system (the "Operational Architecture"), where factors such as control system type, vendor and protocol are more likely to make each authorization unique and non-standard.

D-4 ARMY PLATFORM ENCLAVE APPROACH

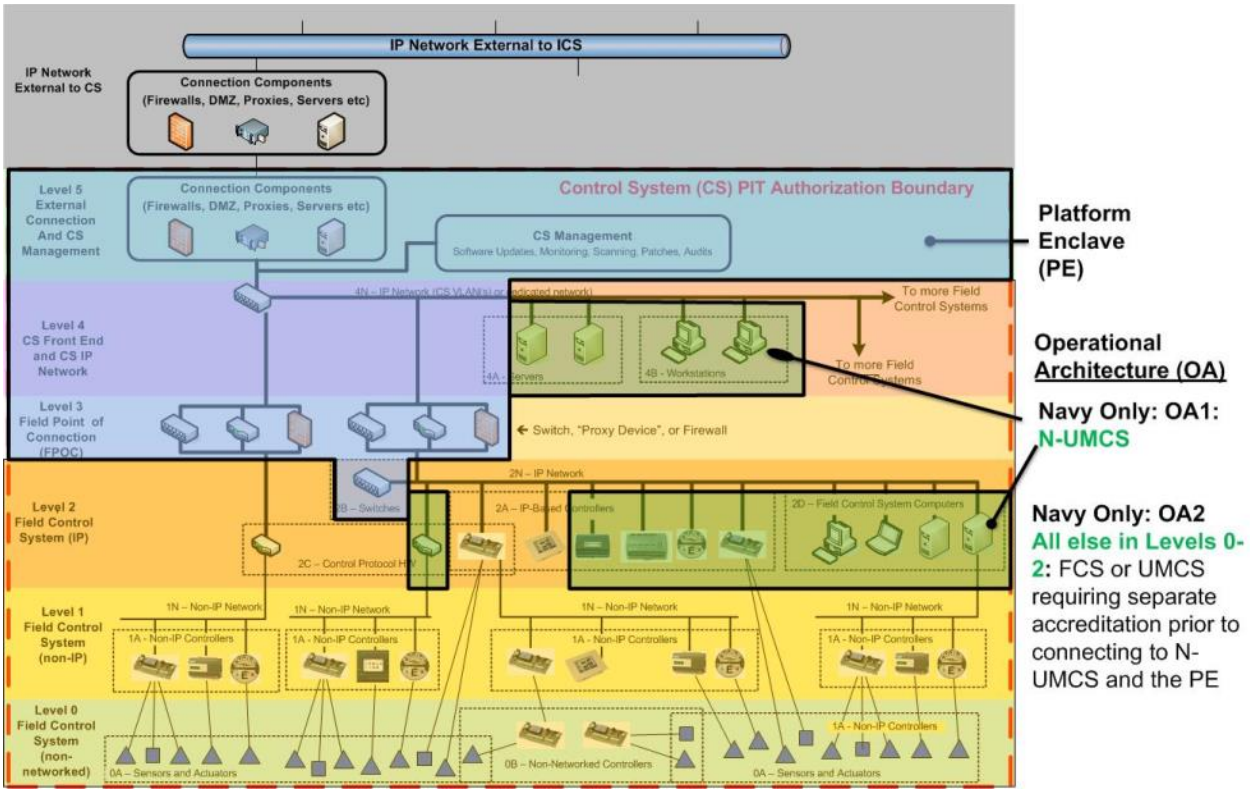
The Army has not formalized a Platform Enclave approach.

D-5 NAVY PLATFORM ENCLAVE APPROACH FOR BCS AND UCS

Figure D-1 shows which components of the 5-Level control system architecture are included in the Navy's Platform Enclave (PE) called the Control System Platform Enclave (CS-PE). The Navy's CS-PE is implemented at and has a presence today at Navy installations. The Navy is deploying an operational architecture (OA) called the Navy Utilities Monitoring and Control System (NUMCS), which is also shown in Figure D-1.

All Control Systems must connect to the Platform Enclave, and must either be separately authorized or fall under the type accreditation of the CS-PE and NUMCS.

Figure D-1 Navy and Air Force Platform Enclave and Operational Architecture



D-6 AIR FORCE PLATFORM ENCLAVE APPROACH

Figure D-1 shows which components of the 5-Level control system architecture are included in the Platform Enclave and Operational Architecture sections. The Platform Enclave section shall be archetype (type-accredited) by the authority of the Air Force Industrial Control System Platform Information Technology Authorizing Official (AF ICS PIT AO). Additionally when feasible and to the greatest extent possible, the Operational Architecture section shall also be archetype across the Air Force by authority of the AF

ICS PIT AO. Finally, the Operations Center (Level 4a-Servers and 4b-Workstations) will eventually be standardized through AF ICS standardization.

Referring to Figure D-1, the Operational Architecture (yellow section), which contains specific “standard IT” and “non-standard IT” components and systems exclusive and unique to the control system operations and maintenance, shall be ASSESS-ONLY under the RMF process by the AF ICS PIT SCA. However, the Platform Enclave (blue section); which contains AF-enterprise IT network components, subsystems, and systems; is governed by AFCYBER and exists as part of the AF Network. Therefore control systems that either join the AF Network or utilizes its IT backbone infrastructure for data-at-rest or data-in-transit, the AF ICS PIT AO shall assess and authorize the Platform Enclave using the full RMF process.

This Page Intentionally Left Blank

APPENDIX E 5-LEVEL CONTROL SYSTEM ARCHITECTURE

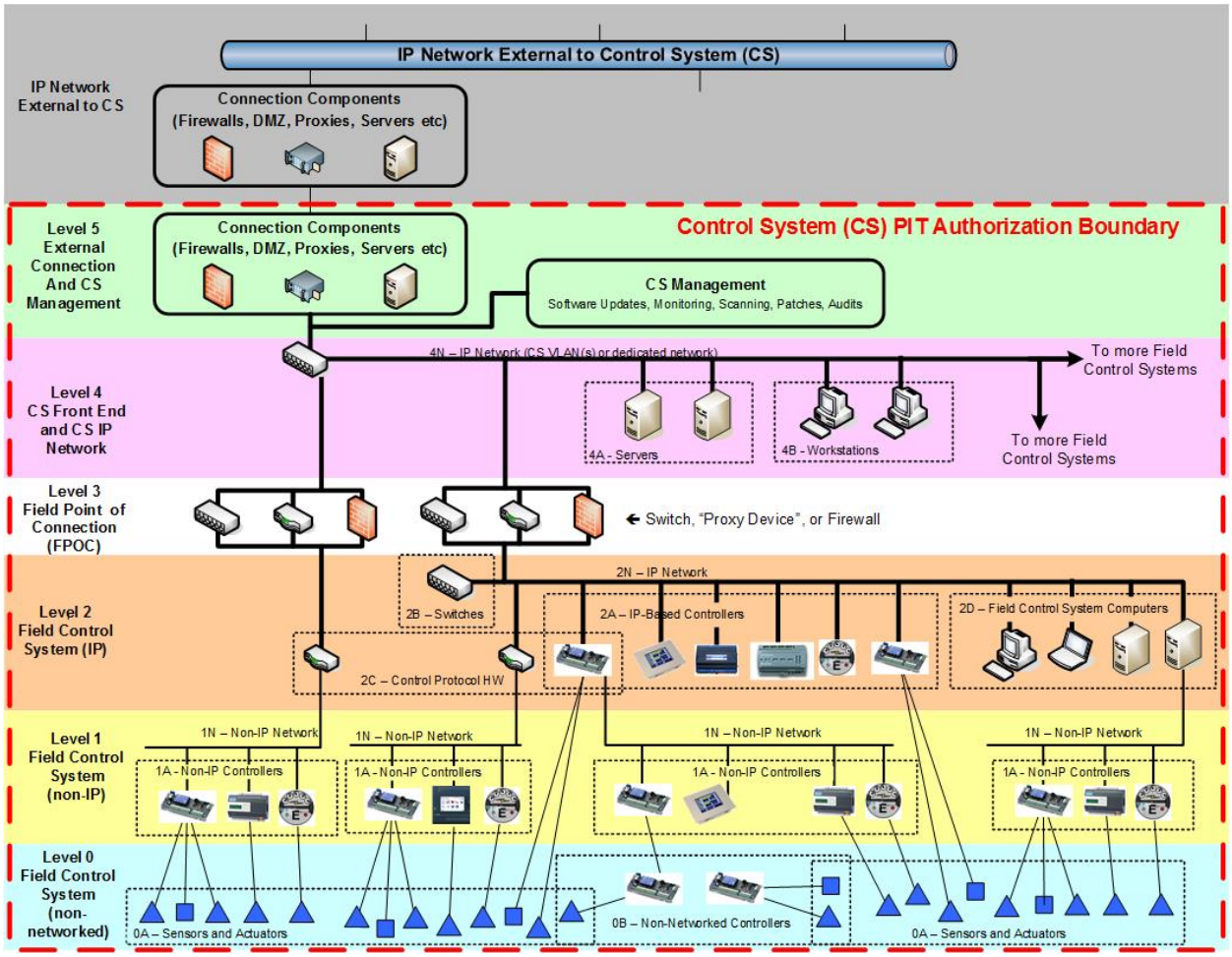
E-1 INTRODUCTION

As shown in Figure E-1, control systems are represented as a 5-Level architecture, where each level represents a collection of components that are logically grouped together by function and which generally share a cybersecurity approach. This architecture is defined as a general architecture suitable for a wide range of control systems, thus there are some key considerations when using it to describe a specific control system:

- Not every implementation of a control system will make use of every level, or every type of component shown at a level.
- The same device may reside in different levels, depending on its configuration. For example, some controllers may support different networks based on onboard switches, and thus the same device could reside in either Level 1 or Level 2.
- In many cases, a device will fit multiple sub-levels within the same principal level, usually within Level 2. For example, a Level 2A controller may act as a Level 2C router to a Level 1 network beneath it.

This Appendix describes the 5-Level architecture for control systems and presents cybersecurity considerations for each level. Note that although there are actually more than five levels in the architecture shown in Figure E-1, it is commonly referred to as the “5-Level Control System Architecture”. This architecture applies to all control system types; while many of the example components or technologies included in this Appendix are based on building or utility control systems this is not meant to imply that this architecture is specific to these types of control systems.

Figure E-1 5-Level Control System Architecture



E-2 5-LEVEL ARCHITECTURE OVERVIEW

A brief description of each Level (from simple to complex devices) is:

Level 0. Non-networked devices which communicate using analog signals. These include ("dumb") sensors and actuators as well as non-networked controllers (including their dedicated sensors and actuators). These communicate with Level 1 via hardware I/O (Analog and Binary signals).

Level 1. Networked controllers not on an IP network (e.g., BACnet MS/TP, RS-485 (e.g., DNP, Modbus), LonWorks TP/FT-10).

Level 2. Networked controllers on an IP network.

Level 3. The Field Point of Connection (FPOC), which is a connection between the field control system IP network at Level 2 and the Level 4 IP network.

Level 4. The site-wide IP network used for the control system, along with front end servers and workstations (desktops and laptops).

Level 5. Interfaces to “external” networks (IP networks other than the control system network).

Note that some levels contain sub-levels as indicated in Figure E-1.

E-3 LEVEL 0: SENSORS AND ACTUATORS

Level 0 consists of non-networked devices which communicate using analog signals. These include (“dumb”) sensors and actuators, as well as non-networked controllers. These communicate with Level 1 or Level 2 via hardware I/O (Analog and Binary signals). Details for Level 0 are shown in Table E-1.

Table E-1 Level 0

LEVEL 0: Sensors and Actuators	
Definition	Level 0 devices lack a network and therefore cannot be attacked over a network. Level 0 devices, if they communicate at all, use only simple analog and binary signals, they do not use any form of digital protocol for communication. A sensor or actuator that uses a communications protocol (e.g., Zigbee, Bluetooth) is a Level 1 (non-IP) or Level 2 (IP) device.
Functional Description	The interface between the control system and the underlying controlled process / equipment where electrical signals in the control system get converted to/from physical values and actions in the underlying controlled system. Level 0A consists of Sensors and actuators Level 0B consists of non-networked controllers and their integral sensors and actuators. Level 0B devices may have some intelligence and may even have an internal network, but the device does not expose any internal network to other devices. These devices are typically packaged units with factory-installed integral controllers. Note that a “stand-alone” built-up unit with multiple field installed controllers which communicate over a network specific to that unit is NOT a Level 0 component, but rather a stand-alone field control system of its own.

LEVEL 0: Sensors and Actuators	
Implemented Via	Devices which: • Convert physical properties (e.g., temperature, pressure, etc.) to a binary or analog electrical signal • Take a binary or analog electrical signal and produce a physical action (e.g., open / close a valve or damper, etc.) These electrical signals are purely binary or analog – there are no exposed digital signals or networks at this level. Also note that "smart" sensors or “smart” actuators which include a controller and network connection are considered to be Level1 or Level 2 devices.
Installed By	Controls contractor during installation or renovation of underlying mechanical or electrical system.
Example Components	The vast majority of these devices are very simple (“dumb”) sensors or actuators, but more complex equipment may be at level 0 – as long as it lacks a network connection. Some examples are: • A thermistor temperature sensor which simply provides a changing resistance as an indication of temperature is a Level 0A device. • An electric actuator which takes a 4-20 mA signal and produces a proportional physical response is a Level 0A device. • An occupancy sensor which uses BACnet to communicate occupancy values is a Level 1 (or Level 2) device, ***not*** a Level 0 device. • A variable frequency drive controlling an air handler fan and using only binary and analog signals to communicate with the air handler controller is a Level 0B device. • A flow sensor using HART over an analog wire is using a digital protocol (HART) and is a Level 1 device, ***not*** a Level 0 device. • A packaged diesel generator operating in a stand-alone configuration – again with no network connection to other devices - is a Level 0B device. The last two examples illustrate that the defining characteristic for Level 0 is not the complexity of the device, but rather whether the device communicates with other devices using a network.

LEVEL 0: Sensors and Actuators	
Security Control Considerations	In general, management and operational controls such as physical security and access control may still apply to this level. These devices are physically attached to the mechanical/electrical system and physical security is dictated and implemented based on the physical access to the equipment. Utility vaults, Mechanical, Electrical, Plumbing rooms, Pump Stations, etc. should be secure and only authorized personnel should have access. These devices, while they do not have network communication, can cause physical damage, for example a valve left in the “Open” position.

E-4 LEVEL 1: FIELD CONTROL SYSTEM (NON-IP)

Level 1 contains networked controllers not on an IP network (e.g., BACnet MS/TP, RS-485 (e.g., DNP, Modbus), LonWorks TP/FT-10). Details for Level 1 are shown in Table E-2.

Table E-2 Level 1

LEVEL 1: Field Control System (non-IP)	
Definition	That portion of the controls network which does not use the IP protocol. This includes both the controllers themselves (Level 1A) and the network (Level 1N).
Functional Description	(Level 1A) This is where the control logic resides and gets converted to or from binary and analog electrical signals, as well as the portion of the control system where: • Analog and binary electrical signals (from sensors) get converted to digital signals via analog-to-digital (A-D) converters. • Digital information is converted to analog and binary electrical signals (to actuators) via digital-to-analog (D-A) converters. • Digital information is transmitted and received over a network. • Digital information is processed according to a user-defined sequence to generate new digital information. • Devices may incorporate integral Level 0 sensors and actuators, for example, many variable air volume (VAV)

LEVEL 1: Field Control System (non-IP)	
	box controllers incorporate an electric actuator. Not all controllers will have hardware inputs. While there is exchange of data over the network, good design practice dictates that most of the data processing occurs using local sensor data and local actuator outputs; the system is designed to minimize dependence on networked data. (Level 1N) The Level 1 network (media and hardware) does not use IP. It uses a variety of media at Layers 1 and 2 (some standard, some not) and it uses Layer 3 protocols other than IP. Some examples are: • BACnet over MS/TP, or BACnet over ARCnet • LonTalk over TP/FT-10 or LonTalk over TP/XF-1250 • Modbus over RS-485 For this reason, it is generally very specific to the control application and cannot be used for "standard" IT protocols and applications.
Implemented Via	(Level 1A) Controllers, typically equipped with multiple analog and binary inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in random access memory (RAM), processing power, and network input/output (I/O). In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware. (Level 1N) The network media and hardware is similarly dedicated to that specific control protocol, and is made by a variety of vendors.
Installed By	Controls contractor during installation or renovation of underlying mechanical or electrical system. Generally during new building construction or major renovation.
Example Components	VAV box controllers Networked (non-IP) electric meter Intelligent (networked) thermostat LonWorks TP/XF-1250 (media) to TP/FT-10 (media) router. (This is not an IP router, but routes the control system protocol at Open Systems Interconnection layer 3.)
Security Control	Since devices (controllers) in this tier tend to be simpler devices,

LEVEL 1: Field Control System (non-IP)	
Considerations	often few security controls can be applied, particularly after the system has been designed and installed. Some basic controls/measures that can be applied at this tier include: • Disabling (or at a minimum prohibiting) secondary network connections (connections other than to the Level 1 network) • The use of passwords on devices such as displays (to the capability supported by the device – many of which do not permit 14 character passwords, for example) • The application of physical security measures – which will be dictated and implemented by the underlying equipment

E-5 LEVEL 2: FIELD CONTROL SYSTEM (IP)

Level 2 consists of networked controllers on an IP network. Details for Level 2 are shown in Table E-3.

Table E-3 Level 2

LEVEL 2: Field Control System (IP)		
Definition		The portion of the control system which uses IP but is not shared with any other system. "Shared" in this context primarily refers to physical equipment and media.
Functional Description	2A	This Level (along with Level 1) is where the control logic resides and where it gets converted to/and from electrical signals and can have the first IP connections. This is the portion of the control system where: • Analog and binary electrical signals (from sensors) get converted to digital signals via A-D converters (although not all controllers will have hardware inputs). • Digital information is converted to analog and binary electrical signals (to actuators) via D-A converters (although not all controllers will have hardware outputs). • Digital information is transmitted and received over a network.

LEVEL 2: Field Control System (IP)		
		• Digital information is processed according to a user-defined sequence to generate new digital information. • These devices may incorporate integral Level 0 sensors and actuators, for example, many Variable Air Volume (VAV) box controllers incorporate an electric actuator.
	2N/2B	The IP network (media and hardware) dedicated to the control network and carrying the control protocol (e.g., Distributed Network Protocol (DNP), IEC-61850, BACnet/IP or Lon/IP)). Generally IP over Ethernet.
	2C	Control Protocol Routers and Gateways. Control Protocol Routers route the control protocol – that is, they selectively forward control protocol packets based on destination address. They are not IP routers. Control Protocol Gateways translate between Control Protocols.
	2D	Where the local control system has an elevated C-I-A requirement, a reliability requirement, an operator response time, or a need for local operators which cannot be met by the remote site-wide front end, the facility control system may contain a local operator interface similar to what is normally found at Level 4, but dedicated to this specific control system. In other cases, for either legacy or stand-alone systems (not necessarily isolated, but stand alone in that they do not rely on another system such as an control system), the front end operator interface may be physically local to that system. In this case, the operator interface is considered to be part of Level 2 since it is dedicated to that building or facility and traffic between it and the Level 1 and Level 2 devices does not pass through the Level 3 FPOC.
Implemented Via	2A	Controllers, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are driven by cost to have the minimal functionality for the application and are very constrained in RAM, processing power, and network I/O. In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware. Aside from the fact that they use IP and are generally more powerful than

LEVEL 2: Field Control System (IP)		
		Level 1A devices, they are otherwise identical to Level 1A devices. Many devices are available as either Level 1A or 2A devices, where the hardware is identical except for the transceiver; some can even be field-configured for one or the other
	2N/2B	The Level 2N network is generally Ethernet and the Level 2B network hardware is standard IT network hardware, though sometimes with reduced functionality. For example, there may not be any requirement for remotely managed switches. Similarly, there is seldom a need for an IP router, since field control systems generally reside within a single (private) IP subnet.
	2C	Controllers very similar in hardware characteristics to Level 2A devices except that these devices typically have multiple network interfaces.
	2D	Computers (as for Level 4) Computers for legacy systems Custom or modified computers with a touch screen interface
Installed By		Controls contractor during installation or renovation of underlying mechanical or electrical system. Generally during new building construction or major renovation
Example Components	2A	Air Handler Controller Chiller Controller Boiler Controller Terminal Unit Controller Hydronic System Controller Supervisory Controller System Scheduler Electric Meter Local Display Panels Electrical Protective Relay

LEVEL 2: Field Control System (IP)		
		Voltage Regulator Controller
	2B	Ethernet Switch
	2C	BACnet MS/TP to BACnet/IP Router LonWorks TP/FT-10 to LonWorks IP Router
	2D	Control system at a central plant where the nature and criticality of the system requires a local operator interface.
Security Control Considerations	2A	Controllers residing on the dedicated IP network vary greatly from devices residing on a typical IP network. • They use a single fixed protocol (or a small number of fixed protocols) • They often do not support “log in” functionality • There is often no “session” capability • They usually do not include a user interface, and if they do it’s generally extremely limited. • They have very limited hardware capabilities (RAM, CPU, storage, etc.) • They generally do not use Windows, and seldom use Linux. They are generally some version of a real time operating system (RTOS). Many of the controllers will have the same limitations as the controllers in Level 1, where most security controls cannot/or will not apply to them. Some controllers will have significantly more capability, however, and additional controls will be applicable. In either case, the controllers should disable any network connections or services not required for operation of the control system.
	2N/2B	This network is dedicated to the control system and is generally installed by the control system contractor, not the IT organization. This doesn’t reduce the need for securing this network, but does affect the way in which this network is secured, and the risks and vulnerabilities that need to be addressed Some key differentiators between the Level 2 network and a standard IP network are: • The network structure and connected devices remain more static throughout the life of the system.

LEVEL 2: Field Control System (IP)		
		Generally components are not added and removed on a regular bases. • The protocol(s) used are fixed, and in many cases only a single protocol is used. The protocols also differ from "regular" IP networks in that they are control system protocols rather than standard IT protocols. • Bandwidth usage is lower. Because the network configuration is more static, the bandwidth usage is also more fixed. • The devices residing on the network have fewer capabilities, and generally don't support network security standards such as IEEE 802.1X. • The control system does not require the level of functionality that Approved Product List (APL) network infrastructure devices provide. The Navy, however, does require APL products for all IP Network Hardware.. • Standard IT devices typically do not meet the UL Listing requirements for fire and life safety systems, so specialized network hardware may be required to meet the control system needs.
	2C	These devices are not manufactured by traditional IT companies and do not run standard IT software. Their functionality is often included as part of a Level 2A device. They do not route IP.
	2D	While functionally, Level 2D components act similarly to computers at Level 4, the fact that they are local to (and dedicated to) a specific control systems means that from a security controls perspective, they are better addressed as Level 2 components. There are two main reasons for computers at Level 2D: • Legacy systems that cannot be patched. The computers at Level 2D may be running an older operating system and may not support some of the security controls. In this case, the controls which can be applied without negatively affecting the availability of the system should be applied, and mitigating controls and measures should be taken

LEVEL 2: Field Control System (IP)		
		when otherwise needed. Systems containing these computers should not be connected to other systems (i.e., should be operated stand-alone) until they can be properly addressed, with the computers replaced or otherwise upgraded to Level 4 standards. • Where a new system requires a local front end that, for whatever reason, cannot be installed on the basewide shared IP network (Level 4). This is typically due to a C-I-A requirement. When installing a new system with a Level 2 front end, it's important to note that the Level 2 front end should be subject to the same controls as a Level 4 front end. While implementation and inheritance of security controls at this level may differ from the Level 4 front end, computers at this Level should be subject to the same controls as a "normal" Level 4 front end of equivalent criticality.

E-6 LEVEL 3: FIELD POINT OF CONNECTION (FPOC)

Level 3 contains Field Point of Connection (FPOC), which is a logical connection between the field control system IP network at Level 2 and the Level 4 IP network. Details for Level 3 are shown in Table E-4

Table E-4 Level 3

LEVEL 3: Field Point of Connection (FPOC)	
Definition	The device which connects the dedicated Level 2 IP network with the Level 4 IP network.
Functional Description	For each field control system, the FPOC is the specific single demarcation point in the control system between that field control system and the front end system. The FPOC is a standard IT device, usually an Ethernet Switch. The FPOC generally has security controls in that it restricts access (by user, protocol, or specific commands) between levels above and levels below. Note that a large system will have hundreds of these FPOC devices, one at each connection of a field control system to the

LEVEL 3: Field Point of Connection (FPOC)	
	local network.
Implemented Via	Almost always an Ethernet switch or IP router
Installed By	Generally installed by installation network staff or by the control system contractor with oversight by the network staff.
Example Components	Standard IT managed Ethernet switch or IP router
Security Control Considerations	This device is critical from a security controls perspective as it is where the dedicated local field control network connects to the installation-wide IP network. Normally, securing this device protects the installation-wide network from the local field systems (which often have a difficult time meeting security controls). Occasionally, where there is a critical field control system, this device can protect the more critical field control system from the less-secure local system (i.e., where there are 99 non-critical systems and 1 critical one, isolate the 1 from the 99 rather than try and secure the 99). This device should, in effect, have a "deny all / permit by exception" policy applied. The FPOC should be set up with the most restrictive set of access control list (ACL) possible.

E-7 LEVEL 4: CONTROL SYSTEM FRONT END AND CONTROL SYSTEM IP NETWORK

Level 4 is the site-wide IP network used for the control system, along with front end servers and workstations (desktops and laptops). Details for Level 4 are shown in Table E-5.

Table E-5 Level 4

LEVEL 4: Control System Front End and Control System IP Network	
Definition	Front End computers and the IP network which connects multiple FCS and is not dedicated to a specific FCS. The IP network may be a dedicated physical network, or a Virtual Local Area Network (VLAN) or a Virtual Private Network (VPN) riding on top of another network.
Functional	(Level 4A and 4B) The multi-facility operator interface for the system. This is typically a web-based client-server system with

LEVEL 4: Control System Front End and Control System IP Network	
Description	the servers (Level 4A) running vendor-specific software on standard server PCs and the clients (Level 4B) accessing the servers via standard web browser software. Some functions of the control system are: • Providing graphical screens for monitoring and control of the system • Allowing operators to schedule systems, set up historical trends, and respond to alarm conditions • Provide for and support global control and optimization strategies that are impractical to implement within the control systems • Perform real-time analytical analysis and take appropriate real-time actions This level usually also includes Engineering Tool Software which provides tools for creating and modifying the control system. The Level 4N network is the network that connects multiple facility networks into a common base-wide network.
Implemented Via	Either a dedicated physical network, or a Virtual Local Area Network (VLAN) or a Virtual Private Network (VPN) riding on top of another network, or some combination of these options.. Personal Computers, servers and network devices.
Installed By	The network (Level 4N) is typically government furnished. The computers (servers and workstations in Levels 4A and 4B) are often government furnished. The software application is typically provided, installed and configured by the controls vendor.
Example Components	Servers and racks, computers, Laptops, operator interfaces, and network devices. The control system racks, hardware and software will likely be located in an Energy Operations Center, Campus Wide Operations Center, Facility Operations Center, Facility and Energy Operations Center, Security Operations Center, or Regional Operations Center.”
Security Control Considerations	Level 4 is where the CSs most closely resemble a “standard” information system, and most security controls can be applied at this layer. It’s critical to remember that control system is NOT a

LEVEL 4: Control System Front End and Control System IP Network	
	standard IS, however, and that controls must be applied in such a way as to not hamper the availability of the system. For example, some control systems require software updates from the manufacturer prior to the implementation of a Java patch, and controls relating to the application of patches must not be implemented in a manner that requires automatic or immediate patching without ensuring that this won't cause the system to go offline. Unlike standard IT applications (such as virus software or office automation tools), these PIT applications are generally a niche product and while standard guidance may cover some aspects of securing these application, it will likely be insufficient to fully secure them.

E-8 LEVEL 5: EXTERNAL CONNECTION AND CONTROL SYSTEM MANAGEMENT

Level 5 contains interfaces to "external" networks (IP networks other than the control system network). Details for Level 5 are shown in Table E-6.

Table E-6 Level 5

LEVEL 5: External Connection and Control System Management	
Definition	Additional hardware, software, and networking used to manage the control system, provide security functionality, user management, and external access. These are IT management and IT security functions, and don't provide control system functionality.
Functional Description	In many architectures, this level provides the enclave boundary defense between the control system (at Level 4 and below) and IP networks external to the control system. (In other architectures, this boundary defense occurs in the external network). In many cases, there is a component within the control system which would reside in Level 5. This level may be absent for a variety of reasons: there may not be an external connection, or the connection may be handled in the external network. Additional functionality allowed through external connections may include: • Sending alarm notification using outbound access to a

	SMTP email server. • Upload of historical data and meter data to an enterprise server using outbound HTTP/HTTPS access for uploading. In some cases, inbound HTTP may be allowed from web clients on the external network to the Level 4A server, but this is not required and is often prohibited for security reasons. The Navy prohibits this functionality.
Implemented Via	Firewalls DMZ/Perimeter Networking Proxy Servers Domain Controller, etc.
Installed By	IT and communications staff and contractors.
Example Components	Wide Area Networks Metropolitan Area Networks Local Area Networks Campus Area Networks Virtual Private Networks Point of Presence Demarcation Point or Main Point of Presence
Security Control Considerations	Generally speaking, if the control system can function in a completely isolated configuration, it should, and external connection should be absent. This Level should implement a "deny all / permit exception" policy to protect the control system from the external network and the external network from the control system.

APPENDIX F CYBERSECURITY CONSIDERATIONS FOR INTEGRATING CRITICAL UTILITY OR BUILDING CONTROL SYSTEMS WITH NON-CRITICAL UMCS

NOTE: This appendix applies to Utility Control Systems (UCS) and Building Control Systems (BCS). For the purpose of this Appendix, the term Field Control Systems (FCS) is used to refer to both UCS and BCS, but not necessarily to other Field Control System (FCS) types.

F-1 INTRODUCTION

In those cases where a Building Control System (BCS) or Utility Control System (UCS) contains classified information, controls critical infrastructure, or otherwise supports critical missions or life safety, the FCS is a critical system. While some of the requirements for securing the FCS are covered in the list of CCIs to be applied to a MODERATE or HIGH system, there are issues specifically related to critical systems on a typical installation where the preponderance of systems are non-critical.

There are three main approaches to address the connection of a critical FCS to a UMCS:

1. **Secure the UMCS at the same Impact level as the FCS**. Conceptually, this is the most straightforward approach, but it requires the UMCS Front End to be addressed at the higher Impact level, and also requires special consideration all other connected FCS which are not at the higher impact level (and are therefore connecting to a higher impact system). A typical DoD installation will have many more non-critical FCS than critical FCS, so this approach will often prove to be impractical, particularly when connecting a lower impact FCS to a higher impact UMCS Front End is difficult. This approach is the preferred solution for the Navy, and the Navy has identified an approach to connect the lower impact systems without requiring them to be assessed at the higher impact level.

2. **Implement a stand-alone UMCS for the FCS.** In this case, the FCS is part of a dedicated critical UMCS which is not connected to the UMCS serving the larger installation. This approach eliminates the risk of connection to a less critical system, but requires that the critical UMCS function independently, with its own dedicated UMCS operators. It also removes the ability to remotely monitor the critical system or to include the critical system in installation-wide supervisory functions.

   In many cases this approach is logistically infeasible to sustain, and must be carefully considered before implementing. Facility operation and maintenance staff must be willing and able to operate the stand-alone facility for this approach to work.

3. **Provide a secure connection between the critical FCS and a non-critical UMCS**. This approach connects the critical FCS to the

installation-wide UMCS in a way that does not increase the impact level of the UMCS. While this connection requires a great deal of planning and care, it can provide a more practical means of connecting the critical FCS than either implementing a stand-alone UMCS or raising the Impact level of the installation-wide UMCS.

This approach provides a security separation between the FCS and UMCS and is the preferred approach for the Army.

This Appendix presents design considerations specifically for connecting critical building control systems to a non-critical UMCS as described in approach 3. Considerations for the implementation of approach 1 or 2 are NOT addressed herein. While the considerations in this Appendix may be applicable to other control systems, particularly other building control systems or utility control systems, they are discussed here within the context of a Heating, Ventilation and Air Conditioning (HVAC) Building Control System.

F-2 LIMIT OUTSIDE FUNCTIONALITY

The key concept in connecting a critical FCS to a non-critical UMCS is limiting the ability of the UMCS to affect the FCS. The interactions between the FCS and UMCS should be specific and well-defined, and restricted to those required for system operation. In general this will entail information from the FCS being sent to the UMCS for monitoring while greatly restricting or even eliminating information from the UMCS being sent to the FCS for control purposes. For example, a critical FCS may send status and alarm information to the non-critical UMCS, but should not be receiving start/stop commands from the UMCS as this introduces vulnerabilities to the critical system. Manual changes to the critical FCS should always be carefully considered – by an operator in the zone, with ***full awareness of their actions and understanding of the impact of their actions***.

F-3 FCS-UMCS CONNECTION METHODS

Limiting ***possible*** actions is a very difficult requirement for networked controllers, in many cases the aggressor can connect their laptop to the UMCS network and download a new program to a device in the critical FCS. This is not to trivialize the significant barriers preventing this action, but by assumption, the UMCS is not sufficiently secured to protect the FCS, so it must be assumed that this action is possible and guard against it. This is similar to the additional physical security usually protecting a critical facility. Even though there are barriers limiting access to the installation in general, the assumption is that an aggressor can get access to the installation and critical facilities have additional physical security to further limit access.

There are three primary methods which can be employed to provide a secure connection between a critical FCS and a non-critical UMCS: a Hardware I/O interface, Hardware Gateway, and Network Firewall. Of these three, the recommended approach for critical FCS is the use of the Hardware I/O interface.

F-3.1 Hardware I/O Interface

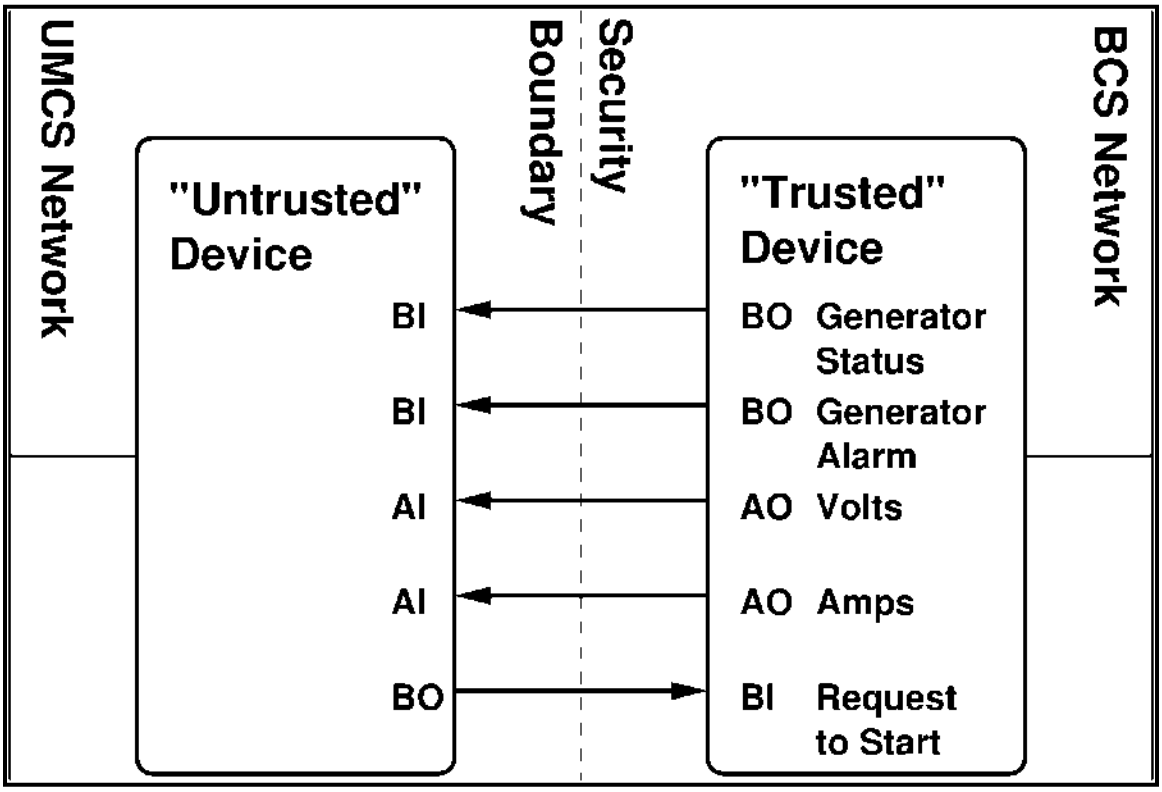
The most secure method to connect a FCS to a UMCS is to share data across the boundary using only analog and binary signals. Do ***not*** connect the FCS to the UMCS via a network. Using hardware I/O prevents an aggressor from "piggybacking" an unwanted command onto the interface as the information exchange is defined and restricted by the hardware connections. Even if an aggressor controls the untrusted device, the trusted device can only receive the commands that it has been designed and constructed to receive.

F-3.1.1 Hardware I/O Interface Overview

A Hardware I/O Interface consists of two controllers which share information between systems via binary or analog I/O, typically using dry contacts, 4-20mA signals or 0-10V signals.

Figure F-1 illustrates a Hardware I/O Interface where a generator serving a critical facility provides a few key monitoring points to a UMCS, and receives a control point, "Request to Start" from the UMCS. It's important that this point is only a ***Request*** for the system to start, and that the actual decision of whether the generator will start or stop ***must*** be made by the critical FCS.

Figure F-1 Hardware I/O Interface Example



F-3.1.2 Hardware I/O Interface Implementation

Implementing a Hardware I/O Interface requires controllers on the FCS and UMCS with matching hardware points. An aggressor could apply excessive voltages to the I/O lines and physically damage the controller on the FCS side. To mitigate this vulnerability, either:

- Use a controller dedicated to the communication interface and performing no other functions on the FCS side so that damage to it doesn't impact the control system.

  or

- Provide optical isolation of the analog and binary signals between the devices.

The controller on the UMCS side of the connection may be on a controller which performs other functions as the concern is exposing the more critical FCS to risk from the UMCS, and not the other direction. While the controller on the UMCS side is logically part of the UMCS (a "hardware I/O gateway"), procurement and installation may be simpler if it is furnished and installed by the FCS contractor.

F-3.1.3 Hardware I/O Interface Advantages and Disadvantages

This method is by far the most secure method of communication between the FCS and UMCS, as there is nothing an aggressor can do to the untrusted device that impairs the critical system. The potential disadvantage of this approach is the additional cost in the procurement and installation of two additional hardware I/O points each monitoring and/or control point. Depending on the amount and complexity of data being shared this may or may not be more costly than other approaches.

This approach is also conceptually the easiest to implement and requires no particular cybersecurity expertise skill, other than careful attention to limiting control points.

F-3.2 Hardware Gateway Interface

A Hardware Gateway is another means of connecting a critical FCS to a non-critical UMCS. While not as secure as a Hardware I/O Interface, it will be much more cost-effective if there is a large amount of data to exchange between the FCS and UMCS.

F-3.2.1 Hardware Gateway Overview

In this context, a gateway is a device with a connection to the UMCS network and a ***separate*** connection to the FCS network that does not pass network traffic between the two connections (i.e., it does not route packets between the two networks). Instead, information from one network is received by the gateway, processed by the gateway and then identical information is transmitted on the other network. While in theory the UMCS and FCS could both use the same protocol (e.g. BACnet), in practice it may be

difficult to find a gateway using the same protocol on “both sides” that is sufficiently secure, as typical designs would use the same connection for matching protocols.

F-3.2.2 Hardware Gateway Implementation

The key requirements for implementing a secure gateway are:

- The gateway must provide complete isolation / separation between the UMCS network and FCS network. This requires 2 separate network connections and may be difficult to meet if the FCS and UMCS protocols are the same.
- The gateway must not be able to be programmed, configured, or otherwise modified from the UMCS network. Since the gateway can likely be configured over the “primary” network, this requirement may be difficult to achieve if the UMCS and FCS protocols are the same. If both use the same protocol, the gateway is more likely to be configurable from both the UMCS and FCS. The configuration capability depends on the actual implementation of the gateway, so care must be taken to specify that the Gateway is not configurable from the UMCS network.
- The gateway must be configured to only expose those points absolutely necessary for the UMCS.

The gateway is part of the FCS and should be installed by the FCS contractor.

F-3.2.3 Hardware Gateway Advantages and Disadvantages

The main security concern with the gateway (assuming the above requirements are met) is security flaws in the gateway implementation. Just as a web server may have a flaw which allows an aggressor to take control of the server, a gateway may have an implementation flaw which would allow control of the gateway; once in control of the gateway, the aggressor could reconfigure the gateway to attack the FCS itself.

The gateway may provide a cost-effective alternative to the use of Hardware I/O points for systems with a requirement to share many points, and the cost of the gateway is not as dependent on the number of points as the Hardware I/O Interface.

F-3.3 Firewall Interface

The third option for securing a network connection between the UMCS and FCS is to allow a network connection but use a firewall to selectively block traffic between the two networks. The firewall requires a network connection, and is therefore only applicable when the UMCS and FCS use the same protocol.

F-3.3.1 Firewall Interface Overview

Unlike a gateway where there is no network connection between the two networks and the gateway explicitly transmits information from one to the other, with the firewall the

two networks are connected and the firewall selectively limits the traffic allowed between the two. This inherently makes the firewall less secure than the gateway.

F-3.3.2 Firewall Interface Implementation

The key requirements for a secure firewall are:

- The firewall can only be programmed from within the critical facility. This is usually not a difficult requirement to meet because as security appliances, firewalls are designed with a "secure" side and an "insecure" side.
- Unlike traditional IT firewalls, the firewall must be able to filter traffic based on the detailed information in the packet. While a standard firewall can limit traffic based on IP address and TCP/UDP port, and might block all traffic except that going to or from the UMCS server, the control system firewall must also be able to block all but specific commands. In addition to blocking all traffic except to/from the UMCS front end server, it might also block all traffic except for very specific messages – such as a BACnet ReadProperty requests for specific point values. This requires a firewall that understands the specific control protocol (BACnet in this case) and can selectively block traffic based on the specific message.

F-3.3.3 Firewall Interface Pros and Cons

The main implementation problem with a firewall is the lack of availability of a firewall that can decode control protocol packets and selectively filter based on the message. One advantage of the firewall over the gateway is that the firewall is designed for security and is less likely to have an implementation flaw than the gateway, which is typically not designed as a security device.

F-4 OTHER CONSIDERATIONS

F-4.1 Local User Interfaces

Critical systems should be provided with additional local User Interfaces to allow maintenance personnel inside the secure area access to control data to allow for troubleshooting. Liberal use of local display panels is strongly recommended. For larger critical systems, it might be desirable to provide a more functional interface than normally obtainable via LDPs, such as an independent UMCS front end or a web interface appliance. For the largest or most critical systems, consideration should be given to installing a full-featured UMCS as specified in UFGS 25 10 10. This UMCS should be dedicated to the FCS (e.g. a Level 2D front end) and should reside fully within the physical security footprint of the critical systems.

F-4.2 Management of Risk

It must always be remembered that there is no perfect solution for cybersecurity for control systems. Cybersecurity experts often say “there is no such thing as an air gap”.

While it may be more accurate to say “there are always ways to go around the air gap”, the intent remains – a determined aggressor will always find a way around, over, or through the protections put in place. The goal in the design of cybersecurity of control systems, and critical control systems in particular, is to do whatever is practical to make this as hard as possible.

This Page Intentionally Left Blank

APPENDIX G IMPLEMENTATION GUIDANCE FOR SECURITY CONTROLS

G-1 INTRODUCTION

This Appendix contains guidance to control system designers on the implementation of security controls for control systems. The focus of this guidance is on LOW impact systems (L-L-L C-I-A Impact rating) which are being fielded on a DoD installation, particularly building control systems and utility monitoring and control systems. The CCI tables in APPENDIX H provide specific breakout of responsibilities by security control and CCI. The notes in this appendix supplement those CCI tables.

G-2 GENERAL GUIDANCE

G-2.1 Control System versus Standard IT System Terminology

Security controls and CCIs were written for traditional IT systems and many contain terminology and requirements that are confusing and conflicting when applied to a control system. For example, “incident” as used in the IR family of security controls includes all incidents – a broken fan belt is an “incident”, but “flaw” as used in security control SI-2 only covers security flaws, not operational flaws – an inaccurate sensor is not a “flaw”.

In most cases, the notes below will help make the application of the security control to a control system clear. In other cases NIST SP 800-53 should be consulted as it contains the best definition of the security controls as well as “Supplemental Guidance” that can assist in the interpretation and application of the CCI to a control system. NIST SP 800-82 (section 6.2 of revision 2) also has general information on the security control families, as well as guidance on the application of the security controls to Industrial Control Systems, which are a subset of control systems and have similar characteristics to facility-related control systems.

G-2.2 DoD-Defined Values

Many CCIs have DoD defined values of “all employees”, and many CCIs have DoD defined values of “all components” or similar where this level of detail is not appropriate for a LOW impact control system. It will be necessary to re-define (and document) values for CCIs when the DoD-defined values do not make sense for control systems.

G-2.3 Security Controls Which are “Automatically Met”

Some security controls may be “automatic” in the sense that they have already been implemented for another information system or control system. A security control that states “the organization does <something>…” may have already been met as a requirement for a different authorization for a different system.

G-2.4 Security Controls Applicability by Architecture Level

Many security controls may be difficult or impossible to apply below Level 3 for most control systems. Note, however, that some system, Electronic Security Systems (ESS) in particular, may be able to meet many of these security controls below Level 3. For example, an air handler controller (with a user interface) may have only a 4-character password, or no password support at all. A door lock on an ESS may have a CAC reader.

G-2.5 Impact Level Applicability

Only security controls for systems categorized with L-L-L ("LOW impact level") and M-M-M ("MODERATE impact level") are addressed by this Appendix and the CCI tables in APPENDIX H. The guidance provided for the baseline security controls is determined by the C-I-A impact level value for the control system:

- L-L-L Baseline Security Controls: Guidance is provided for a system categorized with a LOW impact value. These same security controls are also required for a system determined to have a MODERATE (or HIGH) impact level value, but additional security enhancements and implementation guidance may be required. When applying this guidance to MODERATE (or HIGH) impact systems, evaluate the guidance to determine if it applies or must be modified for the system.
- M-M-M Baseline Security Controls: Guidance is provided for a system categorized with a MODERATE impact value. These security controls aren't used for LOW impact value systems. The guidance may not be the same for HIGH impact systems (using the same security controls).

The guidance in this Appendix and in the CCI tables in APPENDIX H is primarily targeted to LOW impact systems which are most capable of being addressed in a standard fashion. Care must be taken when extrapolating this guidance to systems with MODERATE or HIGH impact values.

G-3 GUIDANCE FOR INDIVIDUAL SECURITY CONTROLS

G-3.1 Access Control (AC) Control Family

Design guidance for the Access Control (AC) control family is shown in Table G-1

Table G-1 Access Control (AC) Control Family

Security Control ID	Security Control Name and Design Guidance
AC-2	**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.
AC-3	**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”
AC-4	**Information Flow Enforcement:** Information flow can be regulated by the IT organization at the FPOC. Level 2N devices exist that could be used at Level 2 to regulate flow. Similar Level 1N devices may exist. Include requirements in the specification that the installing contractor document necessary communications (to be used for “whitelisting”). If information flow enforcement at Level 2N is a requirement, include implementation requirements in the specification.

Security Control ID	Security Control Name and Design Guidance
AC-6	**Least Privilege:** Within the control system (as opposed to the Platform Enclave) least privilege should be met by specifications that limit functionality at the front end by user and roles (e.g., some users can only viewpoints, others can change values, etc.). Note the DoD definition of what requires explicit authorization includes (for a control system) everything – up to and including hardware. This may not be practical. Designer would need to ensure implementation via project specification requirements including physical security. Note also that AC-6 (2) requires that control system operators with access to privileged functions (via login to a privileged account) have a separate account when accessing non-privileged functions. This is probably not practical, or desirable for control system applications when considering the role that operators play (where it's impractical to expect an operator to log out and then back in to override a point, for example).
AC-7	**Unsuccessful Logon Attempts**: Note that a requirement for a HIGH availability at the front end may preclude locking out an account for failed login attempts. This control may be impractical below Level 3 and, even at Level 4, may only be implemented by login to the OS as a prerequisite for access to the control system. Designer needs to identify where this can be supported, and include requirements in the specification where this is needed.
AC-8	**System Use Notification:** Login banners must be implemented at user login to government computers – e.g. at the Platform Enclave, Level 4 and Level 2 computers. User interfaces at Levels 0, 1 and 2 (e.g. Local Display Panels (LDP)) generally won't support a login banner. Require login banners where practical according to best industry practice and indicate where implementation is not practical.
AC-11 and AC-12	**Session Lock and Session Termination:** The whole notion of a "session" generally only makes sense at a computer (i.e., Level 4) and for the computer these controls should be implemented by the operating system and inherited from the Platform Enclave. At Level 1 and Level 2, devices generally lack user interfaces. Designers should require that devices with user interfaces (e.g. LDPs) be password protected and automatically log out a user after a certain period of inactivity.

Security Control ID	Security Control Name and Design Guidance
AC-14	**Permitted Actions Without Identification Or Authentication:** At Level 4, all actions should require authentication to the (Windows) Operating System. User interfaces at Level 1 or 2 should be password protected. Note that this security control is specifically about user actions, not "processes acting for a user". In most cases, this is met by virtue of the user having logged into a computer. Physical security may be required to deny access to devices and equipment, and can be implemented at multiple levels through means such as lockable enclosures, tamper switches, room access control, people trap, and paper access logs. Some user access (local display panels, Hand-Off-Auto switches, etc.) may not support authentication and necessary physical security should be considered. When considering physical security of such devices, it is generally not beneficial to secure an interface which is co-located with the controlled equipment without also securing the controlled equipment, as the equipment would remain vulnerable.
AC-17	**Remote Access:** Remote access should be covered by the Platform Enclave (see general notes for AC control family).
AC-18	**Wireless Access:** Wireless at Level 4 should be provided by the appropriate IT organization. Avoid wireless to the greatest extent possible at Levels 1 and 2. Wireless may be considered for retrofits where running wires would be prohibitive, but other technologies (such as powerline carrier) should be considered first. When permitting wireless, require extremely limited range such that signals are not available beyond the necessary ranges. In many cases Authentication and Encryption support will be marginal at Levels 1 and 2.
AC-19	**Access Control For Mobile Devices:** Mobile devices refer to tablets, phones, etc. These are addressed at the Platform Enclave. When permitted they may be used as workstations for browser-based clients, or may be restricted to receiving alerts/notifications from the control system.
AC-20	**Use Of External Information Systems:** Connections from External systems, and portable storage, should all be handled at the Platform Enclave.
AC-21	**Collaboration And Information Sharing:** Control systems typically shouldn't share information. Any sharing is handled at the Platform Enclave.

Security Control ID	Security Control Name and Design Guidance
AC-22	**Publicly Accessible Content:** Control systems should not be publicly accessible.

G-3.2 Audit and Accountability (AU) Control Family

Auditing (in the cybersecurity sense) can typically only be performed at Level 4, although some Level 1 or 2 devices may provide limited auditing capability. Designer needs to require auditing where possible, and be prepared to justify not auditing where it is simply impractical. Designer may provide input into what can be audited, where it can be audited, and what types of information may be gathered. It might make sense for these controls to be inherited from the Platform Enclave.

Design guidance for controls in the Audit and Accountability (AU) control family is shown in Table G-2.

Table G-2 Audit and Accountability (AU) Control Family

Security Control ID	Security Control Name and Design Guidance
AU-2	**Audit Events:** No additional control-specific guidance. Use general control family guidance preceding this table for this control.
AU-3	**Content Of Audit Records:** Note that this – particularly the “user” portion - may only be possible at Level 4
AU-4	**Audit Storage Capacity:** Long term audit storage will be at a computer at Level 4. Transfer from the control system to long term storage is likely a manual process, or perhaps scripted via by the computer operating system, but it is likely not an inherent feature of the control system. Designer needs to require that control system auditing can be accessed by operating system tools (e.g. control system supports or exports to standard file formats).
AU-5	**Response To Audit Processing Failures:** Notifications and specific actions may only be possible at Level 4.

Security Control ID	Security Control Name and Design Guidance
AU-6	**Audit Review, Analysis, And Reporting:** No additional control-specific guidance. Use general control family guidance preceding this table for this control.
AU-7	**Audit Reduction And Report Generation:** Post-processing of audit logs can typically only be done by external tools at Level 4, but since the tools are specific to the control system audit log format, this will likely need to be met within the control system, not the Platform Enclave.
AU-8	**Time Stamps:** Typically, the timing requirement inherent in the control system will be sufficient.
AU-9	**Protection Of Audit Information:** Can only be done at the Level 4 front end server or other computer. Audit logs must be stored (and protected) there.
AU-11	**Audit Record Retention:** No additional control-specific guidance. Use general control family guidance preceding this table for this control.
AU-12	**Audit Generation:** No additional control-specific guidance. Use general control family guidance preceding this table for this control.

G-3.3 Security Assessment and Authorization (CA) Control Family

Design guidance for controls in the Security Assessment and Authorization (CA) control family is shown in Table G-3.

Table G-3 Security Assessment and Authorization (CA) Control Family

Security Control ID	Security Control Name and Design Guidance
CA-3	**System Interconnections:** Note this is about connections to other systems. These should be documented at the Platform Enclave. Specifications should define a specific protocol.
CA-6	**Security Authorization:** The Authorizing Official is a senior-level executive or manager.

Security Control ID	Security Control Name and Design Guidance
CA-9	**Internal System Connections:** The control system is a special purpose system. By design, only necessary connections should be allowed; typically this means use of a single specific protocol with limited capabilities. The specifications, points schedules, and network design document these controls.

G-3.4 Configuration Management (CM) Control Family

Design guidance for controls in the Configuration Management (CM) control family is shown in Table G-4.

Table G-4 Configuration Management (CM) Control Family

Security Control ID	Security Control Name and Design Guidance
CM-2	**Baseline Configuration:** Typical control system contract submittals (drawings, software licenses, programmable controller "source code" etc.) should meet this CCI. Designer should assist in determining which devices are in areas of significant risk, and what additional configurations should be applied to those devices. Note that control systems (supporting fixed facilities) are not mobile.
CM-5	**Access Restrictions for Change:** Much of the control system may be in space outside the organization's control. May only apply at Level 4. See comments on PE Controls.
CM-6	**Configuration Settings:** For the designer, this is largely ensuring that other security design requirements are included in the control system requirements document and that these requirements are verified during control system commissioning. Designer should ensure specifications disable unnecessary ports, protocols, and services. Note that the assumption that the control system is "automatically" compliant because of existing STIGs etc. is completely false below Level 3 and designer may need to provide justification for the control system not meeting the standard checklists. As a control system is designed to have regularly configurable parameters, documentation and approval for all changes to controllers at Levels 1 and 2 is not practical. Significant architectural configuration changes should still be documented and approved.

Security Control ID	Security Control Name and Design Guidance
CM-7	**Least Functionality:** The control system has a specific purpose (not a general one) and its functions (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.
CM-8	**Information System Component Inventory:** Initial configuration is specified by as-built documentation. In most cases automated tools for component inventory below Level 3 do not currently exist for many systems, although new tools may be available for systems in the future and should be implemented once available.
CM-9 and CM-10	**Configuration Management Plan and Software Usage Restrictions:** Contract documents must require that the software licenses grant the Government the Rights in Technical Data to operate and maintain the systems and use the software as required.

G-3.5 Contingency Planning (CP) Control Family

Design guidance for controls in the Contingency Planning (CP) control family is shown in Table G-5.

Table G-5 Contingency Planning (CP) Control Control Family

Security Control ID	Security Control Name and Design Guidance
CP-2	**Contingency Plan:** Designer should assist in identifying critical control system assets supporting essential missions.
CP-6	**Alternate Storage Site:** For a control system, alternate storage only makes sense for backups and is at the Platform Enclave.

Security Control ID	Security Control Name and Design Guidance
CP-7 and CP-8	**Alternate Processing Site and Telecommunications Services:** A PIT system can have an alternate front end (Level 4) and/or alternate connections from the front end to the lower levels, but you can't separate the control system from the controlled equipment – whatever site-wide incident disables the AHU controller will also disable the AHU. These controls only apply at the Platform Enclave (Level 4), and, when determining whether to apply them, note that the front end (Level 4) will typically have lower availability requirements than the field controls (Levels 1 and 2). If the requirements are for a redundant control system at the field control system, then redundant controlled equipment and/or redundant tenant spaces should be considered as well.
CP-9	**Information System Backup:** Backups at Level 4 / Platform Enclave only
CP-10	**Information System Recovery And Reconstitution:** Designer should require submittals containing data, documentation and software sufficient to restore the system to its final accepted as-built state. This must include custom programming and configuration for controllers or workstations.
CP-12	**Safe Mode:** The designer should determine, based on the criticality of the controlled equipment, what conditions to consider and which actions, if any, the control system should take when these conditions are true. This should all be specified in the control logic (e.g. sequence of operations), in particular by addressing normal/failed positions of output devices, and in the overall system design. Where high reliability is required, the analysis should consider the addition of redundant equipment to the design. See also SC-24 and SI-17, and CHAPTER 4.

G-3.6 Identification and Authorization (IA) Control Family

Note that authenticators might be either physical authenticators (e.g., CAC cards, tokens), non-physical ones (e.g., passwords), or biometrics. While Level 4 (Platform Enclave) may use any of these, most control systems will not support anything other than passwords at Level 2 and below – and even password support may only allow for "weak" passwords (e.g. much of IA-5 will not be supported except at Level 4). Therefore, DoD defined requirements may not be appropriate at Level 2 or below. Note that ESS is an exception, ESS will likely support CAC or biometrics - for example a door swipe. Designer should specify where possible to standard/best industry practice and be prepared to defend that decision when it does not meet DoD IT-centric standards.

Design guidance for controls in the Identification and Authorization (IA) control family is shown in Table G-6.

Table G-6 Identification and Authorization (IA) Control Control Family

Security Control ID	Security Control Name and Design Guidance
IA-2	**Identification And Authentication (Organizational Users):** Much of this can only be met at Level 4, and much of it depends on the computer operating system. Designer should provide specifications where possible, and be prepared to justify non-implementation in the control system. Whenever possible, require that the control system (for access via a computer) support CAC (or similar) logins. Note that remote access is covered at the Platform Enclave.
IA-3	**Device Identification And Authentication:** Much of this can only be met at Level 4, and much of it depends on the computer operating system. Typically, authentication between devices can be implemented between computers (Level 2 and 4) or between network hardware (Level 2, 3 or 4). Authentication may be supported between controllers, where not all controllers will support this capability and it will be more often supported at Level 4 than at Level 2. In general, device authentication between controllers will not be required, for LOW impact system, but may be required for MODERATE or HIGH systems. Designer should provide specifications requiring authentication where possible, and be prepared to justify non-implementation in the control system.
IA-5	**Authenticator Management:** The DoD-defined password complexity values may be impractical for control system components to meet. Specify password complexity at DoD-defined values where practical. Require that default passwords be changed from defaults, and that passwords are submitted in a secure manner.. For PKI systems, certificate paths should be provided by the Platform Enclave.
IA-6 and IA-7	**Authenticator Feedback and Cryptographic Module Authentication:** Almost certainly Platform Enclave only and not supported below that level. Designer may need to provide input/justification for this.

Security Control ID	Security Control Name and Design Guidance
IA-8	**Identification And Authentication (Non-Organizational Users):** As this deals with non-organizational users, this control generally doesn't apply to control systems other than some ESS. This may be addressed by the Platform Enclave (via computer login requirements).

G-3.7 Incident Response (IR) Control Family

Note that the definition of "incident" includes non-security related failures. A broken fan belt is an incident, as is a sticking valve, or an out-of-calibration sensor. The designer may need to provide input to the incident response plan to address any control system-specific actions. For example, the response to a successful attack on the front end might be to place equipment in Manual / Hand operation.

G-3.8 Maintenance (MA) Control Family

Design guidance for controls in the Maintenance (MA) control family is shown in Table G-7.

Table G-7 Maintenance (MA) Control Control Family

Security Control ID	Security Control Name and Design Guidance
MA-3	**Maintenance Tools:** Require that control system maintenance tools (software or hardware required to maintain the control system – most commonly engineering tool software) be provided.
MA-4	**Nonlocal Maintenance:** This is met through operating system login for the use of the engineering tool maintenance software.

G-3.9 Media Protection (MP) Control Family

Media Protection is addressed only at the Platform Enclave.

Design guidance for controls in the Media Protection (MP) control family is shown in Table G-8.

Table G-8 Media Protection (MP) Control Family

Security Control ID	Security Control Name and Design Guidance
MP-5	**Media Transport:** CCI-001027 (MP-5 (4)) places a requirement on the control system, but only when the control system is outside a "controlled area" where "controlled area" is defined in CCI-001016 as areas approved for processing the information. By definition, an area must be approved for processing the information necessary for the control systems in that area. For transportation outside that area, the data would have to be encrypted by tools provided by the Platform Enclave.

G-3.10 Physical and Environmental Protection (PE) Control Family

Note that control systems are often distributed, with large portions of the system being in spaces outside the control of the organization. This impacts many of the PE controls, in particular PE-16 can only be met for spaces controlled by the organization. In general, these are met at the Platform Enclave, but implementation may be spotty below that. Designer should require locked rooms where possible. Level 4, 3, and 2N equipment should either be in locked rooms or locked enclosures. Level 2, Level 1 and Level 0 equipment will frequently be located in tenant spaces and outside the control of the organization. For some systems, it may be necessary to require lockable enclosures for some controllers at Level 2 and Level 1, but this must be weighed against the need for maintenance personnel to access the equipment. In general, there is little benefit in requiring lockable enclosures for controllers when the underlying equipment is readily accessible from the controller location.

Most of the control system is not in "normal" server spaces. For the normal server spaces, PE requirements will be met at the Platform Enclave. For the remainder of the control system, PE requirements (e.g. PE-14's temperature and humidity requirements) are either N/A or are covered by design specifications. Note that NIST guidance states that several PEs (e.g. PE-10, PE-12, PE-13, PE-14, and PE-15) only apply at major server rooms, not individual components. These are covered by the Platform Enclave and are N/A in the control system. Design guidance for controls in the Physical and Environmental Protection (PE) control family is shown in Table G-9.

Table G-9 Physical and Environmental Protection (PE) Control Family

Security Control ID	Security Control Name and Design Guidance
PE-4	**Access Control For Transmission Medium:** Designer should require physical security for network media and may need to coordinate with electrical designer for conduit requirements. Note that physical security may be required outside spaces controlled by the organization as well. See SC-8.
PE-5	**Access Control For Output Devices:** Note that "physical outputs" for a control system correspond to the location of the controlled equipment, which must also be secured so there are unlikely to be additional requirements for the control system components
PE-9	**Power Equipment And Cabling:** For systems requiring redundant power, designer should coordinate with electrical designer. Note that the weak link in reliability will often be the controlled equipment. For example, if a single backup generator is needed, a system with 2 generators - each with a single controller - will be more reliable than a single generator with redundant controllers.
PE-11	**Emergency Power:** Within the control system, require an uninterruptible power supply (UPS), either in the control system specification or by coordination with electrical specification, when backup power is required. At the front end, this could either be met by the Platform Enclave, or by control system specification requirements also. For the majority of LOW impact systems, this control will not be implemented.
PE-16	**Delivery And Removal:** No additional control-specific guidance. Use general control family guidance preceding this table for this control.
PE-17	**Alternate Work Site:** PE-17 can't be applied except at Level 4 – there is no possible "alternate work site" for PIT. This is all at the Platform Enclave.

G-3.11 Planning (PL) Control Family

Design guidance for controls in the Planning (PL) control family is shown in Table G-10.

Table G-10 Planning (PL) Control Family

Security Control ID	Security Control Name and Design Guidance
PL-2	**System Security Plan:** While the designer is not directly responsible for the system security plan itself, the design must provide information to be used in this plan. For example, the system architecture drawing is part of the definition of the authorization boundary. The designer may also provide input for the security categorization since they have the specific knowledge of the underlying mechanical/electrical systems and can help assess the impact of those systems on control system tenants
PL-4	**Rules Of Behavior:** As indicated in CHAPTER 4, social media should be completely inaccessible from the control system.
PL-7	**Security Concept Of Operations:** Designer needs to provide input to a security concept of operations since the range of possible operations is defined by the underlying equipment, sequences of operation, selection of controllers, and front end capabilities.
PL-8	**Information Security Architecture:** System architecture submittals are necessary inputs to the security architecture. Dependencies on external services should be minimal, if any.

G-3.12 Program Management (PM) Control Family

Generally, the designer does not get involved in project planning; therefore the PM controls are not a primary designer responsibility, but designer may need to provide input to support others.

Design guidance for controls in the Program Management (PM) control family is shown in Table G-11.

Table G-11 Program Management (PM) Control Family

Security Control ID	Security Control Name and Design Guidance
PM-3	**Information Security Resources:** See General Guidance for PM Control Family and SA-2.
PM-5	**Information System Inventory:** Initial inventory is provided by as-built bill of materials.
PM-11	**Mission/Business Process Definition:** Calls for "…an achievable set of protection needs are obtained" and may require designer input.

G-3.13 Personnel Security (PS) Control Family

None of the Personnel Security controls are the responsibility of the designer.

G-3.14 Risk Assessment (RA) Control Family

By and large, the implementation of the RA controls is outside the responsibility of the designer.

Design guidance for controls in the Risk Assessment (RA) control family is shown in Table G-12.

Table G-12 Risk Assessment (RA) Control Family

Security Control ID	Security Control Name and Design Guidance
RA-3	**Risk Assessment:** The designer is well versed in the control system and the underlying mechanical / electrical system and may therefore need to assist in identifying risks to the tenants served by the control system.
RA-5	**Vulnerability Scanning:** Scanning can be performed at Levels 3 and 4, and scanning of the control system at this level should be performed by the Platform Enclave. Scanning below this level – and particularly at Level 1 - is problematic at best since typical control systems do not support scanning, and traditional IT-centric scanning tools will often completely fail when scanning a controller. Note that scanning tools should be within the Platform Enclave, scanning from outside the Platform Enclave just opens up a hole for an attacker. Designer may need to provide input to organizations attempting to meet RA-5. See SC-7, SI-3

G-3.15 System and Services Acquisition (SA) Control Family

The NIST description of “External information services” (SA-9) makes it clear that it’s an “external information system” not “external services (e.g. contractor) on this information system”

Design guidance for controls in the System and Services Acquisition (SA) control family is shown in Table G-13.

Table G-13 System and Services Acquisition (SA) Control Family

Security Control ID	Security Control Name and Design Guidance
SA-2	**Allocation Of Resources:** Designer may need to provide input to this process. See PM-3
SA-4	**Acquisition Process:** SA-4 is at least partially met by the designer incorporating security-specific requirements in the design, including acceptance testing. Requirements for FIPS PUB 201-2 probably only apply at the Platform Enclave and designer may need to provide rationale for not meeting those requirement in the control system. Similarly, many of the requirements on the developer probably cannot be enforced on a COTS system. ESS systems may need to meet FIPS PUB 201-2 at Levels 1 and 2.
SA-5	**Information System Documentation**: Designer should require submittals providing the documentation which is required by these CCIs. Note that some of the required documentation may not be obtainable, particularly for a COTS system.
SA-9	**External Information System Services:** In general, control systems should not use external IS, so this control should not apply. Where it does, it should be addressed at the Platform Enclave.
SA-10 and SA-11	**Developer Configuration Management and Developer Security Testing And Evaluation:** SA-10, SA-11 are likely impossible for COTS systems. Designer needs to specify what can be specified (which will often require additional submittals) and explain what can't be specified. Note that the control assumes the developer has a role during implementation and/or operation – this is often not true.

G-3.16 System and Communications Protection (SC) Control Family

Design guidance for controls in the System and Services Acquisition (SA) control family is shown in Table G-14.

Table G-14 System and Communications Protection (SC) Control Family

Security Control ID	Security Control Name and Design Guidance
SC-2	**Application Partitioning:** This is met by separating out computer administration and by design specifications that require different user permissions within the control system (e.g. “view data” vs “modify data”).
SC-4	**Information In Shared Resources:** Typically the control system will all be dedicated hardware and software, so there are no shared resources. This control might have some applicability at Level 4 if computer resources are shared.
SC-5	**Denial Of Service Protection:** Within the control system, denial of service attacks are mitigated by designing the system to not depend on the network. Otherwise, this is a Platform Enclave control.
SC-7	**Boundary Protection:** Implementation at the external boundary should be the responsibility of the Platform Enclave. The Platform Enclave can perform monitoring/traffic control at Level 3, and perhaps key points near Level 4 assets. Aside from those locations, this control may be difficult to meet within the control system. Designer may need to provide justification for not monitoring or controlling traffic below Level 3. It may not be prudent for the control system to fail to a “secure” state after loss of a boundary protection device since this allows an attack vector to disable controlled equipment by taking out the boundary device. Control systems must continue to run independently when boundary devices are lost. See CP-12 comments and RA-5, SI-3, SC-24
SC-8	**Transmission Confidentiality And Integrity:** Note that NIST guidance suggests this only applies to information outside a secure physical boundary, and that, when this control cannot be met, alternate physical security safeguards such as a protected distribution system can be employed.
SC-10	**Network Disconnect:** Data within a control system is often communicated without setting up a “session”. Most control systems will not use sessions other than for communications within Level 4.
SC-12	**Cryptographic Key Establishment And Management:** Below Level 4, control systems support for cryptographic keys is extremely limited and it is impractical to implement many of these controls.

Security Control ID	Security Control Name and Design Guidance
SC-13	**Cryptographic Protection:** Note that NIST states this control does not require cryptography, it merely provides requirements for the implementation of cryptography where it is required. The vast majority of control systems should not have any information requiring the use of cryptography (and in the few cases where it is even possible, the designer should review whether it is really necessary for the control system to have this information).
SC-15	**Collaborative Computing Devices:** In general, control systems shouldn't use collaborative computing devices
SC-18	**Mobile Code:** This control can and should be fully applied at Level 4. Below that, there's an important distinction between "mobile code" and "mobile code technologies": Java is a "mobile code technology" used by many control systems at Level 2 (and possibly other Levels), but Java should not be used as "mobile code" – which is code that is downloaded and executed without explicit user action. So, while mobile code technologies may be permissible below Level 4, mobile code should not be. Mobile code restrictions within the control system should be covered by design specifications. For example, common building control system products use Java, and serve web pages to clients. These pages do not constitute mobile code. Downloading a Java application, however, would be an example of mobile code.
SC-21 and SC-22	**Secure Name /Address Resolution Service (Recursive Or Caching Resolver) and Architecture And Provisioning For Name / Address Resolution Service:** These controls apply only at the Platform Enclave.
SC-23	**Session Authenticity:** See comments on SC-10.
SC-24	**Fail In Known State:** What is key here is the status of controlled equipment after a control system failure. Designer should specify this where necessary. Note that the DoD requirement of a "secure state" may not be applicable, and would be superseded by a "safe state", or by a "support the mission" state. Data preserved through a failure may be limited by the nature of the control system and designer should specify what is reasonable. See CP-12.

Security Control ID	Security Control Name and Design Guidance
SC-28	**Protection Of Information At Rest:** Note that many (if not most) control systems will not have any data requiring protection at rest since they will not have PII or classified data. Note, however, that Electronic Security Systems will often require protection of data at rest.
SC-39	**Process Isolation:** For control systems controlling multiple systems, a distributed control system meets this.
SC-41	**Port And I/O Device Access:** See comments on CM-7

G-3.17 System and Information Integrity (SI) Control Family

Design guidance for controls in the System and Information Integrity (SI) control family is shown in Table G-15.

Table G-15 System and Information Integrity (SI) Control Family

Security Control ID	Security Control Name and Design Guidance
SI-2	**Flaw Remediation:** SI-2 is about security updates and patches for software and firmware. While this can (and should) be applied at Level 3 and Level 4, this control may be largely "not applicable" or "impractical" below Level 3, due to both the relative infrequency of available updates and also the difficulty of patching controllers at Level 1 and 2. This is also largely irrelevant at Level 1 and 2, since it completely ignores flaws in the underlying equipment, which are likely to be much more common and much more significant.
SI-3	**Malicious Code Protection:** Should be implemented by the Platform Enclave at entry/exit points. Periodic scans within the control system may be difficult and the designer may need to justify their non-implementation. See RA-5, SC-7.

Security Control ID	Security Control Name and Design Guidance
SI-4	**Information System Monitoring:** Data collected can only be preserved at the Platform Enclave. Designer should provide input to monitoring objectives and methods based on the control system, the underlying mechanical/electrical system, and the impact on tenants. Note that this is not about operational monitoring of the control system (e.g. viewing graphics, receiving alarms), but about monitoring for security.
SI-7	**Software, Firmware, And Information Integrity:** Integrity verification tools may only be possible at Level 4. Designer should provide input on what is reasonable based on the control system capabilities, and where this control is not feasible.
SI-10	**Information Input Validation:** This could cover network data, sensor input, or input from a user. Designer could require additional sanity checks on sensor input, or redundant sensors. User input validation would likely need to be addressed by policy. Network validation may not be possible except at Level 4.
SI-11	**Error Handling:** Designer should require alarm messages and other control system feedback to meet this. Note that the DoD definition of recipients is not applicable for a control system.
SI-16	**Memory Protection:** Memory Protection only makes sense at Level 4.
SI-17	**Fail-Safe Procedures:** See SC-24 and CP-12 comments, where failure is one of the conditions to consider.

APPENDIX H CONTROL CORRELATION IDENTIFIER (CCI) TABLES

H-1 INTRODUCTION

This appendix provides a number of tables which help classify the CCIs for a LOW or MODERATE system on a DoD installation where there is a separate authorization for the Platform Enclave and the minimum cybersecurity design requirements have been followed.

H-2 TABLE STRUCTURE AND CONTENT

Within each table, the following columns are defined. Note that not all tables use all columns:

- **CCI**: The CCI number.
- **NIST SP 800-53 Control Text Indicator**: NIST SP 800-53 breaks individual controls (i.e., single Control IDs) down into multiple elements and enhancements, where an enhancement is a more stringent requirement than the base control. The Control Text Indicator uniquely identifies each of these elements and enhancements. A letter indicates an element within a control, a number is an enhancement. For example, "AC-17 (4)(b)" is the second element of the fourth enhancement to AC-17.
- **CCI Definition**: The definition of the CCI.
- **Applies At or Above Impact**: This CCI should be applied if the control system impact is this or above.
- **Table Reference:** Indicated which other table(s) in this Appendix the CCI is found in.
- **Applicable to a Control System:** Is this CCI applicable to a control system?
- **Rational for non-inclusion:** Reason the CCI is not applicable to control systems
- **Rational for Removal from a LOW Baseline:** Reason the CCI should be removed from the baseline for a LOW impact control system.
- **Responsibility:** Indicates who has responsibility for implementing the control. One or more of:
    - ***DoD-Defined:*** Either the DoD has provided a value for the "organization selected" values, or the DoD implementation guidance states that the CCI is already met by existing policy or regulation. ***Note that definition or guidance provided may not be relevant for a control system – the organization definitions were determined from the perspective of a traditional information system, not for a control system.***

- ***Designer:*** The designer has a role to address for this CCI. Either the designer needs to provide design specifications to cover a requirement on the control system itself, or the designer must provide input to others regarding the implementation or lack of feasibility of the CCI (typically because the CCI was written with an IT system, not a control system, in mind).
- ***Non-Designer:*** The CCI is beyond the responsibility of the designer, and is the responsibility of someone else – typically the System Owner (SO). This does not diminish the importance of these CCIs, but as these CCIs are not the responsibility of the designer they are beyond the scope of this UFC.
- ***Platform Enclave:*** The CCI contains a requirement which is assumed to be implemented at the Platform Enclave and inherited by the control system, or is mostly implemented at the Platform Enclave but also needed within the field control system. Note that if there is no Platform Enclave, then CCIs listed in the "Platform Enclave" category are instead in the "Non-Designer" category.
- ***Impractical:*** The CCI is impractical to fully implement in a control system, but may be applied in a limited manner to at least some part of the control system. Most often CCIs that can be applied to only part of the control system can be implemented at Level 4 of the architecture, but would be prohibitively difficult to implement at Levels 1 or 2. Note that "prohibitively" is a judgment based on a typical LOW control system – for a MODERATE or HIGH system, it may be worthwhile to implement these controls at all possible levels even if this adds significant cost and complexity.

H-3 CCI TABLE NOTES

H-3.1 Controls Inherited from Platform Enclave

Note that not all controls that can be inherited from the Platform Enclave have ***necessarily*** been identified as such -- some controls labeled "Non-Designer" may in fact be implemented at the Platform Enclave and the control system inherits from that.

H-3.2 CCIs in Multiple Tables

Note that some CCIs will appear in multiple tables, typically "Designer and Platform Enclave" or "Platform Enclave and Other". For example, scanning (RA-5) should happen at the Platform Enclave level and not in the control system. But the designer may need to provide input to the selection of scanning tools appropriate for the control system. The purpose of these tables is to break down the responsibilities for each control such that a specific individual/role would not be required to look at all the tables to determine what needs to be done.

H-4 CCI TABLE DESCRIPTIONS

Multiple CCI tables are included in this Appendix, each including CCIs that meet certain characteristics as described. An electronic version of the CCI tables in Excel format is available at the RMF Knowledge Service website.

H-4.1 CCI Summary Table

Table H-1 summarizes all the CCIs that can be applied to a MODERATE or lower control system, based on NIST 800-82. This table also indicates which other tables each CCI can be found in.

H-4.2 CCI Not Applicable to Control Systems

Table H-2 lists CCIs that (assuming the minimum cybersecurity requirements in CHAPTER 4 have been met) never apply to a control system, and provides a rationale for not using them.

H-4.3 CCIs Removed from LOW Impact Control System Baseline

Table H-3 lists CCIs that NIST 800-82 includes in the LOW baseline, but do not apply to a LOW control system, and provides a rationale. Note that CCIs here are listed as LOW, but aren't used at LOW.

H-4.4 Designer CCIs

For a LOW Impact system, use Table H-4 to determine CCIs that should be addressed in design. For a MODERATE Impact system, use both Table H-4 and Table H-5 to determine CCIs that should be addressed in design. In many cases, guidance on addressing specific security controls in design is provided in 0.

H-4.5 Platform Enclave CCIs

Table H-6 lists CCIs in the "Platform Enclave" category that should be applied for a LOW or MODERATE system. Table H-7 lists CCIs in the "Platform Enclave" category that should be applied for a MODERATE system (above what is applied for a LOW).

While implementation of the Platform Enclave is not the designer's responsibility (a key point of the Platform Enclave is that it is a standard approach that can be implemented across multiple control systems), those responsible for the Platform Enclave need to be aware of CCIs that the control system expects to inherit from the Platform Enclave

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
CCI-001361	AC-2(2)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001365	AC-2(2)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000017	AC-2(3)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE

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-000217	AC-2(3)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000018	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001403	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001404	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001405	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002130	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002131	AC-2(4)	MODERATE	None (Non Designer)	TRUE
CCI-001683	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001684	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001685	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001686	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002132	AC-2(4)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000213	AC-3	LOW	Table H-4 (Designer)	TRUE
CCI-001368	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001414	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001548	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001549	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001550	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001551	AC-4	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000036	AC-5(a)	MODERATE	None (Non Designer)	TRUE
CCI-002219	AC-5(a)	MODERATE	None (Non Designer)	TRUE
CCI-001380	AC-5(b)	MODERATE	None (Non Designer)	TRUE
CCI-002220	AC-5(c)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000225	AC-6	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001558	AC-6(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002221	AC-6(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002222	AC-6(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002223	AC-6(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000039	AC-6(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001419	AC-6(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002226	AC-6(5)	MODERATE	None (Non Designer)	TRUE
CCI-002227	AC-6(5)	MODERATE	None (Non Designer)	TRUE
CCI-002234	AC-6(9)	MODERATE	Table H-5 (Designer)	TRUE

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-002235	AC-6(10)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000043	AC-7(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000044	AC-7(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001423	AC-7(a)	LOW	Table H-4 (Designer)	TRUE
CCI-002236	AC-7(b)	LOW	Table H-4 (Designer)	TRUE
CCI-002237	AC-7(b)	LOW	Table H-4 (Designer)	TRUE
CCI-002238	AC-7(b)	LOW	Table H-4 (Designer)	TRUE
CCI-000048	AC-8(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002247	AC-8(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002243	AC-8(a)(1)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002244	AC-8(a)(2)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002245	AC-8(a)(3)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002246	AC-8(a)(4)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000050	AC-8(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001384	AC-8(c)(1)	LOW		FALSE
CCI-002248	AC-8(c)(1)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001385	AC-8(c)(2)	LOW		FALSE
CCI-001386	AC-8(c)(2)	LOW		FALSE
CCI-001387	AC-8(c)(2)	LOW		FALSE
CCI-001388	AC-8(c)(3)	LOW		FALSE
CCI-002332	AC-10(b)	LOW	None (Non-Designer)	TRUE
CCI-000058	AC-11(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000059	AC-11(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000056	AC-11(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000060	AC-11(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002360	AC-12	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002361	AC-12	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000061	AC-14(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000232	AC-14(b)	LOW	Table H-4 (Designer)	TRUE
CCI-000063	AC-17(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002310	AC-17(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002311	AC-17(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002312	AC-17(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000065	AC-17(b)	LOW	Table H-6 (Enclave)	TRUE

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-000067	AC-17(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002314	AC-17(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000068	AC-17(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001453	AC-17(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000069	AC-17(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001561	AC-17(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002315	AC-17(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000070	AC-17(4)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002316	AC-17(4)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002317	AC-17(4)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002318	AC-17(4)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002319	AC-17(4)(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002320	AC-17(4)(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001438	AC-18(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001439	AC-18(a)	LOW	Table H-4 (Designer)	TRUE
CCI-002323	AC-18(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001441	AC-18(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001443	AC-18(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001444	AC-18(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000082	AC-19(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000083	AC-19(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002325	AC-19(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002326	AC-19(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000084	AC-19(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002231	AC-19(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002329	AC-19(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002330	AC-19(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000093	AC-20(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002333	AC-20(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002334	AC-20(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002335	AC-20(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002336	AC-20(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002337	AC-20(1)(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000097	AC-20(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000098	AC-21(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001470	AC-21(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001471	AC-21(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001472	AC-21(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001473	AC-22(a)	LOW		FALSE
CCI-001474	AC-22(b)	LOW		FALSE
CCI-001475	AC-22(c)	LOW		FALSE
CCI-001476	AC-22(d)	LOW		FALSE
CCI-001477	AC-22(d)	LOW		FALSE
CCI-001478	AC-22(e)	LOW		FALSE
CCI-002048	AT-1(a)	LOW	None (Non-Designer)	TRUE
CCI-002049	AT-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000100	AT-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000101	AT-1(a)(1)	LOW	None (Non-Designer)	TRUE

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-000103	AT-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000104	AT-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000102	AT-1(b)(1)	LOW		TRUE
CCI-001564	AT-1(b)(1)	LOW		TRUE
CCI-000105	AT-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001565	AT-1(b)(2)	LOW		TRUE
CCI-000106	AT-2(a)	LOW	None (Non-Designer)	TRUE
CCI-000112	AT-2(b)	LOW		TRUE
CCI-001479	AT-2(c)	LOW		TRUE
CCI-001480	AT-2	LOW		TRUE
CCI-002055	AT-2(2)	MODERATE	None (Non Designer)	TRUE
CCI-000108	AT-3(a)	LOW		TRUE
CCI-000109	AT-3(b)	LOW	None (Non-Designer)	TRUE
CCI-000110	AT-3(c)	LOW	None (Non-Designer)	TRUE
CCI-000111	AT-3(c)	LOW		TRUE
CCI-000113	AT-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000114	AT-4(a)	LOW	None (Non-Designer)	TRUE
CCI-001336	AT-4(b)	LOW	None (Non-Designer)	TRUE
CCI-001337	AT-4(b)	LOW		TRUE
CCI-001930	AU-1(a)	LOW		TRUE
CCI-001931	AU-1(a)	LOW		TRUE
CCI-000117	AU-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-001832	AU-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000120	AU-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-001834	AU-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000119	AU-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-001569	AU-1(b)(1)	LOW		TRUE
CCI-000122	AU-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001570	AU-1(b)(2)	LOW		TRUE
CCI-000123	AU-2(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001571	AU-2(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000124	AU-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000125	AU-2(c)	LOW	Table H-4 (Designer)	TRUE
CCI-000126	AU-2(d)	LOW	None (Non-Designer)	TRUE
CCI-001485	AU-2(d)	LOW	Table H-4 (Designer)	TRUE
CCI-001484	AU-2(d)	LOW		TRUE
CCI-000127	AU-2(3)	MODERATE	None (Non Designer)	TRUE
CCI-001486	AU-2(3)	MODERATE		TRUE
CCI-000130	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-000131	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-000132	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-000133	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-000134	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-001487	AU-3	LOW	Table H-4 (Designer)	TRUE
CCI-000135	AU-3(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001488	AU-3(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001848	AU-4	LOW	Table H-4 (Designer)	TRUE
CCI-001849	AU-4	LOW	Table H-4 (Designer)	TRUE

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-001850	AU-4(1)	LOW	None (Non-Designer)	TRUE
CCI-001851	AU-4(1)	LOW	None (Non-Designer)	TRUE
CCI-000139	AU-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001572	AU-5(a)	LOW	None (Non-Designer)	TRUE
CCI-000140	AU-5(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001490	AU-5(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000148	AU-6(a)	LOW	None (Non-Designer)	TRUE
CCI-000151	AU-6(a)	LOW		TRUE
CCI-001862	AU-6(a)	LOW	None (Non-Designer)	TRUE
CCI-000149	AU-6(b)	LOW	None (Non-Designer)	TRUE
CCI-001863	AU-6(b)	LOW		TRUE
CCI-001864	AU-6(1)	MODERATE	None (Non Designer)	TRUE
CCI-001865	AU-6(1)	MODERATE	None (Non Designer)	TRUE
CCI-000153	AU-6(3)	MODERATE	None (Non Designer)	TRUE
CCI-001875	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001876	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001877	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001878	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001879	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001880	AU-7(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001881	AU-7(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001882	AU-7(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000158	AU-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001883	AU-7(1)	MODERATE	None (Non Designer)	TRUE
CCI-000159	AU-8(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001889	AU-8(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001890	AU-8(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001888	AU-8(b)	LOW		TRUE
CCI-001891	AU-8(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001892	AU-8(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002046	AU-8(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000161	AU-8(1)	MODERATE	None (Non Designer)	TRUE
CCI-001492	AU-8(1)	MODERATE	None (Non Designer)	TRUE
CCI-000162	AU-9	LOW	Table H-6 (Enclave)	TRUE
CCI-000163	AU-9	LOW	Table H-6 (Enclave)	TRUE
CCI-000164	AU-9	LOW	Table H-6 (Enclave)	TRUE

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-001493	AU-9	LOW	Table H-6 (Enclave)	TRUE
CCI-001494	AU-9	LOW	Table H-6 (Enclave)	TRUE
CCI-001495	AU-9	LOW	Table H-6 (Enclave)	TRUE
CCI-001894	AU-9(4)	MODERATE	None (Non Designer)	TRUE
CCI-001351	AU-9(4)(a)	MODERATE	None (Non Designer)	TRUE
CCI-000167	AU-11	LOW	None (Non-Designer)	TRUE
CCI-000168	AU-11	LOW		TRUE
CCI-000169	AU-12(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001459	AU-12(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000171	AU-12(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001910	AU-12(b)	LOW	Table H-4 (Designer)	TRUE
CCI-000172	AU-12(c)	LOW	Table H-4 (Designer)	TRUE
CCI-002061	CA-1(a)	LOW	None (Non-Designer)	TRUE
CCI-002062	CA-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000239	CA-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000240	CA-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000242	CA-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000243	CA-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000238	CA-1(b)(1)	LOW		TRUE
CCI-000241	CA-1(b)(1)	LOW		TRUE
CCI-000244	CA-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001578	CA-1(b)(2)	LOW		TRUE
CCI-000245	CA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-000246	CA-2(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000247	CA-2(a)(2)	LOW		TRUE
CCI-000248	CA-2(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-002070	CA-2(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-000251	CA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000252	CA-2(b)	LOW		TRUE
CCI-000253	CA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000254	CA-2(d)	LOW	None (Non-Designer)	TRUE
CCI-002071	CA-2(d)	LOW		TRUE
CCI-000255	CA-2(1)	MODERATE	None (Non Designer)	TRUE
CCI-002063	CA-2(1)	MODERATE	None (Non Designer)	TRUE
CCI-000257	CA-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000258	CA-3(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000259	CA-3(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000260	CA-3(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002083	CA-3(c)	LOW	None (Non-Designer)	TRUE
CCI-002084	CA-3(c)	LOW		TRUE
CCI-002080	CA-3(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002081	CA-3(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002082	CA-3(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000264	CA-5(a)	LOW	None (Non-Designer)	TRUE
CCI-000265	CA-5(b)	LOW		TRUE
CCI-000266	CA-5(b)	LOW	None (Non-Designer)	TRUE
CCI-000270	CA-6(a)	LOW	None (Non-Designer)	TRUE

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-000271	CA-6(b)	LOW	None (Non-Designer)	TRUE
CCI-000272	CA-6(c)	LOW	None (Non-Designer)	TRUE
CCI-000273	CA-6(c)	LOW		TRUE
CCI-002087	CA-7(a)	LOW	None (Non-Designer)	TRUE
CCI-002088	CA-7(b)	LOW	None (Non-Designer)	TRUE
CCI-002089	CA-7(b)	LOW	None (Non-Designer)	TRUE
CCI-000279	CA-7(c)	LOW	None (Non-Designer)	TRUE
CCI-002090	CA-7(d)	LOW	None (Non-Designer)	TRUE
CCI-002091	CA-7(e)	LOW	None (Non-Designer)	TRUE
CCI-002092	CA-7(f)	LOW	None (Non-Designer)	TRUE
CCI-000280	CA-7(g)	LOW	None (Non-Designer)	TRUE
CCI-000281	CA-7(g)	LOW	None (Non-Designer)	TRUE
CCI-001581	CA-7(g)	LOW	None (Non-Designer)	TRUE
CCI-000274	CA-7	LOW	None (Non-Designer)	TRUE
CCI-000282	CA-7(1)	MODERATE	None (Non Designer)	TRUE
CCI-002085	CA-7(1)	MODERATE	None (Non Designer)	TRUE
CCI-002102	CA-9(a)	LOW	Table H-4 (Designer)	TRUE
CCI-002101	CA-9(a)	LOW	None (Non-Designer)	TRUE
CCI-002103	CA-9(b)	LOW	Table H-4 (Designer)	TRUE
CCI-002104	CA-9(b)	LOW	Table H-4 (Designer)	TRUE
CCI-002105	CA-9(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001821	CM-1(a)	LOW	None (Non-Designer)	TRUE
CCI-001824	CM-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000287	CM-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-001822	CM-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000290	CM-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-001825	CM-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000286	CM-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000289	CM-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000292	CM-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001584	CM-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-000293	CM-2	LOW	Table H-4 (Designer)	TRUE
CCI-000295	CM-2	LOW	None (Non-Designer)	TRUE
CCI-000296	CM-2(1)(a)	MODERATE	None (Non Designer)	TRUE
CCI-001497	CM-2(1)(a)	MODERATE		TRUE
CCI-000297	CM-2(1)(b)	MODERATE	None (Non Designer)	TRUE
CCI-001585	CM-2(1)(b)	MODERATE		TRUE
CCI-000298	CM-2(1)(c)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000299	CM-2(1)(c)	MODERATE	None (Non Designer)	TRUE
CCI-000304	CM-2(3)	MODERATE	None (Non Designer)	TRUE
CCI-001736	CM-2(3)	MODERATE	None (Non Designer)	TRUE
CCI-001739	CM-2(7)a	MODERATE		FALSE
CCI-001737	CM-2(7)a	MODERATE	Table H-5 (Designer)	TRUE
CCI-001738	CM-2(7)a	MODERATE	Table H-5 (Designer)	TRUE
CCI-001815	CM-2(7)b	MODERATE		FALSE
CCI-001816	CM-2(7)b	MODERATE		FALSE
CCI-000313	CM-3(a)	MODERATE	None (Non Designer)	TRUE
CCI-000314	CM-3(b)	MODERATE	None (Non Designer)	TRUE

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-001740	CM-3(b)	MODERATE	None (Non Designer)	TRUE
CCI-001741	CM-3(c)	MODERATE	None (Non Designer)	TRUE
CCI-001819	CM-3(d)	MODERATE	None (Non Designer)	TRUE
CCI-000316	CM-3(e)	MODERATE	None (Non Designer)	TRUE
CCI-002056	CM-3(e)	MODERATE	None (Non Designer)	TRUE
CCI-000318	CM-3(f)	MODERATE	None (Non Designer)	TRUE
CCI-000319	CM-3(g)	MODERATE	None (Non Designer)	TRUE
CCI-000320	CM-3(g)	MODERATE	None (Non Designer)	TRUE
CCI-000321	CM-3(g)	MODERATE	None (Non Designer)	TRUE
CCI-001586	CM-3(g)	MODERATE	None (Non Designer)	TRUE
CCI-000327	CM-3(2)	MODERATE	None (Non Designer)	TRUE
CCI-000328	CM-3(2)	MODERATE	None (Non Designer)	TRUE
CCI-000329	CM-3(2)	MODERATE	None (Non Designer)	TRUE
CCI-000333	CM-4	LOW	None (Non-Designer)	TRUE
CCI-000338	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000339	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000340	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000341	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000342	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000343	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000344	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000345	CM-5	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000363	CM-6(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000364	CM-6(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000365	CM-6(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001588	CM-6(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000366	CM-6(b)	LOW	None (Non-Designer)	TRUE
CCI-000367	CM-6(c)	LOW	None (Non-Designer)	TRUE
CCI-000368	CM-6(c)	LOW	None (Non-Designer)	TRUE
CCI-000369	CM-6(c)	LOW	None (Non-Designer)	TRUE
CCI-001755	CM-6(c)	LOW	Table H-4 (Designer)	TRUE
CCI-001756	CM-6(c)	LOW	None (Non-Designer)	TRUE
CCI-001502	CM-6(d)	LOW	None (Non-Designer)	TRUE
CCI-001503	CM-6(d)	LOW	None (Non-Designer)	TRUE
CCI-000381	CM-7(a)	LOW	Table H-4 (Designer)	TRUE
CCI-000380	CM-7(b)	LOW	Table H-4 (Designer)	TRUE
CCI-000382	CM-7(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001760	CM-7(1)(a)	LOW		TRUE
CCI-000384	CM-7(1)(a)	LOW	None (Non-Designer)	TRUE
CCI-001761	CM-7(1)(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001762	CM-7(1)(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001592	CM-7(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001763	CM-7(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001764	CM-7(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001772	CM-7(5)a	MODERATE	Table H-5 (Designer)	TRUE
CCI-001773	CM-7(5)a	MODERATE	Table H-5 (Designer)	TRUE
CCI-001774	CM-7(5)b	MODERATE	Table H-5 (Designer)	TRUE
CCI-001775	CM-7(5)c	MODERATE	None (Non Designer)	TRUE

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-001777	CM-7(5)c	MODERATE	None (Non Designer)	TRUE
CCI-000389	CM-8(a)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-000392	CM-8(a)(2)	LOW	Table H-4 (Designer)	TRUE
CCI-000395	CM-8(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-000398	CM-8(a)(4)	LOW	Table H-4 (Designer)	TRUE
CCI-000399	CM-8(a)(4)	LOW	None (Non-Designer)	TRUE
CCI-001779	CM-8(b)	LOW	None (Non-Designer)	TRUE
CCI-001780	CM-8(b)	LOW	None (Non-Designer)	TRUE
CCI-000408	CM-8(1)	MODERATE	None (Non Designer)	TRUE
CCI-000409	CM-8(1)	MODERATE	None (Non Designer)	TRUE
CCI-000410	CM-8(1)	MODERATE	None (Non Designer)	TRUE
CCI-000415	CM-8(3)(a)	MODERATE	None (Non Designer)	TRUE
CCI-000416	CM-8(3)(a)	MODERATE	None (Non Designer)	TRUE
CCI-001783	CM-8(3)(b)	MODERATE		TRUE
CCI-001784	CM-8(3)(b)	MODERATE	None (Non Designer)	TRUE
CCI-000419	CM-8(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000421	CM-9(a)	MODERATE	None (Non Designer)	TRUE
CCI-000423	CM-9(a)	MODERATE	None (Non Designer)	TRUE
CCI-001790	CM-9(b)	MODERATE	None (Non Designer)	TRUE
CCI-001792	CM-9(b)	MODERATE	None (Non Designer)	TRUE
CCI-001793	CM-9(b)	MODERATE	None (Non Designer)	TRUE
CCI-001795	CM-9(b)	MODERATE	None (Non Designer)	TRUE
CCI-000424	CM-9(c)	MODERATE	None (Non Designer)	TRUE
CCI-000426	CM-9(c)	MODERATE	None (Non Designer)	TRUE
CCI-001796	CM-9(c)	MODERATE	None (Non Designer)	TRUE
CCI-001798	CM-9(c)	MODERATE	None (Non Designer)	TRUE
CCI-001799	CM-9(d)	MODERATE	None (Non Designer)	TRUE
CCI-001801	CM-9(d)	MODERATE	None (Non Designer)	TRUE
CCI-001726	CM-10(a)	LOW	None (Non-Designer)	TRUE
CCI-001727	CM-10(a)	LOW	None (Non-Designer)	TRUE
CCI-001728	CM-10(a)	LOW	None (Non-Designer)	TRUE
CCI-001729	CM-10(a)	LOW	None (Non-Designer)	TRUE
CCI-001730	CM-10(b)	LOW	None (Non-Designer)	TRUE
CCI-001731	CM-10(b)	LOW	None (Non-Designer)	TRUE
CCI-001802	CM-10(b)	LOW	None (Non-Designer)	TRUE
CCI-001803	CM-10(b)	LOW	None (Non-Designer)	TRUE
CCI-001732	CM-10(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-001733	CM-10(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-001804	CM-11(a)	LOW	None (Non-Designer)	TRUE
CCI-001805	CM-11(a)	LOW	None (Non-Designer)	TRUE
CCI-001806	CM-11(b)	LOW	None (Non-Designer)	TRUE
CCI-001807	CM-11(b)	LOW	None (Non-Designer)	TRUE
CCI-001808	CM-11(c)	LOW		TRUE
CCI-001809	CM-11(c)	LOW	None (Non-Designer)	TRUE
CCI-000438	CP-1(a)(1)	LOW		TRUE
CCI-000439	CP-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-002825	CP-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000441	CP-1(a)(2)	LOW		TRUE

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-001597	CP-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-002826	CP-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000437	CP-1(b)(1)	LOW		TRUE
CCI-000440	CP-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-001596	CP-1(b)(2)	LOW		TRUE
CCI-001598	CP-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-000444	CP-2(a)(1)	LOW		FALSE
CCI-000443	CP-2(a)(1)	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000445	CP-2(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000446	CP-2(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000447	CP-2(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000448	CP-2(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000449	CP-2(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-000451	CP-2(a)(4)	LOW		FALSE
CCI-000453	CP-2(a)(4)	LOW		FALSE
CCI-000455	CP-2(a)(4)	LOW		FALSE
CCI-000450	CP-2(a)(4)	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000452	CP-2(a)(4)	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000454	CP-2(a)(4)	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000456	CP-2(a)(5)	LOW	None (Non-Designer)	TRUE
CCI-000457	CP-2(a)(6)	LOW	None (Non-Designer)	TRUE
CCI-002830	CP-2(a)(6)	LOW		TRUE
CCI-000458	CP-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000459	CP-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000460	CP-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000461	CP-2(d)	LOW		TRUE
CCI-000462	CP-2(d)	LOW	None (Non-Designer)	TRUE
CCI-000463	CP-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000464	CP-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000465	CP-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000466	CP-2(e)	LOW	None (Non-Designer)	TRUE
CCI-000468	CP-2(f)	LOW	None (Non-Designer)	TRUE
CCI-002831	CP-2(f)	LOW	None (Non-Designer)	TRUE
CCI-002832	CP-2(g)	LOW	None (Non-Designer)	TRUE
CCI-000469	CP-2(1)	MODERATE	None (Non Designer)	TRUE
CCI-000474	CP-2(3)	MODERATE		FALSE
CCI-000476	CP-2(3)	MODERATE		FALSE
CCI-000473	CP-2(3)	MODERATE		TRUE
CCI-000475	CP-2(3)	MODERATE	None (Non Designer)	TRUE
CCI-002829	CP-2(8)	MODERATE		FALSE
CCI-002828	CP-2(8)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000486	CP-3(a)	LOW	None (Non-Designer)	TRUE
CCI-002833	CP-3(a)	LOW		TRUE
CCI-002834	CP-3(b)	LOW	None (Non-Designer)	TRUE

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-000485	CP-3(c)	LOW		TRUE
CCI-000487	CP-3(c)	LOW	None (Non-Designer)	TRUE
CCI-000490	CP-4(a)	LOW		TRUE
CCI-000492	CP-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000494	CP-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000496	CP-4(b)	LOW	None (Non-Designer)	TRUE
CCI-000497	CP-4(c)	LOW	None (Non-Designer)	TRUE
CCI-000498	CP-4(1)	MODERATE	None (Non Designer)	TRUE
CCI-000505	CP-6(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002836	CP-6(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000507	CP-6(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000509	CP-6(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001604	CP-6(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000514	CP-7(a)	MODERATE		FALSE
CCI-000510	CP-7(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000513	CP-7(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002839	CP-7(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000515	CP-7(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000521	CP-7(c)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000516	CP-7(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000517	CP-7(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001606	CP-7(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000518	CP-7(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000523	CP-8	MODERATE		FALSE
CCI-000525	CP-8	MODERATE		FALSE
CCI-002841	CP-8	MODERATE		FALSE
CCI-000522	CP-8	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000524	CP-8	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002840	CP-8	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000526	CP-8(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000527	CP-8(1)(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000528	CP-8(1)(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000529	CP-8(1)(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000530	CP-8(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000535	CP-9(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000534	CP-9(a)	LOW		TRUE
CCI-000537	CP-9(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000536	CP-9(b)	LOW	None (Non-Designer)	TRUE
CCI-000539	CP-9(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-000538	CP-9(c)	LOW	None (Non-Designer)	TRUE
CCI-000540	CP-9(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-000541	CP-9(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000542	CP-9(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000550	CP-10	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000551	CP-10	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE

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
CCI-001959	IA-3(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001967	IA-3(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001965	IA-3(4)	MODERATE	None (Non Designer)	TRUE
CCI-001966	IA-3(4)	MODERATE	None (Non Designer)	TRUE
CCI-001968	IA-3(4)	MODERATE	None (Non Designer)	TRUE
CCI-001969	IA-3(4)	MODERATE	None (Non Designer)	TRUE
CCI-001970	IA-4(a)	LOW	Table H-6 (Enclave)	TRUE

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-001971	IA-4(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001972	IA-4(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001973	IA-4(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-001974	IA-4(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-001975	IA-4(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-000794	IA-4(e)	LOW	Table H-6 (Enclave)	TRUE
CCI-000795	IA-4(e)	LOW	Table H-6 (Enclave)	TRUE
CCI-001980	IA-5(a)	LOW	None (Non-Designer)	TRUE
CCI-000176	IA-5(b)	LOW	Table H-4 (Designer)	TRUE
CCI-001544	IA-5(c)	LOW	Table H-4 (Designer)	TRUE
CCI-001981	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001982	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001983	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001984	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001985	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001986	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001987	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001998	IA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-001989	IA-5(e)	LOW	Table H-4 (Designer)	TRUE
CCI-000179	IA-5(f)	LOW	None (Non-Designer)	TRUE
CCI-000180	IA-5(f)	LOW	None (Non-Designer)	TRUE
CCI-000181	IA-5(f)	LOW	None (Non-Designer)	TRUE
CCI-000182	IA-5(g)	LOW	Table H-4 (Designer)	TRUE
CCI-001610	IA-5(g)	LOW	Table H-4 (Designer)	TRUE
CCI-000183	IA-5(h)	LOW	None (Non-Designer)	TRUE
CCI-002042	IA-5(h)	LOW	None (Non-Designer)	TRUE
CCI-002365	IA-5(i)	LOW	None (Non-Designer)	TRUE
CCI-002366	IA-5(i)	LOW	None (Non-Designer)	TRUE
CCI-001990	IA-5(j)	LOW	Table H-6 (Enclave)	TRUE
CCI-000192	IA-5(1)(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000193	IA-5(1)(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000194	IA-5(1)(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000205	IA-5(1)(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001611	IA-5(1)(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001612	IA-5(1)(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001613	IA-5(1)(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001614	IA-5(1)(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001619	IA-5(1)(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000195	IA-5(1)(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001615	IA-5(1)(b)	LOW	Table H-4 (Designer)	TRUE
CCI-000196	IA-5(1)(c)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE

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-000197	IA-5(1)(c)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000198	IA-5(1)(d)	LOW	Table H-4 (Designer)	TRUE
CCI-000199	IA-5(1)(d)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001616	IA-5(1)(d)	LOW	Table H-4 (Designer)	TRUE
CCI-001617	IA-5(1)(d)	LOW	Table H-4 (Designer)	TRUE
CCI-000200	IA-5(1)(e)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001618	IA-5(1)(e)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002041	IA-5(1)(f)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000185	IA-5(2)(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000186	IA-5(2)(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-000187	IA-5(2)(c)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001991	IA-5(2)(d)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001992	IA-5(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001993	IA-5(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001994	IA-5(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001995	IA-5(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002002	IA-5(11)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002003	IA-5(11)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000206	IA-6	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000803	IA-7	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-000804	IA-8	LOW	Table H-6 (Enclave)	TRUE
CCI-002009	IA-8(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002010	IA-8(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002011	IA-8(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-002012	IA-8(3)	LOW	None (Non-Designer)	TRUE
CCI-002013	IA-8(3)	LOW	Table H-6 (Enclave)	TRUE
CCI-002014	IA-8(4)	LOW	Table H-6 (Enclave)	TRUE
CCI-002776	IR-1(a)	LOW	None (Non-Designer)	TRUE
CCI-002777	IR-1(a)	LOW		TRUE
CCI-000805	IR-1(a)(1)	LOW		TRUE
CCI-000806	IR-1(a)(1)	LOW		TRUE
CCI-000809	IR-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000810	IR-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000807	IR-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000808	IR-1(b)(1)	LOW		TRUE

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-000811	IR-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-000812	IR-1(b)(2)	LOW		TRUE
CCI-000813	IR-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002778	IR-2(a)	LOW		TRUE
CCI-002779	IR-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000814	IR-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000815	IR-2(c)	LOW		TRUE
CCI-000818	IR-3	MODERATE	None (Non Designer)	TRUE
CCI-000819	IR-3	MODERATE		TRUE
CCI-000820	IR-3	MODERATE		TRUE
CCI-001624	IR-3	MODERATE	None (Non Designer)	TRUE
CCI-002780	IR-3(2)	MODERATE	None (Non Designer)	TRUE
CCI-000822	IR-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000823	IR-4(b)	LOW	None (Non-Designer)	TRUE
CCI-000824	IR-4(c)	LOW	None (Non-Designer)	TRUE
CCI-001625	IR-4(c)	LOW	None (Non-Designer)	TRUE
CCI-000825	IR-4(1)	MODERATE	None (Non Designer)	TRUE
CCI-000832	IR-5	LOW	None (Non-Designer)	TRUE
CCI-000834	IR-6(a)	LOW	None (Non-Designer)	TRUE
CCI-000835	IR-6(a)	LOW	None (Non-Designer)	TRUE
CCI-000836	IR-6(b)	LOW	None (Non-Designer)	TRUE
CCI-002791	IR-6(b)	LOW		TRUE
CCI-000837	IR-6(1)	MODERATE	None (Non Designer)	TRUE
CCI-000839	IR-7	LOW	None (Non-Designer)	TRUE
CCI-000840	IR-7(1)	MODERATE	None (Non Designer)	TRUE
CCI-002794	IR-8(a)	LOW	None (Non-Designer)	TRUE
CCI-002795	IR-8(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-002796	IR-8(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-002797	IR-8(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-002798	IR-8(a)(4)	LOW	None (Non-Designer)	TRUE
CCI-002799	IR-8(a)(5)	LOW	None (Non-Designer)	TRUE
CCI-002800	IR-8(a)(6)	LOW	None (Non-Designer)	TRUE
CCI-002801	IR-8(a)(7)	LOW	None (Non-Designer)	TRUE
CCI-000844	IR-8(a)(8)	LOW	None (Non-Designer)	TRUE
CCI-002802	IR-8(a)(8)	LOW		TRUE
CCI-000845	IR-8(b)	LOW		TRUE
CCI-000846	IR-8(b)	LOW	None (Non-Designer)	TRUE
CCI-000847	IR-8(c)	LOW		TRUE
CCI-000848	IR-8(c)	LOW		TRUE
CCI-000849	IR-8(d)	LOW	None (Non-Designer)	TRUE
CCI-000850	IR-8(e)	LOW	None (Non-Designer)	TRUE
CCI-002803	IR-8(e)	LOW		TRUE
CCI-002804	IR-8(f)	LOW	None (Non-Designer)	TRUE
CCI-002861	MA-1(a)	LOW		TRUE
CCI-002862	MA-1(a)	LOW		TRUE
CCI-000852	MA-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000853	MA-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000855	MA-1(a)(2)	LOW	None (Non-Designer)	TRUE

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-000856	MA-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000851	MA-1(b)(1)	LOW		TRUE
CCI-000854	MA-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000857	MA-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001628	MA-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-002866	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002867	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002868	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002869	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002870	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002871	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002872	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002873	MA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-000859	MA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000860	MA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-002874	MA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000861	MA-2(d)	LOW	None (Non-Designer)	TRUE
CCI-000862	MA-2(e)	LOW	None (Non-Designer)	TRUE
CCI-002875	MA-2(f)	LOW	None (Non-Designer)	TRUE
CCI-002876	MA-2(f)	LOW	None (Non-Designer)	TRUE
CCI-000865	MA-3	MODERATE	Table H-5 (Designer)	TRUE
CCI-000866	MA-3	MODERATE	None (Non Designer)	TRUE
CCI-000867	MA-3	MODERATE	None (Non Designer)	TRUE
CCI-000869	MA-3(1)	MODERATE	None (Non Designer)	TRUE
CCI-000870	MA-3(2)	MODERATE	None (Non Designer)	TRUE
CCI-000873	MA-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000874	MA-4(a)	LOW	None (Non-Designer)	TRUE
CCI-000876	MA-4(b)	LOW	None (Non-Designer)	TRUE
CCI-000877	MA-4(c)	LOW	None (Non-Designer)	TRUE
CCI-000878	MA-4(d)	LOW	None (Non-Designer)	TRUE
CCI-000879	MA-4(e)	LOW	None (Non-Designer)	TRUE
CCI-000881	MA-4(2)	MODERATE	None (Non Designer)	TRUE
CCI-000890	MA-5(a)	LOW	None (Non-Designer)	TRUE
CCI-000891	MA-5(a)	LOW	None (Non-Designer)	TRUE
CCI-002894	MA-5(b)	LOW	None (Non-Designer)	TRUE
CCI-002895	MA-5(c)	LOW	None (Non-Designer)	TRUE
CCI-000903	MA-6	MODERATE	None (Non Designer)	TRUE
CCI-002896	MA-6	MODERATE	None (Non Designer)	TRUE
CCI-002897	MA-6	MODERATE		TRUE
CCI-000995	MP-1(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-000996	MP-1(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002566	MP-1(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-000999	MP-1(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-001000	MP-1(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-000997	MP-1(b)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-000998	MP-1(b)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-001001	MP-1(b)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-001002	MP-1(b)(2)	LOW	Table H-6 (Enclave)	TRUE

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-001003	MP-2	LOW	Table H-6 (Enclave)	TRUE
CCI-001004	MP-2	LOW	Table H-6 (Enclave)	TRUE
CCI-001005	MP-2	LOW	Table H-6 (Enclave)	TRUE
CCI-001010	MP-3(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001011	MP-3(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001012	MP-3(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001013	MP-3(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001014	MP-4(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001015	MP-4(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001016	MP-4(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001018	MP-4(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001020	MP-5(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001021	MP-5(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001022	MP-5(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001023	MP-5(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001025	MP-5(c)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001024	MP-5(d)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001027	MP-5(4)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001028	MP-6(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002578	MP-6(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002579	MP-6(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002580	MP-6(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002581	MP-7	LOW	Table H-6 (Enclave)	TRUE
CCI-002582	MP-7	LOW	Table H-6 (Enclave)	TRUE
CCI-002583	MP-7	LOW	Table H-6 (Enclave)	TRUE
CCI-002584	MP-7	LOW	Table H-6 (Enclave)	TRUE
CCI-002585	MP-7(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002908	PE-1(a)	LOW	None (Non-Designer)	TRUE
CCI-002909	PE-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000904	PE-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000905	PE-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000908	PE-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000909	PE-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-000906	PE-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000907	PE-1(b)(1)	LOW		TRUE
CCI-000910	PE-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-000911	PE-1(b)(2)	LOW		TRUE
CCI-000912	PE-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002910	PE-2(a)	LOW	None (Non-Designer)	TRUE
CCI-002911	PE-2(a)	LOW	None (Non-Designer)	TRUE
CCI-000913	PE-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000914	PE-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000915	PE-2(c)	LOW	None (Non-Designer)	TRUE
CCI-001635	PE-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000919	PE-3(a)	LOW	None (Non-Designer)	TRUE
CCI-002915	PE-3(a)	LOW	None (Non-Designer)	TRUE
CCI-000920	PE-3(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000921	PE-3(a)(2)	LOW	None (Non-Designer)	TRUE

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-002916	PE-3(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-002917	PE-3(b)	LOW	None (Non-Designer)	TRUE
CCI-002918	PE-3(b)	LOW	None (Non-Designer)	TRUE
CCI-002919	PE-3(c)	LOW	None (Non-Designer)	TRUE
CCI-002920	PE-3(c)	LOW	None (Non-Designer)	TRUE
CCI-002921	PE-3(d)	LOW	None (Non-Designer)	TRUE
CCI-002922	PE-3(d)	LOW	None (Non-Designer)	TRUE
CCI-002923	PE-3(d)	LOW	None (Non-Designer)	TRUE
CCI-002924	PE-3(d)	LOW	None (Non-Designer)	TRUE
CCI-000923	PE-3(e)	LOW	None (Non-Designer)	TRUE
CCI-000924	PE-3(f)	LOW	None (Non-Designer)	TRUE
CCI-000925	PE-3(f)	LOW		TRUE
CCI-002925	PE-3(f)	LOW		TRUE
CCI-000926	PE-3(g)	LOW	None (Non-Designer)	TRUE
CCI-000927	PE-3(g)	LOW		TRUE
CCI-000936	PE-4	MODERATE	Table H-5 (Designer)	TRUE
CCI-002930	PE-4	MODERATE	Table H-5 (Designer)	TRUE
CCI-002931	PE-4	MODERATE	Table H-5 (Designer)	TRUE
CCI-000937	PE-5	MODERATE	Table H-5 (Designer)	TRUE
CCI-002939	PE-6(a)	LOW	None (Non-Designer)	TRUE
CCI-000939	PE-6(b)	LOW	None (Non-Designer)	TRUE
CCI-000940	PE-6(b)	LOW		TRUE
CCI-002940	PE-6(b)	LOW	None (Non-Designer)	TRUE
CCI-002941	PE-6(b)	LOW	None (Non-Designer)	TRUE
CCI-000941	PE-6(c)	LOW	None (Non-Designer)	TRUE
CCI-000942	PE-6(1)	MODERATE	None (Non Designer)	TRUE
CCI-002950	PE-6(4)	MODERATE	None (Non Designer)	TRUE
CCI-002951	PE-6(4)	MODERATE	None (Non Designer)	TRUE
CCI-000947	PE-8(a)	LOW	None (Non-Designer)	TRUE
CCI-002952	PE-8(a)	LOW		TRUE
CCI-000948	PE-8(b)	LOW	None (Non-Designer)	TRUE
CCI-000949	PE-8(b)	LOW		TRUE
CCI-000952	PE-9	MODERATE	Table H-5 (Designer)	TRUE
CCI-002953	PE-9(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002954	PE-9(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000956	PE-10(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000957	PE-10(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000958	PE-10(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000959	PE-10(c)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002955	PE-11	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000961	PE-11(1)	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000963	PE-12	LOW		FALSE
CCI-000965	PE-13	LOW	Table H-6 (Enclave)	TRUE
CCI-000968	PE-13(3)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000971	PE-14(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000972	PE-14(a)	LOW	Table H-6 (Enclave)	TRUE

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-000973	PE-14(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000974	PE-14(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000977	PE-15	LOW	Table H-6 (Enclave)	TRUE
CCI-000978	PE-15	LOW	Table H-6 (Enclave)	TRUE
CCI-000979	PE-15	LOW	Table H-6 (Enclave)	TRUE
CCI-000981	PE-16	LOW	Table H-6 (Enclave)	TRUE
CCI-000982	PE-16	LOW	Table H-6 (Enclave)	TRUE
CCI-000983	PE-16	LOW	Table H-6 (Enclave)	TRUE
CCI-000984	PE-16	LOW	Table H-6 (Enclave)	TRUE
CCI-002974	PE-16	LOW	Table H-6 (Enclave)	TRUE
CCI-000985	PE-17(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002975	PE-17(a)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000987	PE-17(b)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000988	PE-17(c)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-003047	PL-1(a)	LOW	None (Non-Designer)	TRUE
CCI-003048	PL-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000563	PL-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000564	PL-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-000566	PL-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-001636	PL-1(b)(1)	LOW		TRUE
CCI-001637	PL-1(b)(1)	LOW	None (Non-Designer)	TRUE
CCI-000567	PL-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-000568	PL-1(b)(2)	LOW	None (Non-Designer)	TRUE
CCI-001638	PL-1(b)(2)	LOW		TRUE
CCI-003049	PL-2(a)	LOW	None (Non-Designer)	TRUE
CCI-003050	PL-2(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003051	PL-2(a)(2)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-003052	PL-2(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-003053	PL-2(a)(4)	LOW	Table H-4 (Designer)	TRUE
CCI-003054	PL-2(a)(5)	LOW	None (Non-Designer)	TRUE
CCI-003055	PL-2(a)(6)	LOW	None (Non-Designer)	TRUE
CCI-003056	PL-2(a)(7)	LOW	None (Non-Designer)	TRUE
CCI-003057	PL-2(a)(8)	LOW	None (Non-Designer)	TRUE
CCI-000571	PL-2(a)(9)	LOW	None (Non-Designer)	TRUE
CCI-003059	PL-2(b)	LOW	None (Non-Designer)	TRUE
CCI-003060	PL-2(b)	LOW		TRUE
CCI-003061	PL-2(b)	LOW	None (Non-Designer)	TRUE
CCI-003062	PL-2(b)	LOW		TRUE
CCI-000572	PL-2(c)	LOW		TRUE
CCI-000573	PL-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000574	PL-2(d)	LOW	None (Non-Designer)	TRUE
CCI-003063	PL-2(e)	LOW	None (Non-Designer)	TRUE
CCI-003064	PL-2(e)	LOW	None (Non-Designer)	TRUE
CCI-003065	PL-2(3)	LOW	None (Non-Designer)	TRUE
CCI-003067	PL-2(3)	LOW	None (Non-Designer)	TRUE
CCI-000592	PL-4(a)	LOW	None (Non-Designer)	TRUE
CCI-001639	PL-4(a)	LOW	None (Non-Designer)	TRUE

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-000593	PL-4(b)	LOW	None (Non-Designer)	TRUE
CCI-003068	PL-4(c)	LOW	None (Non-Designer)	TRUE
CCI-003069	PL-4(c)	LOW		TRUE
CCI-003070	PL-4(d)	LOW	None (Non-Designer)	TRUE
CCI-000594	PL-4(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-000595	PL-4(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-003071	PL-7(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000577	PL-7(b)	MODERATE		TRUE
CCI-000578	PL-7(b)	MODERATE	None (Non Designer)	TRUE
CCI-003072	PL-8(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003073	PL-8(a)(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003074	PL-8(a)(2)	MODERATE	None (Non Designer)	TRUE
CCI-003075	PL-8(a)(3)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003076	PL-8(b)	MODERATE	None (Non Designer)	TRUE
CCI-003077	PL-8(b)	MODERATE		TRUE
CCI-003078	PL-8(c)	MODERATE	None (Non Designer)	TRUE
CCI-003079	PL-8(c)	MODERATE	None (Non Designer)	TRUE
CCI-003080	PL-8(c)	MODERATE	None (Non Designer)	TRUE
CCI-000073	PM-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-002985	PM-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-001680	PM-1(a)(2)	LOW		TRUE
CCI-002986	PM-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-002984	PM-1(a)(3)	LOW		TRUE
CCI-002987	PM-1(a)(3)	LOW	None (Non-Designer)	TRUE
CCI-000074	PM-1(a)(4)	LOW		TRUE
CCI-002988	PM-1(a)(4)	LOW	None (Non-Designer)	TRUE
CCI-000075	PM-1(b)	LOW	None (Non-Designer)	TRUE
CCI-000076	PM-1(b)	LOW		TRUE
CCI-000077	PM-1(c)	LOW	None (Non-Designer)	TRUE
CCI-002989	PM-1(d)	LOW	None (Non-Designer)	TRUE
CCI-002990	PM-1(d)	LOW	None (Non-Designer)	TRUE
CCI-000078	PM-2	LOW		TRUE
CCI-000080	PM-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000081	PM-3(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000141	PM-3(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-000142	PM-4(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002991	PM-4(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-000170	PM-4(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-002992	PM-4(a)(3)	LOW	Table H-6 (Enclave)	TRUE
CCI-002993	PM-4(b)	LOW	None (Non-Designer)	TRUE
CCI-000207	PM-5	LOW	Table H-4 (Designer)	TRUE
CCI-000209	PM-6	LOW		TRUE
CCI-000210	PM-6	LOW		TRUE
CCI-000211	PM-6	LOW	None (Non-Designer)	TRUE
CCI-000212	PM-7	LOW	None (Non-Designer)	TRUE
CCI-000216	PM-8	LOW	Table H-3 (Removed from LOW)	TRUE

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-001640	PM-8	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-000227	PM-9(a)	LOW		TRUE
CCI-000228	PM-9(b)	LOW		TRUE
CCI-002994	PM-9(c)	LOW		TRUE
CCI-002995	PM-9(c)	LOW		TRUE
CCI-000229	PM-10(a)	LOW		TRUE
CCI-000230	PM-10(a)	LOW		TRUE
CCI-000231	PM-10(a)	LOW		TRUE
CCI-000233	PM-10(b)	LOW		TRUE
CCI-000234	PM-10(c)	LOW		TRUE
CCI-000235	PM-11(a)	LOW		TRUE
CCI-000236	PM-11(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002996	PM-12	LOW	None (Non-Designer)	TRUE
CCI-002997	PM-13	LOW		TRUE
CCI-002998	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-002999	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003000	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003001	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003002	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003003	PM-14(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-003004	PM-14(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-003005	PM-14(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-003006	PM-14(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-003007	PM-14(b)	LOW	None (Non-Designer)	TRUE
CCI-003008	PM-14(b)	LOW	None (Non-Designer)	TRUE
CCI-003009	PM-14(b)	LOW	None (Non-Designer)	TRUE
CCI-003010	PM-15(a)	LOW	None (Non-Designer)	TRUE
CCI-003011	PM-15(b)	LOW	None (Non-Designer)	TRUE
CCI-003012	PM-15(c)	LOW	None (Non-Designer)	TRUE
CCI-003013	PM-16	LOW	None (Non-Designer)	TRUE
CCI-003017	PS-1(a)	LOW	None (Non-Designer)	TRUE
CCI-003018	PS-1(a)	LOW	None (Non-Designer)	TRUE
CCI-001504	PS-1(a)(1)	LOW		TRUE
CCI-001505	PS-1(a)(1)	LOW		TRUE
CCI-001509	PS-1(a)(2)	LOW		TRUE
CCI-001510	PS-1(a)(2)	LOW		TRUE
CCI-001506	PS-1(b)(1)	LOW		TRUE
CCI-001507	PS-1(b)(1)	LOW		TRUE
CCI-001508	PS-1(b)(2)	LOW		TRUE
CCI-001511	PS-1(b)(2)	LOW		TRUE
CCI-001512	PS-2(a)	LOW	None (Non-Designer)	TRUE
CCI-001513	PS-2(b)	LOW		TRUE
CCI-001514	PS-2(c)	LOW	None (Non-Designer)	TRUE
CCI-001515	PS-2(c)	LOW		TRUE
CCI-001516	PS-3(a)	LOW	None (Non-Designer)	TRUE
CCI-001517	PS-3(b)	LOW	None (Non-Designer)	TRUE

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-001518	PS-3(b)	LOW	None (Non-Designer)	TRUE
CCI-001519	PS-3(b)	LOW	None (Non-Designer)	TRUE
CCI-001522	PS-4(a)	LOW	None (Non-Designer)	TRUE
CCI-003022	PS-4(a)	LOW		TRUE
CCI-003023	PS-4(b)	LOW	None (Non-Designer)	TRUE
CCI-001523	PS-4(c)	LOW	None (Non-Designer)	TRUE
CCI-003024	PS-4(c)	LOW	None (Non-Designer)	TRUE
CCI-001524	PS-4(d)	LOW	None (Non-Designer)	TRUE
CCI-001525	PS-4(e)	LOW	None (Non-Designer)	TRUE
CCI-001526	PS-4(e)	LOW	None (Non-Designer)	TRUE
CCI-003016	PS-4(f)	LOW		TRUE
CCI-003025	PS-4(f)	LOW		TRUE
CCI-003026	PS-4(f)	LOW		TRUE
CCI-001527	PS-5(a)	LOW	None (Non-Designer)	TRUE
CCI-001528	PS-5(b)	LOW	None (Non-Designer)	TRUE
CCI-001529	PS-5(b)	LOW		TRUE
CCI-001530	PS-5(b)	LOW		TRUE
CCI-003031	PS-5(c)	LOW	None (Non-Designer)	TRUE
CCI-003032	PS-5(d)	LOW	None (Non-Designer)	TRUE
CCI-003033	PS-5(d)	LOW		TRUE
CCI-003034	PS-5(d)	LOW		TRUE
CCI-003035	PS-6(a)	LOW	None (Non-Designer)	TRUE
CCI-001532	PS-6(b)	LOW	None (Non-Designer)	TRUE
CCI-001533	PS-6(b)	LOW		TRUE
CCI-001531	PS-6(c)(1)	LOW	None (Non-Designer)	TRUE
CCI-003036	PS-6(c)(2)	LOW	None (Non-Designer)	TRUE
CCI-003037	PS-6(c)(2)	LOW		TRUE
CCI-001539	PS-7(a)	LOW		TRUE
CCI-003040	PS-7(b)	LOW	None (Non-Designer)	TRUE
CCI-001540	PS-7(c)	LOW	None (Non-Designer)	TRUE
CCI-003041	PS-7(d)	LOW	None (Non-Designer)	TRUE
CCI-003042	PS-7(d)	LOW		TRUE
CCI-003043	PS-7(d)	LOW		TRUE
CCI-001541	PS-7(e)	LOW	None (Non-Designer)	TRUE
CCI-001542	PS-8(a)	LOW	None (Non-Designer)	TRUE
CCI-003044	PS-8(b)	LOW	None (Non-Designer)	TRUE
CCI-003045	PS-8(b)	LOW		TRUE
CCI-003046	PS-8(b)	LOW		TRUE
CCI-002368	RA-1(a)	LOW		TRUE
CCI-002369	RA-1(a)	LOW		TRUE
CCI-001037	RA-1(a)(1)	LOW		TRUE
CCI-001038	RA-1(a)(1)	LOW		TRUE
CCI-001041	RA-1(a)(2)	LOW		TRUE
CCI-001042	RA-1(a)(2)	LOW		TRUE
CCI-001039	RA-1(b)(1)	LOW		TRUE
CCI-001040	RA-1(b)(1)	LOW		TRUE
CCI-001043	RA-1(b)(2)	LOW		TRUE
CCI-001044	RA-1(b)(2)	LOW		TRUE

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-001045	RA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-001046	RA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-001047	RA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-001048	RA-3(a)	LOW	Table H-4 (Designer)	TRUE
CCI-001049	RA-3(b)	LOW	None (Non-Designer)	TRUE
CCI-001642	RA-3(b)	LOW		TRUE
CCI-001050	RA-3(c)	LOW	None (Non-Designer)	TRUE
CCI-001051	RA-3(c)	LOW		TRUE
CCI-002370	RA-3(d)	LOW	None (Non-Designer)	TRUE
CCI-002371	RA-3(d)	LOW		TRUE
CCI-001052	RA-3(e)	LOW	None (Non-Designer)	TRUE
CCI-001053	RA-3(e)	LOW		TRUE
CCI-001054	RA-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001055	RA-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001056	RA-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001641	RA-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001643	RA-5(a)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001057	RA-5(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001058	RA-5(c)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001059	RA-5(d)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-001060	RA-5(d)	LOW		TRUE
CCI-001061	RA-5(e)	LOW	None (Non-Designer)	TRUE
CCI-002376	RA-5(e)	LOW		TRUE
CCI-001062	RA-5(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001063	RA-5(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001064	RA-5(2)	MODERATE		TRUE
CCI-001067	RA-5(5)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001645	RA-5(5)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002906	RA-5(5)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-003089	SA-1(a)	LOW	None (Non-Designer)	TRUE
CCI-003090	SA-1(a)	LOW	None (Non-Designer)	TRUE
CCI-000602	SA-1(a)(1)	LOW		TRUE
CCI-000603	SA-1(a)(1)	LOW		TRUE
CCI-000605	SA-1(a)(2)	LOW		TRUE
CCI-000606	SA-1(a)(2)	LOW		TRUE
CCI-000601	SA-1(b)(1)	LOW		TRUE

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-000604	SA-1(b)(1)	LOW		TRUE
CCI-000607	SA-1(b)(2)	LOW		TRUE
CCI-001646	SA-1(b)(2)	LOW		TRUE
CCI-003091	SA-2(a)	LOW	None (Non-Designer)	TRUE
CCI-000610	SA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000611	SA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000612	SA-2(b)	LOW	None (Non-Designer)	TRUE
CCI-000613	SA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000614	SA-2(c)	LOW	None (Non-Designer)	TRUE
CCI-000615	SA-3(a)	LOW	None (Non-Designer)	TRUE
CCI-003092	SA-3(a)	LOW	None (Non-Designer)	TRUE
CCI-000616	SA-3(b)	LOW	None (Non-Designer)	TRUE
CCI-000618	SA-3(c)	LOW	None (Non-Designer)	TRUE
CCI-003093	SA-3(d)	LOW	None (Non-Designer)	TRUE
CCI-003094	SA-4(a)	LOW	None (Non-Designer)	TRUE
CCI-003095	SA-4(b)	LOW	None (Non-Designer)	TRUE
CCI-003096	SA-4(c)	LOW	None (Non-Designer)	TRUE
CCI-003097	SA-4(d)	LOW	None (Non-Designer)	TRUE
CCI-003098	SA-4(e)	LOW	None (Non-Designer)	TRUE
CCI-003099	SA-4(f)	LOW	None (Non-Designer)	TRUE
CCI-003100	SA-4(g)	LOW	None (Non-Designer)	TRUE
CCI-000623	SA-4(1)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003101	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003102	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003103	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003104	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003105	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003106	SA-4(2)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003114	SA-4(9)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003116	SA-4(10)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-003124	SA-5(a)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-003125	SA-5(a)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-003126	SA-5(a)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-003127	SA-5(a)(2)	LOW	Table H-4 (Designer)	TRUE
CCI-003128	SA-5(a)(3)	LOW	Table H-4 (Designer)	TRUE
CCI-003129	SA-5(b)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-003130	SA-5(b)(2)	LOW	Table H-4 (Designer)	TRUE
CCI-003131	SA-5(b)(3)	LOW	Table H-4 (Designer)	TRUE
CCI-000642	SA-5(c)	LOW	None (Non-Designer)	TRUE
CCI-003132	SA-5(c)	LOW	None (Non-Designer)	TRUE
CCI-003133	SA-5(c)	LOW	None (Non-Designer)	TRUE
CCI-003134	SA-5(d)	LOW	None (Non-Designer)	TRUE
CCI-003135	SA-5(e)	LOW	None (Non-Designer)	TRUE
CCI-003136	SA-5(e)	LOW		TRUE
CCI-000664	SA-8	MODERATE	None (Non Designer)	TRUE
CCI-000665	SA-8	MODERATE	None (Non Designer)	TRUE
CCI-000666	SA-8	MODERATE	None (Non Designer)	TRUE

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-000667	SA-8	MODERATE	None (Non Designer)	TRUE
CCI-000668	SA-8	MODERATE	None (Non Designer)	TRUE
CCI-000669	SA-9(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000670	SA-9(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-003137	SA-9(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-000671	SA-9(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000672	SA-9(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000673	SA-9(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-000674	SA-9(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-003138	SA-9(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-003139	SA-9(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-003143	SA-9(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-003144	SA-9(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-003155	SA-10(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003156	SA-10(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003157	SA-10(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003158	SA-10(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003159	SA-10(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000692	SA-10(c)	MODERATE	Table H-5 (Designer)	TRUE
CCI-000694	SA-10(d)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003160	SA-10(d)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003161	SA-10(e)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003162	SA-10(e)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003163	SA-10(e)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003164	SA-10(e)	MODERATE	None (Non Designer)	TRUE
CCI-003171	SA-11(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003172	SA-11(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003173	SA-11(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003174	SA-11(b)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003175	SA-11(c)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003176	SA-11(c)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003177	SA-11(d)	MODERATE	Table H-5 (Designer)	TRUE
CCI-003178	SA-11(e)	MODERATE	Table H-5 (Designer)	TRUE
CCI-002378	SC-1(a)	LOW		TRUE
CCI-002380	SC-1(a)	LOW	None (Non-Designer)	TRUE
CCI-001074	SC-1(a)(1)	LOW		TRUE
CCI-001075	SC-1(a)(1)	LOW		TRUE
CCI-002377	SC-1(a)(1)	LOW		TRUE
CCI-001078	SC-1(a)(2)	LOW		TRUE
CCI-001079	SC-1(a)(2)	LOW		TRUE
CCI-002379	SC-1(a)(2)	LOW	None (Non-Designer)	TRUE
CCI-001076	SC-1(b)(1)	LOW		TRUE
CCI-001077	SC-1(b)(1)	LOW		TRUE
CCI-001080	SC-1(b)(2)	LOW		TRUE
CCI-001081	SC-1(b)(2)	LOW		TRUE
CCI-001082	SC-2	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001090	SC-4	MODERATE	Table H-7 (Enclave)	TRUE

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
CCI-001133	SC-10	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001134	SC-10	MODERATE	Table H-5 (Designer)	TRUE
CCI-002428	SC-12	LOW	Table H-6 (Enclave)	TRUE
CCI-002429	SC-12	LOW	Table H-6 (Enclave)	TRUE
CCI-002430	SC-12	LOW	Table H-6 (Enclave)	TRUE
CCI-002431	SC-12	LOW	Table H-6 (Enclave)	TRUE
CCI-002432	SC-12	LOW	Table H-6 (Enclave)	TRUE
CCI-002433	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002434	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002435	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002436	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002437	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002438	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002439	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002440	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002441	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002442	SC-12	LOW	None (Non-Designer)	TRUE
CCI-002449	SC-13	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-002450	SC-13	LOW	Table H-3 (Removed from LOW)	TRUE
CCI-001150	SC-15(a)	LOW	Table H-6 (Enclave)	TRUE

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-001151	SC-15(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001152	SC-15(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001159	SC-17	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002456	SC-17	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001160	SC-18(a)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001161	SC-18(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001162	SC-18(b)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001163	SC-18(c)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001164	SC-18(c)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001165	SC-18(c)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001173	SC-19(a)	MODERATE		FALSE
CCI-001174	SC-19(a)	MODERATE		FALSE
CCI-001175	SC-19(b)	MODERATE		FALSE
CCI-001176	SC-19(b)	MODERATE		FALSE
CCI-001177	SC-19(b)	MODERATE		FALSE
CCI-001178	SC-20(a)	LOW		FALSE
CCI-002462	SC-20(a)	LOW		FALSE
CCI-001179	SC-20(b)	LOW		FALSE
CCI-001663	SC-20(b)	LOW		FALSE
CCI-002465	SC-21	LOW	Table H-6 (Enclave)	TRUE
CCI-002466	SC-21	LOW	Table H-6 (Enclave)	TRUE
CCI-002467	SC-21	LOW	Table H-6 (Enclave)	TRUE
CCI-002468	SC-21	LOW	Table H-6 (Enclave)	TRUE
CCI-001182	SC-22	LOW		FALSE
CCI-001183	SC-22	LOW		FALSE
CCI-001184	SC-23	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-001190	SC-24	MODERATE	Table H-5 (Designer)	TRUE
CCI-001191	SC-24	MODERATE	Table H-5 (Designer)	TRUE
CCI-001192	SC-24	MODERATE	Table H-5 (Designer)	TRUE
CCI-001193	SC-24	MODERATE	Table H-5 (Designer)	TRUE
CCI-001665	SC-24	MODERATE	Table H-5 (Designer)	TRUE
CCI-001199	SC-28	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002472	SC-28	MODERATE	Table H-5 (Designer)	TRUE
CCI-002530	SC-39	LOW	Table H-4 (Designer)	TRUE
CCI-002546	SC-41	LOW	Table H-4 (Designer)	TRUE
CCI-002544	SC-41	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002545	SC-41	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002601	SI-1(a)	LOW		TRUE

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-001217	SI-1(a)(1)	LOW		TRUE
CCI-001218	SI-1(a)(1)	LOW	None (Non-Designer)	TRUE
CCI-001220	SI-1(a)(2)	LOW		TRUE
CCI-001221	SI-1(a)(2)	LOW		TRUE
CCI-001219	SI-1(b)(1)	LOW		TRUE
CCI-001223	SI-1(b)(1)	LOW		TRUE
CCI-001222	SI-1(b)(2)	LOW		TRUE
CCI-001224	SI-1(b)(2)	LOW		TRUE
CCI-001227	SI-2(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001225	SI-2(a)	LOW	None (Non-Designer)	TRUE
CCI-001226	SI-2(a)	LOW	None (Non-Designer)	TRUE
CCI-001228	SI-2(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001229	SI-2(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002602	SI-2(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002603	SI-2(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-002604	SI-2(c)	LOW		TRUE
CCI-002605	SI-2(c)	LOW	None (Non-Designer)	TRUE
CCI-002606	SI-2(c)	LOW		TRUE
CCI-002607	SI-2(c)	LOW	None (Non-Designer)	TRUE
CCI-001230	SI-2(d)	LOW	None (Non-Designer)	TRUE
CCI-001233	SI-2(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001234	SI-2(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002619	SI-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002620	SI-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002621	SI-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002622	SI-3(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001240	SI-3(b)	LOW	None (Non-Designer)	TRUE
CCI-001241	SI-3(c)(1)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002623	SI-3(c)(1)	LOW	Table H-4 (Designer)	TRUE
CCI-001242	SI-3(c)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002624	SI-3(c)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-001243	SI-3(c)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-001244	SI-3(c)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-001245	SI-3(d)	LOW	None (Non-Designer)	TRUE
CCI-001246	SI-3(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001247	SI-3(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001253	SI-4(a)(1)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002641	SI-4(a)(1)	LOW	Table H-6 (Enclave)	TRUE
CCI-002644	SI-4(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-002642	SI-4(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-002643	SI-4(a)(2)	LOW	Table H-6 (Enclave)	TRUE
CCI-002645	SI-4(b)	LOW	Table H-4 (Designer) Table H-6 (Enclave)	TRUE
CCI-002646	SI-4(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001255	SI-4(c)	LOW	None (Non-Designer)	TRUE
CCI-001256	SI-4(c)	LOW	Table H-6 (Enclave)	TRUE

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-002647	SI-4(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-002648	SI-4(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-002649	SI-4(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-001257	SI-4(e)	LOW	Table H-6 (Enclave)	TRUE
CCI-001258	SI-4(f)	LOW	Table H-6 (Enclave)	TRUE
CCI-002650	SI-4(g)	LOW	Table H-6 (Enclave)	TRUE
CCI-002651	SI-4(g)	LOW	Table H-6 (Enclave)	TRUE
CCI-002652	SI-4(g)	LOW	Table H-6 (Enclave)	TRUE
CCI-002654	SI-4(g)	LOW	Table H-6 (Enclave)	TRUE
CCI-001260	SI-4(2)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002659	SI-4(4)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002660	SI-4(4)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002661	SI-4(4)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002662	SI-4(4)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001264	SI-4(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002663	SI-4(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002664	SI-4(5)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-001285	SI-5(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-002692	SI-5(a)	LOW	Table H-6 (Enclave)	TRUE
CCI-001286	SI-5(b)	LOW	Table H-6 (Enclave)	TRUE
CCI-001287	SI-5(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-001288	SI-5(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-002693	SI-5(c)	LOW	Table H-6 (Enclave)	TRUE
CCI-002694	SI-5(c)	LOW		TRUE
CCI-001289	SI-5(d)	LOW	Table H-6 (Enclave)	TRUE
CCI-002703	SI-7	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002704	SI-7	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002705	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002706	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002707	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002710	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002711	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002712	SI-7(1)	MODERATE	Table H-5 (Designer) Table H-7 (Enclave)	TRUE
CCI-002708	SI-7(1)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002709	SI-7(1)	MODERATE		TRUE
CCI-002719	SI-7(7)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002720	SI-7(7)	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002741	SI-8(a)	MODERATE		FALSE
CCI-002742	SI-8(a)	MODERATE		FALSE
CCI-001306	SI-8(b)	MODERATE		FALSE
CCI-001307	SI-8(1)	MODERATE		FALSE

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-001308	SI-8(2)	MODERATE		FALSE
CCI-001310	SI-10	MODERATE	Table H-5 (Designer)	TRUE
CCI-002744	SI-10	MODERATE	Table H-5 (Designer)	TRUE
CCI-001312	SI-11(a)	MODERATE	Table H-5 (Designer)	TRUE
CCI-001314	SI-11(b)	MODERATE	None (Non Designer)	TRUE
CCI-002759	SI-11(b)	MODERATE	None (Non Designer)	TRUE
CCI-001315	SI-12	LOW	None (Non-Designer)	TRUE
CCI-001678	SI-12	LOW	None (Non-Designer)	TRUE
CCI-002823	SI-16	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002824	SI-16	MODERATE	Table H-7 (Enclave)	TRUE
CCI-002773	SI-17	LOW	Table H-4 (Designer)	TRUE
CCI-002774	SI-17	LOW	Table H-4 (Designer)	TRUE
CCI-002775	SI-17	LOW	Table H-4 (Designer)	TRUE

Table H-2 CCIs Not Applicable to Control Systems (CS)			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for non-inclusion**
CCI-001473	AC-22(a)	The organization designates individuals authorized to post information onto a publicly accessible information system.	Control Systems are not publically accessible
CCI-001474	AC-22(b)	The organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information.	Control Systems are not publically accessible
CCI-001475	AC-22(c)	The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.	Control Systems are not publically accessible
CCI-001476	AC-22(d)	The organization reviews the content on the publicly accessible information system for nonpublic information on an organization-defined frequency.	Control Systems are not publically accessible
CCI-001477	AC-22(d)	The organization defines a frequency for reviewing the content on the publicly accessible information system for nonpublic information.	Control Systems are not publically accessible
CCI-001478	AC-22(e)	The organization removes nonpublic information from the publicly accessible information system, if discovered.	Control Systems are not publically accessible
CCI-001384	AC-8(c)(1)	The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access.	Control Systems are not publically accessible
CCI-001385	AC-8(c)(2)	The information system, for publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.	Control Systems are not publically accessible
CCI-001386	AC-8(c)(2)	The information system for publicly accessible systems displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.	Control Systems are not publically accessible
CCI-001387	AC-8(c)(2)	The information system for publicly accessible systems displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.	Control Systems are not publically accessible
CCI-001388	AC-8(c)(3)	The information system, for publicly accessible systems, includes a description of the authorized uses of the system.	Control Systems are not publically accessible
CCI-001739	CM-2(7)a	The organization issues organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations the organization deems to be of significant risk.	Control Systems aren't mobile.

Table H-2 CCIs Not Applicable to Control Systems (CS)			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for non-inclusion**
CCI-001815	CM-2(7)b	The organization defines the security safeguards to be applied to devices when they return from areas of significant risk.	Control Systems aren't mobile.
CCI-001816	CM-2(7)b	The organization applies organization-defined security safeguards to devices when individuals return from areas of significant risk.	Control Systems aren't mobile.
CCI-000474	CP-2(3)	The organization defines the time period for planning the resumption of essential business functions as a result of contingency plan activation.	Control Systems are not business systems
CCI-000476	CP-2(3)	The organization plans for the resumption of essential business functions within the organization-defined time period of contingency plan activation.	Control Systems are not business systems
CCI-002829	CP-2(8)	The organization identifies critical information system assets supporting essential business functions.	Control Systems are not business systems
CCI-000444	CP-2(a)(1)	The organization develops a contingency plan for the information system that identifies essential business functions.	Control Systems are not business systems
CCI-000451	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system disruption.	Control Systems are not business systems
CCI-000453	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system compromise.	Control Systems are not business systems
CCI-000455	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential business functions despite an information system failure.	Control Systems are not business systems
CCI-000514	CP-7(a)	The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential business functions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.	Control Systems are not business systems
CCI-000523	CP-8	The organization defines the time period to permit the resumption of organization-defined information system operations for essential business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Control Systems are not business systems

Table H-2 CCIs Not Applicable to Control Systems (CS)			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for non-inclusion**
CCI-000525	CP-8	The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential business functions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Control Systems are not business systems
CCI-002841	CP-8	The organization defines the information system operations to be resumed for essential business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Control Systems are not business systems
CCI-000963	PE-12	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Control Systems do not need lighting, it functions perfectly well in the dark
CCI-001173	SC-19(a)	The organization establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	Control Systems do not use VoIP
CCI-001174	SC-19(a)	The organization establishes implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.	Control Systems do not use VoIP
CCI-001175	SC-19(b)	The organization authorizes the use of VoIP within the information system.	Control Systems do not use VoIP
CCI-001176	SC-19(b)	The organization monitors the use of VoIP within the information system.	Control Systems do not use VoIP
CCI-001177	SC-19(b)	The organization controls the use of VoIP within the information system.	Control Systems do not use VoIP
CCI-001178	SC-20(a)	The information system provides additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	Control Systems do not act as DNS server for external clients
CCI-002462	SC-20(a)	The information system provides additional integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.	Control Systems do not act as DNS server for external clients
CCI-001179	SC-20(b)	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child zones.	Control Systems do not act as DNS server for external clients

Table H-2 CCIs Not Applicable to Control Systems (CS)			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for non-inclusion**
CCI-001663	SC-20(b)	The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).	Control Systems do not act as DNS server for external clients
CCI-001182	SC-22	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant.	Control Systems do not act as DNS server for external clients
CCI-001183	SC-22	The information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.	Control Systems do not act as DNS server for external clients
CCI-002395	SC-7(b)	The information system implements subnetworks for publicly accessible system components that are physically and/or logically separated from internal organizational networks.	Control Systems are not publically accessible
CCI-002741	SI-8(a)	The organization employs spam protection mechanisms at information system entry points to detect and take action on unsolicited messages.	Control System doesn't use incoming email.
CCI-002742	SI-8(a)	The organization employs spam protection mechanisms at information system exit points to detect and take action on unsolicited messages.	Control System doesn't use incoming email.
CCI-001306	SI-8(b)	The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Control System doesn't use incoming email.
CCI-001307	SI-8(1)	The organization centrally manages spam protection mechanisms.	Control System doesn't use incoming email.
CCI-001308	SI-8(2)	The information system automatically updates spam protection mechanisms.	Control System doesn't use incoming email.

Table H-3 CCIs Removed from LOW Impact Control Systems Baseline			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for removal from the LOW baseline**
CCI-000443	CP-2(a)(1)	The organization develops a contingency plan for the information system that identifies essential missions.	A LOW CS doesn't have any "essential" mission
CCI-000450	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system disruption.	A LOW CS doesn't have any "essential" mission
CCI-000452	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system compromise.	A LOW CS doesn't have any "essential" mission
CCI-000454	CP-2(a)(4)	The organization develops a contingency plan for the information system that addresses maintaining essential missions despite an information system failure.	A LOW CS doesn't have any "essential" mission
CCI-002955	PE-11	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.	NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "CS may support critical activities....". By definition, a CS supporting "critical activities" is not a LOW system.
CCI-000961	PE-11(1)	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	NIST 800-53 does not have this in a LOW baseline. NIST 800-82 included it with the rationale "CS may support critical activities....". By definition, a CS supporting "critical activities" is not a LOW system.
CCI-000216	PM-8	The organization develops and documents a critical infrastructure and key resource protection plan that addresses information security issues.	A LOW Control System doesn’t deal with critical infrastructure.
CCI-001640	PM-8	The organization updates the critical infrastructure and key resources protection plan that addresses information security issues.	A LOW Control System doesn’t deal with critical infrastructure.
CCI-002449	SC-13	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.	A LOW CS doesn't have any classified information

Table H-3 CCIs Removed from LOW Impact Control Systems Baseline			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Rationale for removal from the LOW baseline**
CCI-002450	SC-13	The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	A LOW CS doesn't have any classified information

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
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-Defined Enclave Designer Impractical
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.	Enclave Designer Impractical
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).	Enclave Designer Impractical
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).	Enclave Designer Non-Designer Impractical

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.	Enclave Designer Non-Designer
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.	Enclave Designer Non-Designer
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.	Enclave Designer Non-Designer
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.	Enclave Designer Non-Designer
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Enclave Designer Impractical
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.	Enclave Designer Impractical
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.	Enclave Designer Impractical
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity Verification (PIV) credentials.	Enclave Designer Impractical
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.	DoD-Defined Enclave Designer Impractical
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.	Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.	Enclave Designer
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.	Enclave Designer
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.	Enclave Designer
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.	Enclave Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the minimum number of special characters used.	Enclave Designer
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.	Enclave Designer
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-protected passwords.	Enclave Designer Impractical
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.	Enclave Designer
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.	Enclave Designer
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.	Enclave Designer Non-Designer Impractical
CCI-001618	IA-5(1)(e)	The organization defines the number of generations for which password reuse is prohibited.	DoD-Defined Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.	DoD-Defined Enclave Designer Impractical
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	Enclave Designer Impractical
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.	Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.	Enclave Designer Non-Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Enclave Designer Non-Designer
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.	Enclave Designer Non-Designer
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.	DoD-Defined Enclave Designer Impractical
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported.	Enclave Designer Non-Designer
CCI-001641	RA-5(a)	The organization defines the process for conducting random vulnerability scans on the information system and hosted applications.	Enclave Designer Non-Designer 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.	Enclave Designer Non-Designer
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability 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.	Enclave Designer Non-Designer Impractical
CCI-001058	RA-5(c)	The organization analyzes vulnerability scan reports and results from security control assessments.	Enclave Designer Non-Designer
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.	Enclave Designer Non-Designer Impractical
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.	Enclave Designer Impractical
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.	Enclave Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Enclave Designer
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.	Enclave Designer Non-Designer
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.	DoD-Defined Enclave Designer Impractical
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.	Enclave Designer Non-Designer
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.	Enclave Designer Non-Designer
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.	Enclave Designer Non-Designer
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-Defined Enclave Designer Impractical
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.	Enclave Designer Non-Designer
CCI-002110	AC-2(a)	The organization defines the information system account types that support the organizational missions/business functions.	Designer
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.	Designer
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-Defined Designer Impractical
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.	Designer
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-Defined Designer Impractical

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-002236	AC-7(b)	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-Defined Designer Impractical
CCI-002237	AC-7(b)	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-Defined Designer Impractical
CCI-002238	AC-7(b)	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.	Designer Impractical
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.	Designer
CCI-000232	AC-14(b)	The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	Designer
CCI-001438	AC-18(a)	The organization establishes usage restrictions for wireless access.	Designer Non-Designer
CCI-001439	AC-18(a)	The organization establishes implementation guidance for wireless access.	Designer Non-Designer
CCI-002323	AC-18(a)	The organization establishes configuration/connection requirements for wireless access.	Designer Non-Designer
CCI-001441	AC-18(b)	The organization authorizes wireless access to the information system prior to allowing such connections.	Designer Non-Designer
CCI-000123	AU-2(a)	The organization determines the information system must be capable of auditing an organization-defined list of auditable events.	Designer Non-Designer
CCI-001571	AU-2(a)	The organization defines the information system auditable events.	DoD-Defined Designer Impractical
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.	Designer Non-Designer
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.	Designer Non-Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-000130	AU-3	The information system generates audit records containing information that establishes what type of event occurred.	Designer
CCI-000131	AU-3	The information system generates audit records containing information that establishes when an event occurred.	Designer
CCI-000132	AU-3	The information system generates audit records containing information that establishes where the event occurred.	Designer
CCI-000133	AU-3	The information system generates audit records containing information that establishes the source of the event.	Designer
CCI-000134	AU-3	The information system generates audit records containing information that establishes the outcome of the event.	Designer
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.	Designer Impractical
CCI-001848	AU-4	The organization defines the audit record storage requirements.	Designer Non-Designer
CCI-001849	AU-4	The organization allocates audit record storage capacity in accordance with organization-defined audit record storage requirements.	Designer Non-Designer
CCI-000159	AU-8(a)	The information system uses internal system clocks to generate time stamps for audit records.	Designer
CCI-001889	AU-8(b)	The information system records time stamps for audit records that meets organization-defined granularity of time measurement.	Designer
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).	Designer
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.	Designer
CCI-001459	AU-12(a)	The organization defines information system components that provide audit record generation capability.	DoD-Defined Designer Impractical
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.	Designer Impractical
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-Defined Designer Impractical

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer
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.	Designer
CCI-002103	CA-9(b)	The organization documents, for each internal connection, the interface characteristics.	Designer
CCI-002104	CA-9(b)	The organization documents, for each internal connection, the security requirements.	Designer
CCI-002105	CA-9(b)	The organization documents, for each internal connection, the nature of the information communicated.	Designer
CCI-000293	CM-2	The organization develops and documents a current baseline configuration of the information system.	Designer
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.	Designer
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.	Designer
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-Defined Designer Non-Designer Impractical
CCI-001588	CM-6(a)	The organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements.	DoD-Defined Designer Non-Designer Impractical
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-Defined Designer Non-Designer Impractical
CCI-000381	CM-7(a)	The organization configures the information system to provide only essential capabilities.	Designer
CCI-000380	CM-7(b)	The organization defines for the information system prohibited or restricted functions, ports, protocols, and/or services.	Designer
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.	Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer
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.	Designer Impractical
CCI-000389	CM-8(a)(1)	The organization develops and documents an inventory of information system components that accurately reflects the current information system.	Designer
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.	Designer
CCI-000398	CM-8(a)(4)	The organization defines information deemed necessary to achieve effective information system component accountability.	DoD-Defined Designer Non-Designer Impractical
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.	Designer
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.	Designer
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.	Designer
CCI-000176	IA-5(b)	The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization.	Designer Non-Designer
CCI-001544	IA-5(c)	The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.	Designer Non-Designer Impractical
CCI-001989	IA-5(e)	The organization manages information system authenticators by changing default content of authenticators prior to information system installation.	Designer
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.	DoD-Defined Designer Non-Designer Impractical
CCI-001610	IA-5(g)	The organization defines the time period (by authenticator type) for changing/refreshing authenticators.	DoD-Defined Designer Non-Designer Impractical

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-001611	IA-5(1)(a)	The organization defines the minimum number of special characters for password complexity enforcement.	DoD-Defined Designer Impractical
CCI-001612	IA-5(1)(a)	The organization defines the minimum number of upper case characters for password complexity enforcement.	DoD-Defined Designer Impractical
CCI-001613	IA-5(1)(a)	The organization defines the minimum number of lower case characters for password complexity enforcement.	DoD-Defined Designer Impractical
CCI-001614	IA-5(1)(a)	The organization defines the minimum number of numeric characters for password complexity enforcement.	DoD-Defined Designer Impractical
CCI-001615	IA-5(1)(b)	The organization defines the minimum number of characters that are changed when new passwords are created.	DoD-Defined Designer Impractical
CCI-000198	IA-5(1)(d)	The information system enforces minimum password lifetime restrictions.	Designer Impractical
CCI-001616	IA-5(1)(d)	The organization defines minimum password lifetime restrictions.	DoD-Defined Designer Impractical
CCI-001617	IA-5(1)(d)	The organization defines maximum password lifetime restrictions.	DoD-Defined Designer Impractical
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.	Designer Non-Designer
CCI-000207	PM-5	The organization develops and maintains an inventory of its information systems.	Designer Non-Designer Impractical
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 unauthorized access, use, disclosure, disruption, modification, or destruction.	Designer Non-Designer
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.	Designer Non-Designer
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.	Designer Non-Designer
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.	Designer Non-Designer

Table H-4 Designer CCIs for LOW and MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer Non-Designer
CCI-003128	SA-5(a)(3)	The organization obtains administrator 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.	Designer Non-Designer
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.	Designer Non-Designer
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 service in a more secure manner.	Designer Non-Designer
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.	Designer Non-Designer
CCI-002530	SC-39	The information system maintains a separate execution domain for each executing process.	Designer
CCI-002546	SC-41	The organization physically disables or removes organization-defined connection ports or input/output devices on organization-defined information systems or information system components.	Designer Impractical
CCI-002623	SI-3(c)(1)	The organization defines the frequency for performing periodic scans of the information system for malicious code.	DoD-Defined Designer 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.	Designer
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.	Designer
CCI-002775	SI-17	The information system implements organization-defined fail-safe procedures when organization-defined failure conditions occur.	Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	DoD-Defined Enclave Designer Non-Designer Impractical
CCI-001361	AC-2(2)	The organization defines a time period after which temporary accounts are automatically terminated.	DoD-Defined Enclave Designer Non-Designer Impractical
CCI-001365	AC-2(2)	The organization defines a time period after which emergency accounts are automatically terminated.	DoD-Defined Enclave Designer Non-Designer Impractical
CCI-000017	AC-2(3)	The information system automatically disables inactive accounts after an organization-defined time period.	DoD-Defined Enclave Designer Non-Designer Impractical
CCI-000217	AC-2(3)	The organization defines a time period after which inactive accounts are automatically disabled.	DoD-Defined Designer Impractical
CCI-000018	AC-2(4)	The information system automatically audits account creation actions.	Enclave Designer Impractical
CCI-001403	AC-2(4)	The information system automatically audits account modification actions.	Enclave Designer Impractical
CCI-001404	AC-2(4)	The information system automatically audits account disabling actions.	Enclave Designer Impractical
CCI-001405	AC-2(4)	The information system automatically audits account removal actions.	Enclave Designer Impractical
CCI-002130	AC-2(4)	The information system automatically audits account enabling actions.	Enclave Designer Impractical
CCI-001683	AC-2(4)	The information system notifies organization-defined personnel or roles for account creation actions.	Enclave Designer
CCI-001684	AC-2(4)	The information system notifies organization-defined personnel or roles for account modification actions.	Enclave Designer
CCI-001685	AC-2(4)	The information system notifies organization-defined personnel or roles for account disabling actions.	Enclave Designer
CCI-001686	AC-2(4)	The information system notifies organization-defined personnel or roles for account removal actions.	Enclave Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-002132	AC-2(4)	The information system notifies organization-defined personnel or roles for account enabling actions.	Enclave Designer
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.	Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-001548	AC-4	The organization defines the information flow control policies for controlling the flow of information within the system.	Enclave Designer Non-Designer Impractical
CCI-001549	AC-4	The organization defines the information flow control policies for controlling the flow of information between interconnected systems.	Enclave Designer Non-Designer Impractical
CCI-001550	AC-4	The organization defines approved authorizations for controlling the flow of information within the system.	Enclave Designer Non-Designer Impractical
CCI-001551	AC-4	The organization defines approved authorizations for controlling the flow of information between interconnected systems.	Enclave Designer Non-Designer Impractical
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-Defined Designer Impractical
CCI-002221	AC-6(1)	The organization defines the security-relevant information for which access must be explicitly authorized.	DoD-Defined Designer Impractical
CCI-002222	AC-6(1)	The organization explicitly authorizes access to organization-defined security functions.	DoD-Defined Designer Impractical
CCI-002223	AC-6(1)	The organization explicitly authorizes access to organization-defined security-relevant information.	DoD-Defined Designer Impractical
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.	DoD-Defined Designer Impractical
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-Defined Designer Impractical

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-002234	AC-6(9)	The information system audits the execution of privileged functions.	Designer Impractical
CCI-002235	AC-6(10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Designer Impractical
CCI-000058	AC-11(a)	The information system provides the capability for users to directly initiate session lock mechanisms.	Enclave Designer Impractical
CCI-000059	AC-11(a)	The organization defines the time period of inactivity after which the information system initiates a session lock.	DoD-Defined Enclave Designer Impractical
CCI-000056	AC-11(b)	The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.	Enclave Designer Impractical
CCI-000060	AC-11(1)	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-002361	AC-12	The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.	Enclave Designer Impractical
CCI-001443	AC-18(1)	The information system protects wireless access to the system using authentication of users and/or devices.	Designer Impractical
CCI-001444	AC-18(1)	The information system protects wireless access to the system using encryption.	Designer Impractical
CCI-000135	AU-3(1)	The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.	Designer Impractical
CCI-001488	AU-3(1)	The organization defines additional, more detailed information to be included in the audit records.	Designer Non-Designer
CCI-001875	AU-7(a)	The information system provides an audit reduction capability that supports on-demand audit review and analysis.	Enclave Designer Impractical
CCI-001876	AU-7(a)	The information system provides an audit reduction capability that supports on-demand reporting requirements.	Enclave Designer Impractical
CCI-001877	AU-7(a)	The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.	Enclave Designer Impractical

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-001878	AU-7(a)	The information system provides a report generation capability that supports on-demand audit review and analysis.	Enclave Designer Impractical
CCI-001879	AU-7(a)	The information system provides a report generation capability that supports on-demand reporting requirements.	Enclave Designer Impractical
CCI-001880	AU-7(a)	The information system provides a report generation capability that supports after-the-fact investigations of security incidents.	Enclave Designer Impractical
CCI-001881	AU-7(b)	The information system provides an audit reduction capability that does not alter original content or time ordering of audit records.	Enclave Designer Impractical
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.	Enclave Designer Impractical
CCI-000158	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.	Enclave Designer Impractical
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.	Designer
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.	Designer Non-Designer
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.	Designer
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.	Designer Non-Designer
CCI-001737	CM-2(7)a	The organization defines the information systems, system components, or devices that are to have organization-defined configurations applied when located in areas of significant risk.	Designer Non-Designer
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.	Designer Non-Designer
CCI-001592	CM-7(2)	The organization defines the rules authorizing the terms and conditions of software program usage on the information system.	Designer
CCI-001763	CM-7(2)	The organization defines the policies regarding software program usage and restrictions.	Designer Non-Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer
CCI-001772	CM-7(5)a	The organization defines the software programs authorized to execute on the information system.	Designer
CCI-001773	CM-7(5)a	The organization identifies the organization-defined software programs authorized to execute on the information system.	Designer
CCI-001774	CM-7(5)b	The organization employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.	Designer
CCI-002828	CP-2(8)	The organization identifies critical information system assets supporting essential missions.	Designer
CCI-000553	CP-10(2)	The information system implements transaction recovery for systems that are transaction-based.	Designer
CCI-000766	IA-2(2)	The information system implements multifactor authentication for network access to non-privileged accounts.	Enclave Designer Impractical
CCI-000767	IA-2(3)	The information system implements multifactor authentication for local access to privileged accounts.	Enclave Designer Impractical
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-Defined Designer Impractical
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.	Designer Impractical
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.	Enclave Designer Impractical
CCI-000186	IA-5(2)(b)	The information system, for PKI-based authentication enforces authorized access to the corresponding private key.	Enclave Designer
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.	Enclave Designer
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.	Enclave Designer
CCI-000865	MA-3	The organization approves information system maintenance tools.	Designer Non-Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer Non-Designer
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.	Designer Non-Designer
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.	Designer Non-Designer
CCI-000937	PE-5	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Designer Non-Designer
CCI-000952	PE-9	The organization protects power equipment and power cabling for the information system from damage and destruction.	Designer Non-Designer
CCI-002953	PE-9(1)	The organization employs redundant power cabling paths that are physically separated by organization-defined distance.	Designer Non-Designer
CCI-002954	PE-9(1)	The organization defines the distance to physically separate redundant power cabling paths.	Designer Non-Designer
CCI-002955	PE-11	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.	Enclave Designer Impractical
CCI-000961	PE-11(1)	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Enclave Designer
CCI-003071	PL-7(a)	The organization develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security.	Designer Non-Designer
CCI-003072	PL-8(a)	The organization develops an information security architecture for the information system.	Designer Non-Designer
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.	Designer Non-Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-003075	PL-8(a)(3)	The organization's information security architecture for the information system describes any information security assumptions about, and dependencies on, external services.	Designer Non-Designer
CCI-001062	RA-5(1)	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Enclave Designer
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.	Enclave Designer
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-Defined Enclave Designer Impractical
CCI-002906	RA-5(5)	The organization defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components.	Enclave Designer
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.	Designer Non-Designer Impractical
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 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.	Designer Non-Designer Impractical
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 implementation information at organization-defined level of detail.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer Non-Designer Impractical
CCI-003105	SA-4(2)	The organization defines 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, or information system services.	Designer Non-Designer Impractical
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.	Designer Non-Designer 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 for organizational use.	Designer Non-Designer Impractical
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, implementation and/or operation.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
CCI-000692	SA-10(c)	The organization requires the developer of the information system, system component, or information system service to implement only organization-approved changes to the system, component, or service.	Designer Non-Designer Impractical

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
CCI-003161	SA-10(e)	The organization requires the developer of the information system, system component, or information system service to track security flaws within the system, component, or service.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
CCI-003171	SA-11(a)	The organization requires the developer of the information system, system component, or information system service to create a security assessment plan.	Designer Non-Designer Impractical
CCI-003172	SA-11(a)	The organization requires the developer of the information system, system component, or information system service to implement a security assessment plan.	Designer Non-Designer Impractical
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-defined depth and coverage.	Designer Non-Designer Impractical
CCI-003174	SA-11(b)	The organization defines the depth and coverage to perform unit, integration, system, and/or regression testing/evaluation.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
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 testing/evaluation.	Designer Non-Designer Impractical

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Designer Non-Designer Impractical
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.	Designer Non-Designer Impractical
CCI-001082	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	Enclave Designer Non-Designer
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).	Enclave Designer
CCI-001126	SC-7(18)	The information system fails securely in the event of an operational failure of a boundary protection device.	Designer Impractical
CCI-002418	SC-8	The information system protects the confidentiality and/or integrity of transmitted information.	Designer
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-Defined Designer
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.	Designer
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.	Enclave Designer Impractical
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-Defined Designer Impractical
CCI-002449	SC-13	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.	DoD-Defined Enclave Designer Impractical
CCI-002450	SC-13	The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Enclave Designer Impractical
CCI-001160	SC-18(a)	The organization defines acceptable and unacceptable mobile code and mobile code technologies.	Enclave Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
CCI-001161	SC-18(b)	The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.	Enclave Designer
CCI-001162	SC-18(b)	The organization establishes implementation guidance for acceptable mobile code and mobile code technologies.	Enclave Designer
CCI-001163	SC-18(c)	The organization authorizes the use of mobile code within the information system.	Enclave Designer
CCI-001164	SC-18(c)	The organization monitors the use of mobile code within the information system.	Enclave Designer
CCI-001165	SC-18(c)	The organization controls the use of mobile code within the information system.	Enclave Designer
CCI-001184	SC-23	The information system protects the authenticity of communications sessions.	Enclave Designer Impractical
CCI-001190	SC-24	The information system fails to an organization-defined known-state for organization-defined types of failures.	Designer
CCI-001191	SC-24	The organization defines the known states the information system should fail to in the event of an organization-defined system failure.	DoD-Defined Designer Impractical
CCI-001192	SC-24	The organization defines types of failures for which the information system should fail to an organization-defined known state.	DoD-Defined Designer Impractical
CCI-001193	SC-24	The organization defines system state information that should be preserved in the event of a system failure.	DoD-Defined Designer Impractical
CCI-001665	SC-24	The information system preserves organization-defined system state information in the event of a system failure.	Designer Impractical
CCI-001199	SC-28	The information system protects the confidentiality and/or integrity of organization-defined information at rest.	Enclave Designer Impractical
CCI-002472	SC-28	The organization defines the information at rest that is to be protected by the information system.	Designer Non-Designer 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.	Enclave Designer
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed.	Enclave Designer
CCI-002706	SI-7(1)	The organization defines the firmware on which integrity checks will be performed.	Enclave Designer
CCI-002707	SI-7(1)	The organization defines the information on which integrity checks will be performed.	Enclave Designer

Table H-5 Additional Designer CCIs for MODERATE Impact Control Systems			
CCI #	**800-53 Control Text Indicator**	**CCI Definition**	**Responsibility**
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.	Enclave Designer
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.	Enclave Designer
CCI-002712	SI-7(1)	The information system performs an integrity check of organization-defined information at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.	Enclave Designer
CCI-001310	SI-10	The information system checks the validity of organization-defined inputs.	Designer Non-Designer
CCI-002744	SI-10	The organization defines the inputs the information system is to conduct validity checks.	DoD-Defined Designer
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.	Designer

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
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.
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.
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.
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.
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.
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.
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.
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.
CCI-000063	AC-17(a)	The organization defines allowed methods of remote access to the information system.
CCI-002310	AC-17(a)	The organization establishes and documents usage restrictions for each type of remote access allowed.
CCI-002311	AC-17(a)	The organization establishes and documents configuration/connection requirements for each type of remote access allowed.
CCI-002312	AC-17(a)	The organization establishes and documents implementation guidance for each type of remote access allowed.
CCI-000065	AC-17(b)	The organization authorizes remote access to the information system prior to allowing such connections
CCI-000082	AC-19(a)	The organization establishes usage restrictions for organization controlled mobile devices.
CCI-000083	AC-19(a)	The organization establishes implementation guidance for organization controlled mobile devices.
CCI-002325	AC-19(a)	The organization establishes configuration requirements for organization controlled mobile devices.
CCI-002326	AC-19(a)	The organization establishes connection requirements for organization controlled mobile devices.
CCI-000084	AC-19(b)	The organization authorizes connection of mobile devices to organizational information systems.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000093	AC-20(a)	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.
CCI-000098	AC-21(a)	The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information circumstances where user discretion is required.
CCI-001470	AC-21(a)	The organization defines information sharing circumstances where user discretion is required.
CCI-001471	AC-21(b)	The organization employs organization-defined automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.
CCI-001472	AC-21(b)	The organization defines the automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions.
CCI-000139	AU-5(a)	The information system alerts designated organization-defined personnel or roles 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).
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).
CCI-000162	AU-9	The information system protects audit information from unauthorized access.
CCI-000163	AU-9	The information system protects audit information from unauthorized modification.
CCI-000164	AU-9	The information system protects audit information from unauthorized deletion.
CCI-001493	AU-9	The information system protects audit tools from unauthorized access.
CCI-001494	AU-9	The information system protects audit tools from unauthorized modification.
CCI-001495	AU-9	The information system protects audit tools from unauthorized deletion.
CCI-000257	CA-3(a)	The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.
CCI-000258	CA-3(b)	The organization documents, for each interconnection, the interface characteristics.
CCI-000259	CA-3(b)	The organization documents, for each interconnection, the security requirements.
CCI-000260	CA-3(b)	The organization documents, for each interconnection, the nature of the information communicated.
CCI-001732	CM-10(c)	The organization controls the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001733	CM-10(c)	The organization documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CCI-000535	CP-9(a)	The organization conducts backups of user-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.
CCI-000537	CP-9(b)	The organization conducts backups of system-level information contained in the information system per organization-defined frequency that is consistent with recovery time and recovery point objectives.
CCI-000539	CP-9(c)	The organization conducts backups of information system documentation including security-related documentation per organization-defined frequency that is consistent with recovery time and recovery point objectives.
CCI-000540	CP-9(d)	The organization protects the confidentiality, integrity, and availability of backup information at storage locations.
CCI-000550	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption.
CCI-000551	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a compromise.
CCI-000552	CP-10	The organization provides for the recovery and reconstitution of the information system to a known state after a failure.
CCI-001933	IA-1(a)	The organization defines the personnel or roles to be recipients of the identification and authentication policy and the procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
CCI-001934	IA-1(a)	The organization documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
CCI-000756	IA-1(a)(1)	The organization develops an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CCI-000757	IA-1(a)(1)	The organization disseminates to organization defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CCI-001932	IA-1(a)(1)	The organization documents an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CCI-000760	IA-1(a)(2)	The organization develops procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
CCI-000761	IA-1(a)(2)	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000758	IA-1(b)(1)	The organization reviews and updates identification and authentication policy in accordance with the organization defined frequency.
CCI-000759	IA-1(b)(1)	The organization defines a frequency for reviewing and updating the identification and authentication policy.
CCI-000762	IA-1(b)(2)	The organization reviews and updates identification and authentication procedures in accordance with the organization defined frequency.
CCI-000763	IA-1(b)(2)	The organization defines a frequency for reviewing and updating the identification and authentication procedures.
CCI-000764	IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
CCI-000765	IA-2(1)	The information system implements multifactor authentication for network access to privileged accounts.
CCI-001953	IA-2(12)	The information system accepts Personal Identity Verification (PIV) credentials.
CCI-001954	IA-2(12)	The information system electronically verifies Personal Identity Verification (PIV) credentials.
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.
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.
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.
CCI-001970	IA-4(a)	The organization defines the personnel or roles that authorize the assignment of individual, group, role, and device identifiers.
CCI-001971	IA-4(a)	The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role or device identifier.
CCI-001972	IA-4(b)	The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device.
CCI-001973	IA-4(c)	The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device.
CCI-001974	IA-4(d)	The organization defines the time period for which the reuse of identifiers is prohibited.
CCI-001975	IA-4(d)	The organization manages information system identifiers by preventing reuse of identifiers for an organization-defined time period.
CCI-000794	IA-4(e)	The organization defines a time period of inactivity after which the identifier is disabled.
CCI-000795	IA-4(e)	The organization manages information system identifiers by disabling the identifier after an organization defined time period of inactivity.
CCI-001990	IA-5(j)	The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.
CCI-000192	IA-5(1)(a)	The information system enforces password complexity by the minimum number of upper case characters used.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000193	IA-5(1)(a)	The information system enforces password complexity by the minimum number of lower case characters used.
CCI-000194	IA-5(1)(a)	The information system enforces password complexity by the minimum number of numeric characters used.
CCI-000205	IA-5(1)(a)	The information system enforces minimum password length.
CCI-001619	IA-5(1)(a)	The information system enforces password complexity by the minimum number of special characters used.
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.
CCI-000196	IA-5(1)(c)	The information system, for password-based authentication, stores only cryptographically-protected passwords.
CCI-000197	IA-5(1)(c)	The information system, for password-based authentication, transmits only cryptographically-protected passwords.
CCI-000199	IA-5(1)(d)	The information system enforces maximum password lifetime restrictions.
CCI-000200	IA-5(1)(e)	The information system prohibits password reuse for the organization defined number of generations.
CCI-001618	IA-5(1)(e)	The organization defines the number of 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.
CCI-002002	IA-5(11)	The organization defines the token quality requirements to be employed by the information system mechanisms for token-based authentication.
CCI-002003	IA-5(11)	The information system, for token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.
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.
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.
CCI-000804	IA-8	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
CCI-002009	IA-8(1)	The information system accepts Personal Identity Verification (PIV) credentials from other federal agencies.
CCI-002010	IA-8(1)	The information system electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.
CCI-002011	IA-8(2)	The information system accepts FICAM-approved third-party credentials.
CCI-002013	IA-8(3)	The organization employs only FICAM-approved information system components in organization-defined information systems to accept third-party credentials.
CCI-002014	IA-8(4)	The information system conforms to FICAM-issued profiles.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000995	MP-1(a)(1)	The organization develops and documents a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
CCI-000996	MP-1(a)(1)	The organization disseminates to organization-defined personnel or roles a media protection policy.
CCI-002566	MP-1(a)(1)	The organization defines personnel or roles to whom a documented media protection policy and procedures will be disseminated.
CCI-000999	MP-1(a)(2)	The organization develops and documents procedures to facilitate the implementation of the media protection policy and associated media protection controls.
CCI-001000	MP-1(a)(2)	The organization disseminates to organization-defined personnel or roles procedures to facilitate the implementation of the media protection policy and associated media protection controls.
CCI-000997	MP-1(b)(1)	The organization reviews and updates the current media protection policy in accordance with organization-defined frequency.
CCI-000998	MP-1(b)(1)	The organization defines a frequency for reviewing and updating the current media protection policy.
CCI-001001	MP-1(b)(2)	The organization reviews and updates the current media protection procedures in accordance with organization-defined frequency.
CCI-001002	MP-1(b)(2)	The organization defines a frequency for reviewing and updating the current media protection procedures.
CCI-001003	MP-2	The organization restricts access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.
CCI-001004	MP-2	The organization defines types of digital and/or non-digital media for which the organization restricts access.
CCI-001005	MP-2	The organization defines personnel or roles to restrict access to organization-defined types of digital and/or non-digital media.
CCI-001028	MP-6(a)	The organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.
CCI-002578	MP-6(a)	The organization defines information system media to sanitize prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies.
CCI-002579	MP-6(a)	The organization defines the sanitization techniques and procedures in accordance with applicable federal and organization standards and policies to be used to sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse.
CCI-002580	MP-6(b)	The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-002581	MP-7	The organization defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards.
CCI-002582	MP-7	The organization defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards.
CCI-002583	MP-7	The organization defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components.
CCI-002584	MP-7	The organization restricts or prohibits the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards.
CCI-000965	PE-13	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
CCI-000971	PE-14(a)	The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels.
CCI-000972	PE-14(a)	The organization defines acceptable temperature and humidity levels to be maintained within the facility where the information system resides.
CCI-000973	PE-14(b)	The organization monitors temperature and humidity levels in accordance with organization-defined frequency.
CCI-000974	PE-14(b)	The organization defines a frequency for monitoring temperature and humidity levels.
CCI-000977	PE-15	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible.
CCI-000978	PE-15	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are working properly.
CCI-000979	PE-15	Key personnel have knowledge of the master water shutoff or isolation valves.
CCI-000981	PE-16	The organization authorizes organization-defined types of information system components entering and exiting the facility.
CCI-000982	PE-16	The organization monitors organization-defined types of information system components entering and exiting the facility.
CCI-000983	PE-16	The organization controls organization-defined types of information system components entering and exiting the facility.
CCI-000984	PE-16	The organization maintains records of information system components entering and exiting the facility.
CCI-002974	PE-16	The organization defines types of information system components to authorize, monitor, and control entering and exiting the facility and to maintain records.
CCI-003051	PL-2(a)(2)	The organization's security plan for the information system explicitly defines the authorization boundary for the system.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000080	PM-3(a)	The organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.
CCI-000081	PM-3(b)	The organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required.
CCI-000141	PM-3(c)	The organization ensures that information security resources are available for expenditure as planned.
CCI-000142	PM-4(a)(1)	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained.
CCI-002991	PM-4(a)(1)	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed.
CCI-000170	PM-4(a)(2)	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation.
CCI-002992	PM-4(a)(3)	The organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are reported in accordance with OMB FISMA reporting requirements.
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.
CCI-001054	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications on an organization-defined frequency.
CCI-001055	RA-5(a)	The organization defines a frequency for scanning for vulnerabilities in the information system and hosted applications.
CCI-001056	RA-5(a)	The organization scans for vulnerabilities in the information system and hosted applications when new 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.
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.
CCI-001057	RA-5(b)	The organization employs vulnerability scanning tools and techniques that facilitate interoperability 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.
CCI-001059	RA-5(d)	The organization remediates legitimate vulnerabilities in organization-defined response times in accordance with an organizational assessment risk.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
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.
CCI-000669	SA-9(a)	The organization requires that providers of external information system services comply with organizational information security requirements.
CCI-000670	SA-9(a)	The organization requires that providers of external information system services employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
CCI-003137	SA-9(a)	The organization defines security controls that providers of external information system services employ in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
CCI-000671	SA-9(b)	The organization defines government oversight with regard to external information system services.
CCI-000672	SA-9(b)	The organization documents government oversight with regard to external information system services.
CCI-000673	SA-9(b)	The organization defines user roles and responsibilities with regard to external information system services.
CCI-000674	SA-9(b)	The organization documents user roles and responsibilities with regard to external information system services.
CCI-003138	SA-9(c)	The organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.
CCI-003139	SA-9(c)	The organization defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis.
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.
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.
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.
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.
CCI-001098	SC-7(c)	The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
CCI-002428	SC-12	The organization defines the requirements for cryptographic key generation to be employed within the information system.
CCI-002429	SC-12	The organization defines the requirements for cryptographic key distribution to be employed within the information system.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-002430	SC-12	The organization defines the requirements for cryptographic key storage to be employed within the information system.
CCI-002431	SC-12	The organization defines the requirements for cryptographic key access to be employed within the information system.
CCI-002432	SC-12	The organization defines the requirements for cryptographic key destruction to be employed within the information system.
CCI-001150	SC-15(a)	The information system prohibits remote activation of collaborative computing devices excluding the organization-defined exceptions where remote activation is to be allowed.
CCI-001151	SC-15(a)	The organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed.
CCI-001152	SC-15(b)	The information system provides an explicit indication of use to users physically present at collaborative computing devices.
CCI-002465	SC-21	The information system requests data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.
CCI-002466	SC-21	The information system requests data integrity verification on the name/address resolution responses the system receives from authoritative sources.
CCI-002467	SC-21	The information system performs data integrity verification on the name/address resolution responses the system receives from authoritative sources.
CCI-002468	SC-21	The information system performs data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.
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.
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.
CCI-001227	SI-2(a)	The organization corrects information system flaws.
CCI-001228	SI-2(b)	The organization tests software updates related to flaw remediation for effectiveness before installation.
CCI-001229	SI-2(b)	The organization tests software updates related to flaw remediation for potential side effects before installation.
CCI-002602	SI-2(b)	The organization tests firmware updates related to flaw remediation for effectiveness before installation.
CCI-002603	SI-2(b)	The organization tests firmware updates related to flaw remediation for potential side effects before installation.
CCI-002619	SI-3(a)	The organization employs malicious code protection mechanisms at information system entry points to detect malicious code.
CCI-002620	SI-3(a)	The organization employs malicious code protection mechanisms at information system exit points to detect malicious code.
CCI-002621	SI-3(a)	The organization employs malicious code protection mechanisms at information system entry points to eradicate malicious code.
CCI-002622	SI-3(a)	The organization employs malicious code protection mechanisms at information system exit points to eradicate malicious code.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
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.
CCI-001242	SI-3(c)(1)	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy.
CCI-002624	SI-3(c)(1)	The organization configures malicious code protection mechanisms to perform real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.
CCI-001243	SI-3(c)(2)	The organization configures malicious code protection mechanisms to perform organization-defined action(s) in response to malicious code detection.
CCI-001244	SI-3(c)(2)	The organization defines one or more actions to perform in response to malicious code detection, such as blocking malicious code, quarantining malicious code, or sending alert to administrator.
CCI-001253	SI-4(a)(1)	The organization defines the objectives of monitoring for attacks and indicators of potential attacks on the information system.
CCI-002641	SI-4(a)(1)	The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives.
CCI-002644	SI-4(a)(2)	The organization monitors the information system to detect unauthorized remote connections.
CCI-002642	SI-4(a)(2)	The organization monitors the information system to detect unauthorized local connections.
CCI-002643	SI-4(a)(2)	The organization monitors the information system to detect unauthorized network connections.
CCI-002645	SI-4(b)	The organization defines the techniques and methods to be used to identify unauthorized use of the information system.
CCI-002646	SI-4(b)	The organization identifies unauthorized use of the information system through organization-defined techniques and methods.
CCI-001256	SI-4(c)	The organization deploys monitoring devices at ad hoc locations within the system to track specific types of transactions of interest to the organization.
CCI-002647	SI-4(d)	The organization protects information obtained from intrusion-monitoring tools from unauthorized access.
CCI-002648	SI-4(d)	The organization protects information obtained from intrusion-monitoring tools from unauthorized modification.
CCI-002649	SI-4(d)	The organization protects information obtained from intrusion-monitoring tools from unauthorized deletion.
CCI-001257	SI-4(e)	The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Table H-6 Platform Enclave CCIs for LOW and MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001258	SI-4(f)	The organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
CCI-002650	SI-4(g)	The organization defines the information system monitoring information that is to be provided the organization-defined personnel or roles.
CCI-002651	SI-4(g)	The organization defines the personnel or roles that are to be provided organization-defined information system monitoring information.
CCI-002652	SI-4(g)	The organization defines the frequency at which the organization will provide the organization-defined information system monitoring information to organization-defined personnel or roles
CCI-002654	SI-4(g)	The organization provides organization-defined information system monitoring information to organization-defined personnel or roles as needed or per organization-defined frequency.
CCI-001285	SI-5(a)	The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis.
CCI-002692	SI-5(a)	The organization defines the external organizations from which it receives information system security alerts, advisories and directives.
CCI-001286	SI-5(b)	The organization generates internal security alerts, advisories, and directives as deemed necessary.
CCI-001287	SI-5(c)	The organization disseminates security alerts, advisories, and directives to organization-defined personnel or roles, organization-defined elements within the organization, and/or organization-defined external organizations.
CCI-001288	SI-5(c)	The organization defines the personnel or roles to whom the organization will disseminate security alerts, advisories and directives.
CCI-002693	SI-5(c)	The organization defines the elements within the organization to whom the organization will disseminate security alerts, advisories and directives.
CCI-001289	SI-5(d)	The organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000015	AC-2(1)	The organization employs automated mechanisms to support the information system account management functions.
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.
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.
CCI-001361	AC-2(2)	The organization defines a time period after which temporary accounts are automatically terminated.
CCI-001365	AC-2(2)	The organization defines a time period after which emergency accounts are automatically terminated.
CCI-000017	AC-2(3)	The information system automatically disables inactive accounts after an organization-defined time period.
CCI-000018	AC-2(4)	The information system automatically audits account creation actions.
CCI-001403	AC-2(4)	The information system automatically audits account modification actions.
CCI-001404	AC-2(4)	The information system automatically audits account disabling actions.
CCI-001405	AC-2(4)	The information system automatically audits account removal actions.
CCI-002130	AC-2(4)	The information system automatically audits account enabling actions.
CCI-001683	AC-2(4)	The information system notifies organization-defined personnel or roles for account creation actions.
CCI-001684	AC-2(4)	The information system notifies organization-defined personnel or roles for account modification actions.
CCI-001685	AC-2(4)	The information system notifies organization-defined personnel or roles for account disabling actions.
CCI-001686	AC-2(4)	The information system notifies organization-defined personnel or roles for account removal actions.
CCI-002132	AC-2(4)	The information system notifies organization-defined personnel or roles for account enabling actions.
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.
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.
CCI-001548	AC-4	The organization defines the information flow control policies for controlling the flow of information within the system.
CCI-001549	AC-4	The organization defines the information flow control policies for controlling the flow of information between interconnected systems.
CCI-001550	AC-4	The organization defines approved authorizations for controlling the flow of information within the system.
CCI-001551	AC-4	The organization defines approved authorizations for controlling the flow of information between interconnected systems.
CCI-002220	AC-5(c)	The organization defines information system access authorizations to support separation of duties.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
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.
CCI-000058	AC-11(a)	The information system provides the capability for users to directly initiate session lock mechanisms.
CCI-000059	AC-11(a)	The organization defines the time period of inactivity after which the information system initiates a session lock.
CCI-000056	AC-11(b)	The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.
CCI-000060	AC-11(1)	The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.
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.
CCI-002361	AC-12	The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.
CCI-000067	AC-17(1)	The information system monitors remote access methods.
CCI-002314	AC-17(1)	The information system controls remote access methods.
CCI-000068	AC-17(2)	The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.
CCI-001453	AC-17(2)	The information system implements cryptographic mechanisms to protect the integrity of remote access sessions.
CCI-000069	AC-17(3)	The information system routes all remote accesses through organization-defined number managed network access control points.
CCI-001561	AC-17(3)	The organization defines managed access control points for remote access to the information system.
CCI-002315	AC-17(3)	The organization defines the number of managed network access control points through which the information system routes all remote access.
CCI-000070	AC-17(4)(a)	The organization authorizes the execution of privileged commands via remote access only for organization-defined needs.
CCI-002316	AC-17(4)(a)	The organization authorizes the access to security-relevant information via remote access only for organization-defined needs.
CCI-002317	AC-17(4)(a)	The organization defines the operational needs when the execution of privileged commands via remote access is to be authorized.
CCI-002318	AC-17(4)(a)	The organization defines the operational needs when access to security-relevant information via remote access is to be authorized.
CCI-002319	AC-17(4)(b)	The organization documents in the security plan for the information system the rationale for authorization of the execution of privilege commands via remote access.
CCI-002320	AC-17(4)(b)	The organization documents in the security plan for the information system the rationale for authorization of access to security-relevant information via remote access.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-002231	AC-19(5)	The organization employs full-device encryption or container encryption to protect the integrity of information on organization-defined mobile devices.
CCI-002329	AC-19(5)	The organization defines the mobile devices that are to employ full-device or container encryption to protect the confidentiality and integrity of the information on device.
CCI-002330	AC-19(5)	The organization employs full-device encryption or container encryption to protect the confidentiality of information on organization-defined mobile devices.
CCI-002333	AC-20(1)(a)	The organization permits authorized individuals to use an external information system to access the information system only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
CCI-002334	AC-20(1)(a)	The organization permits authorized individuals to use an external information system to process organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
CCI-002335	AC-20(1)(a)	The organization permits authorized individuals to use an external information system to store organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
CCI-002336	AC-20(1)(a)	The organization permits authorized individuals to use an external information system to transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
CCI-002337	AC-20(1)(b)	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
CCI-000097	AC-20(2)	The organization restricts or prohibits the use of organization-controlled portable storage devices by authorized individuals on external information systems.
CCI-001875	AU-7(a)	The information system provides an audit reduction capability that supports on-demand audit review and analysis.
CCI-001876	AU-7(a)	The information system provides an audit reduction capability that supports on-demand reporting requirements.
CCI-001877	AU-7(a)	The information system provides an audit reduction capability that supports after-the-fact investigations of security incidents.
CCI-001878	AU-7(a)	The information system provides a report generation capability that supports on-demand audit review and analysis.
CCI-001879	AU-7(a)	The information system provides a report generation capability that supports on-demand reporting requirements.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001880	AU-7(a)	The information system provides a report generation capability that supports after-the-fact investigations of security incidents.
CCI-001881	AU-7(b)	The information system provides an audit reduction capability that does not alter original content or time ordering of audit records.
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.
CCI-000158	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.
CCI-002080	CA-3(5)	The organization employs either an allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.
CCI-002081	CA-3(5)	The organization defines the information systems that employ either allow-all, deny-by-exception or deny-all, permit by exception policy for allowing connection to external information systems.
CCI-002082	CA-3(5)	The organization selects either allow-all, deny-by exception or deny-all, permit by exception policy for allowing organization-defined information systems to connect to external information systems.
CCI-000338	CM-5	The organization defines physical access restrictions associated with changes to the information system.
CCI-000339	CM-5	The organization documents physical access restrictions associated with changes to the information system.
CCI-000340	CM-5	The organization approves physical access restrictions associated with changes to the information system.
CCI-000341	CM-5	The organization enforces physical access restrictions associated with changes to the information system.
CCI-000342	CM-5	The organization defines logical access restrictions associated with changes to the information system.
CCI-000343	CM-5	The organization documents logical access restrictions associated with changes to the information system.
CCI-000344	CM-5	The organization approves logical access restrictions associated with changes to the information system.
CCI-000345	CM-5	The organization enforces logical access restrictions associated with changes to the information system.
CCI-000419	CM-8(5)	The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.
CCI-000505	CP-6(a)	The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.
CCI-002836	CP-6(b)	The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.
CCI-000507	CP-6(1)	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.
CCI-000509	CP-6(3)	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001604	CP-6(3)	The organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.
CCI-000510	CP-7(a)	The organization defines the time period consistent with recovery time and recovery point objectives for essential missions/business functions to permit the transfer and resumption of organization-defined information system operations at an alternate processing site when the primary processing capabilities are unavailable.
CCI-000513	CP-7(a)	The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.
CCI-002839	CP-7(a)	The organization defines information system operations that are permitted to transfer and resume at an alternate processing sites for essential missions/business functions when the primary processing capabilities are unavailable.
CCI-000515	CP-7(b)	The organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.
CCI-000521	CP-7(c)	The organization ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
CCI-000516	CP-7(1)	The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
CCI-000517	CP-7(2)	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.
CCI-001606	CP-7(2)	The organization outlines explicit mitigation actions for organization identified potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.
CCI-000518	CP-7(3)	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).
CCI-000522	CP-8	The organization defines the time period to permit the resumption of organization-defined information system operations for essential missions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
CCI-000524	CP-8	The organization establishes alternate telecommunication services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-002840	CP-8	The organization defines the information system operations to be resumed for essential missions within the organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
CCI-000526	CP-8(1)(a)	The organization develops primary telecommunications service agreements that contain priority-of-service provisions in accordance with the organizations availability requirements (including recovery time objectives).
CCI-000527	CP-8(1)(a)	The organization develops alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organizations availability requirements (including recovery time objectives).
CCI-000528	CP-8(1)(b)	The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary telecommunications services are provided by a common carrier.
CCI-000529	CP-8(1)(b)	The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the alternate telecommunications services are provided by a common carrier.
CCI-000530	CP-8(2)	The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
CCI-000541	CP-9(1)	The organization defines the frequency to test backup information to verify media reliability and information integrity.
CCI-000542	CP-9(1)	The organization tests backup information per organization-defined frequency to verify media reliability and information integrity.
CCI-000766	IA-2(2)	The information system implements multifactor authentication for network access to non-privileged accounts.
CCI-000767	IA-2(3)	The information system implements multifactor authentication for local access to privileged accounts.
CCI-001949	IA-2(11)	The device used in the information system implementation of multifactor authentication for remote access to privileged accounts meets organization-defined strength of mechanism requirements.
CCI-001951	IA-2(11)	The information system implements multifactor authentication for remote access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
CCI-001952	IA-2(11)	The device used in the information system implementation of multifactor authentication for remote access to non-privileged accounts meets organization-defined strength of mechanism requirements.
CCI-001948	IA-2(11)	The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
CCI-001950	IA-2(11)	The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to non-privileged accounts.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001947	IA-2(11)	The organization defines the strength of mechanism requirements for the device that is separate from the system gaining access and is to provide one factor of a multifactor authentication for remote access to privileged accounts.
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.
CCI-000186	IA-5(2)(b)	The information system, for PKI-based authentication enforces authorized access to the corresponding 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.
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.
CCI-001992	IA-5(3)	The organization defines the personnel or roles responsible for authorizing the organization's registration authority accountable for the authenticator registration process.
CCI-001993	IA-5(3)	The organization defines the registration authority accountable for the authenticator registration process.
CCI-001994	IA-5(3)	The organization defines the types of and/or specific authenticators that are subject to the authenticator registration process.
CCI-001995	IA-5(3)	The organization requires that the registration process, to receive organization-defined types of and/or specific authenticators, be conducted in person, or by a trusted third-party, before organization-defined registration authority with authorization by organization-defined personnel or roles.
CCI-001010	MP-3(a)	The organization marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
CCI-001011	MP-3(b)	The organization exempts organization-defined types of information system media from marking as long as the media remain within organization-defined controlled areas.
CCI-001012	MP-3(b)	The organization defines types of information system media to exempt from marking as long as the media remain within organization-defined controlled areas.
CCI-001013	MP-3(b)	The organization defines controlled areas where organization-defined types of information system media are exempt from being marked.
CCI-001014	MP-4(a)	The organization physically controls and securely stores organization-defined types of digital and/or non-digital media within organization-defined controlled areas.
CCI-001015	MP-4(a)	The organization defines types of digital and/or non-digital media to physically control and securely store within organization-defined controlled areas.
CCI-001016	MP-4(a)	The organization defines controlled areas where organization-defined types of digital and/or non-digital media are physically controlled and securely stored.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001018	MP-4(b)	The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
CCI-001020	MP-5(a)	The organization protects and controls organization-defined types of information system media during transport outside of controlled areas using organization-defined security safeguards.
CCI-001021	MP-5(a)	The organization defines types of information system media protected and controlled during transport outside of controlled areas.
CCI-001022	MP-5(a)	The organization defines security safeguards to be used to protect and control organization-defined types of information system media during transport outside of controlled areas.
CCI-001023	MP-5(b)	The organization maintains accountability for information system media during transport outside of controlled areas.
CCI-001025	MP-5(c)	The organization documents activities associated with the transport of information system media.
CCI-001024	MP-5(d)	The organization restricts the activities associated with the transport of information system media to authorized personnel.
CCI-001027	MP-5(4)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
CCI-002585	MP-7(1)	The organization prohibits the use of portable storage devices in organization information systems when such devices have no identifiable owner.
CCI-000956	PE-10(a)	The organization provides the capability of shutting off power to the information system or individual system components in emergency situations.
CCI-000957	PE-10(b)	The organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel.
CCI-000958	PE-10(b)	The organization defines a location for emergency shutoff switches or devices by information system or system component.
CCI-000959	PE-10(c)	The organization protects emergency power shutoff capability from unauthorized activation.
CCI-002955	PE-11	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.
CCI-000961	PE-11(1)	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
CCI-000968	PE-13(3)	The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.
CCI-000985	PE-17(a)	The organization employs organization-defined security controls at alternate work sites.
CCI-002975	PE-17(a)	The organization defines security controls to employ at alternate work sites.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-000987	PE-17(b)	The organization assesses as feasible, the effectiveness of security controls at alternate work sites.
CCI-000988	PE-17(c)	The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.
CCI-000594	PL-4(1)	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites.
CCI-000595	PL-4(1)	The organization includes in the rules of behavior, explicit restrictions on posting organizational information on public websites.
CCI-001062	RA-5(1)	The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.
CCI-001063	RA-5(2)	The organization updates the information system vulnerabilities scanned on an organization-defined frequency, prior to a new scan and/or when new vulnerabilities are identified and reported.
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.
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.
CCI-002906	RA-5(5)	The organization defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components.
CCI-003143	SA-9(2)	The organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services.
CCI-003144	SA-9(2)	The organization defines the external information system services for which the providers are required to identify the functions, ports, protocols, and other services required for the use of such services.
CCI-001082	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.
CCI-001090	SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.
CCI-001101	SC-7(3)	The organization limits the number of external network connections to the information system.
CCI-001102	SC-7(4)(a)	The organization implements a managed interface for each external telecommunication service.
CCI-001103	SC-7(4)(b)	The organization establishes a traffic flow policy for each managed interface for each external telecommunication service.
CCI-002396	SC-7(4)(c)	The organization protects the confidentiality and integrity of the information being transmitted across each interface for each external telecommunication service.
CCI-001105	SC-7(4)(d)	The organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need for each external telecommunication service.
CCI-001106	SC-7(4)(e)	The organization reviews exceptions to the traffic flow policy on an organization-defined frequency for each external telecommunication service.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001108	SC-7(4)(e)	The organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need for each external telecommunication service.
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).
CCI-002397	SC-7(7)	The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
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.
CCI-002449	SC-13	The organization defines the cryptographic uses, and type of cryptography required for each use, to be implemented by the information system.
CCI-002450	SC-13	The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
CCI-001159	SC-17	The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider.
CCI-002456	SC-17	The organization defines the certificate policy employed to issue public key certificates.
CCI-001160	SC-18(a)	The organization defines acceptable and unacceptable mobile code and mobile code technologies.
CCI-001161	SC-18(b)	The organization establishes usage restrictions for acceptable mobile code and mobile code technologies.
CCI-001162	SC-18(b)	The organization establishes implementation guidance for acceptable mobile code and mobile code technologies.
CCI-001163	SC-18(c)	The organization authorizes the use of mobile code within the information system.
CCI-001164	SC-18(c)	The organization monitors the use of mobile code within the information system.
CCI-001165	SC-18(c)	The organization controls the use of mobile code within the information system.
CCI-001184	SC-23	The information system protects the authenticity of communications sessions.
CCI-001199	SC-28	The information system protects the confidentiality and/or integrity of organization-defined information at rest.
CCI-001233	SI-2(2)	The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.
CCI-001234	SI-2(2)	The organization defines a frequency for employing automated mechanisms to determine the state of information system components with regard to flaw remediation.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-001246	SI-3(1)	The organization centrally manages malicious code protection mechanisms.
CCI-001247	SI-3(2)	The information system automatically updates malicious code protection mechanisms.
CCI-001260	SI-4(2)	The organization employs automated tools to support near real-time analysis of events.
CCI-002659	SI-4(4)	The organization defines the frequency on which it will monitor inbound communications for unusual or unauthorized activities or conditions.
CCI-002660	SI-4(4)	The organization defines the frequency on which it will monitor outbound communications for unusual or unauthorized activities or conditions.
CCI-002661	SI-4(4)	The information system monitors inbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.
CCI-002662	SI-4(4)	The information system monitors outbound communications traffic per organization-defined frequency for unusual or unauthorized activities or conditions.
CCI-001264	SI-4(5)	The organization defines indicators of compromise or potential compromise to the security of the information system which will result in information system alerts being provided to organization-defined personnel or roles.
CCI-002663	SI-4(5)	The organization defines the personnel or roles to receive information system alerts when organization-defined indicators of compromise or potential compromise occur.
CCI-002664	SI-4(5)	The information system alerts organization-defined personnel or roles when organization-defined compromise indicators reflect the occurrence of a compromise or a potential compromise.
CCI-002703	SI-7	The organization defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes.
CCI-002704	SI-7	The organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information.
CCI-002705	SI-7(1)	The organization defines the software on which integrity checks will be performed.
CCI-002706	SI-7(1)	The organization defines the firmware on which integrity checks will be performed.
CCI-002707	SI-7(1)	The organization defines the information on which integrity checks will be performed.
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.
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.
CCI-002712	SI-7(1)	The information system performs an integrity check of organization-defined information at startup, at organization-defined transitional states or security-relevant events, or on organization-defined frequency.

Table H-7 Additional Platform Enclave CCIs for MODERATE Impact Control Systems		
CCI #	**800-53 Control Text Indicator**	**CCI Definition**
CCI-002708	SI-7(1)	The organization defines the transitional state or security-relevant events when the information system will perform integrity checks on software, firmware and information.
CCI-002719	SI-7(7)	The organization defines the unauthorized security-relevant changes to the information system that are to be incorporated into the organizational incident response capability.
CCI-002720	SI-7(7)	The organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.
CCI-002823	SI-16	The organization defines the security safeguards to be implemented to protect the information system's memory from unauthorized code execution.
CCI-002824	SI-16	The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution.