ERDC/CERL SR-19-5

US Army Corps of Engineers®
Engineer Research and Development Center

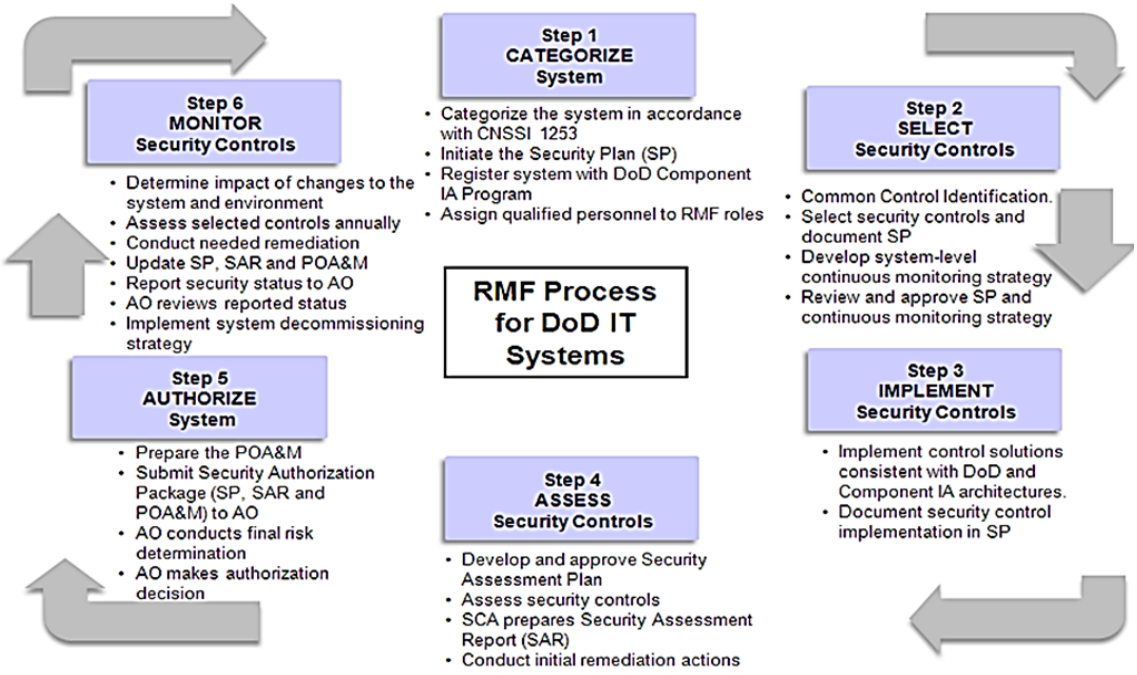
ERDC
ENGINEER RESEARCH & DEVELOPMENT CENTER

An Army Guide to Navigating the Cyber Security Process for Facility Related Control Systems

Cybersecurity and Risk Management Framework explanations for the Real World

Michael Cary Long, Joseph Bush, Stephen Briggs, Tapan Patel,
Eileen Westervelt, Daniel Shepard, Eric Lynch, and David Schwenk

October 2019



Construction Engineering Research Laboratory

The U.S. Army Engineer Research and Development Center (ERDC) solves the nation's toughest engineering and environmental challenges. ERDC develops innovative solutions in civil and military engineering, geospatial sciences, water resources, and environmental sciences for the Army, the Department of Defense, civilian agencies, and our nation's public good. Find out more at www.erdc.usace.army.mil.

To search for other technical reports published by ERDC, visit the ERDC online library at http://acwc.sdp.sirsi.net/client/default.

ERDC/CERL SR-19-5
October 2019

An Army Guide to Navigating the Cyber Security Process for Facility Related Control Systems

Cybersecurity and Risk Management Framework explanations for the Real World

Joseph Bush, Tapan Patel and Eileen T. Westervelt

U.S. Army Engineer Research and Development Center (ERDC)
Construction Engineering Research Laboratory (CERL)
2902 Newmark Dr.
Champaign, IL 61824

Michael Cary Long and Daniel Shepard

U.S. Army Corps of Engineers
Cybersecurity Technical Center of Expertise
Huntsville, Alabama 35816

Eric Lynch

U.S. Army Corps of Engineers
UMCS Mandatory Center of Expertise
Huntsville, Alabama 35816

Stephen J. Briggs

Facilities Dynamics Engineering
Champaign, IL
Columbia, MD 21046

David M. Schwenk

Private Consultant
Urbana, IL 61801

Final Technical Report (TR)

Prepared for Headquarters, U.S. Army Corps of Engineers
Washington, DC 20314-1000

Under Standards and Criteria Program via MIPR 11268080,
"A1040-FY19 TSG Oversight of ITTP."

Abstract

Personnel who maintain Facility Related Control Systems (FRCS) of any type are required to implement cybersecurity to attain and maintain an Authority to Operate (ATO) on their respective systems. This document is a guide for installation personnel owning and operating control systems to assist in addressing the cybersecurity process for FRCS in the Army through the Risk Management Framework (RMF) approach, which encompasses six steps. This manual walks the reader through the administrative aspects of each step.

Contents

Figures and Tables

Figures

Tables

Preface

This study was conducted for Headquarters, U.S. Army Corps of Engineers (HQUSACE) under the HQUSACE Standards and Criteria Program, via Military Interdepartmental Purchase Request (MIPR) 11268080, "A1040-FY19 TSG [Technology Standards Group] Oversight of ITTP." The project monitor was Timothy Gordon, CECW-EC.

The work was performed by the Energy Branch, of the Facilities Division, of the U.S. Army Engineer Research and Development Center, Construction Engineering Research Laboratory (ERDC-CERL). At the time of publication, Jed Alvey was Acting Chief of the Energy Branch, and Giselle Rodriguez was Acting Chief of the Facilities Division. The Deputy Director of ERDC-CERL was Dr. Kumar Topudurti and the Director was Dr. Lance D. Hansen.

COL Teresa A. Schlosser was Commander of ERDC, and Dr. David W. Pittman was the Director.

THIS PAGE INTENTIONALLY LEFT BLANK

1 Introduction

1.1 Background

Personnel who maintain Facility Related Control Systems (FRCSs) of any type are seldom cybersecurity experts. Yet now that many equipment control systems have adopted traditional Information Technology (IT) platforms as an integral part of their functional capabilities, they are required to implement cybersecurity on their respective systems. The U.S. Department of Defense (DoD) defines cybersecurity and the responsibilities and procedures involved in its implementation and maintenance in detail. For example, the Department of Defense Instruction (DoDI) 8500.01, "Cybersecurity" (DoD 2014) and the DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" (DoD 2017) are of key relevance to cybersecurity policy and the implementation of the RMF. Other key policies are noted in their respective sections below. However, it has often been observed that if the language of security is too difficult, the personnel who must implement and maintain security may misunderstand it, or bypass it entirely.

This document was written as a guide to supplements existing policy with applicable processes, written in plain English, for installation personnel who own and operate FRCSs. Specifically, this guide addresses the cybersecurity process for FRCSs in the Army by using the RMF approach to attain and maintain an Authority to Operate (ATO), which is required by DoDI 8510.01. This document defines technical area jargon, references and distills supporting process documents, provides many step-by-step procedures, makes recommendations for navigating the RMF guidance and tracking websites, and gives insights for applying current cybersecurity requirements. The RMF encompasses six steps. This manual walks the reader through the administrative aspects of each step in a logical fashion.

1.2 Key terminology

The terminology used in cybersecurity is extensive, nuanced in meaning, and often expressed in the form of acronyms. This report includes an Acronyms and Abbreviations list (p 100) that defines these terms and an Index (p 105) that the reader may use to locate the terms in context. Although many terms will be defined throughout the document, a few key terms are defined here to set the stage for the discussions that follow.

Cybersecurity

Cybersecurity is defined as

> prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (DoDI 8500.1).

Simply put, cybersecurity refers to securing computer assets against failure or attack. Note that cybersecurity goes beyond the traditional interpretation of "security" that protects assets from outside threats in that it also ensures that internal operations adequately support desired outcomes.

Risk Management and Risk Management Framework (RMF)

Risk Management is defined as

> The program and supporting processes to manage information security risk [i.e., vulnerabilities] to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time (DoDI 8510.01).

RMF is defined as "A structured approach used to oversee and manage risk for an enterprise" (DoDI 8510.01). It relies on developing a protocol of safeguards for information systems that represent a level of effort consistent with the potential impact of those safeguards being compromised. It also includes accountability of an Authorizing Official (AO), third party validation, and ongoing monitoring and improvement (also known as continuous monitoring).

In 2014, DoD adopted the RMF as the sanctioned method of addressing cybersecurity concerns in DoDI 8510.01; it replaces the previous Department of Defense Information Assurance Certification and Accreditation Program (DIACAP).

Control Systems

A control system is a "system of digital controllers, communication architecture, and user interfaces that monitor, or monitor and control, infrastructure and equipment" (NFEC 2017).

Facility Related Control System (FRCS)

An FRCS is "a control system that controls equipment and infrastructure that is part of a DoD building, structure, or linear structure" (NFEC 2017). (Note that "structure" typically refers to a vertical structure such as a bridge, and "linear structure" usually refers to electrical distribution lines.) Although the concepts and instructions in this document can be applied to any type of control system, this guide focuses on FRCSs. The 10 categories of FRCS include:

1. Airfield Systems
2. Building Control Systems
3. Dams, Locks & Levee Systems
4. Electronic Security Systems
5. Environmental Monitoring Systems
6. Fire & Life Safety Systems
7. Fueling Systems
8. Transportation Systems
9. Utility Control Systems
10. Utility Monitoring and Control Systems (which includes Building Control System [BCS] and UCS).

Figure 1 shows a Venn diagram of system naming conventions and their overlap with each other.

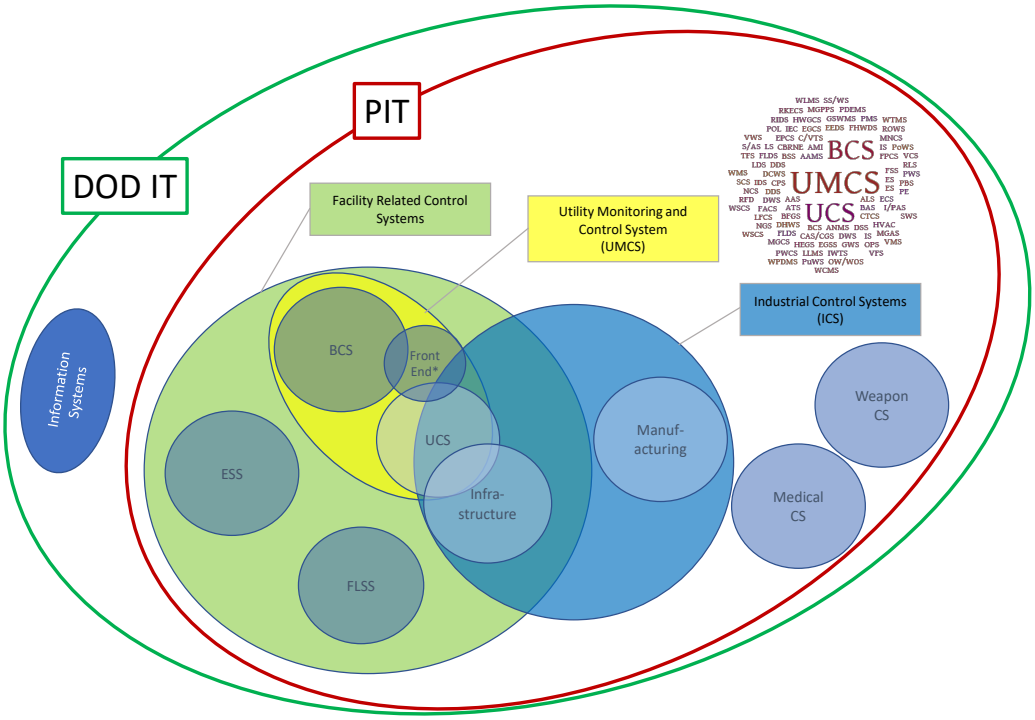
Industrial Control Systems (ICS)

ICSs are

> one type of control system, more specifically a control system that controls an industrial (manufacturing) process. Sometimes also used to refer to other types of control system, particularly utility control systems such as electrical, gas, or water distribution systems" (NFEC 2017).

As the preferred definition of ICS is the first (i.e., for an industrial process), ICS are not included in the list of FRCSs.

Figure 1. IT system naming conventions.

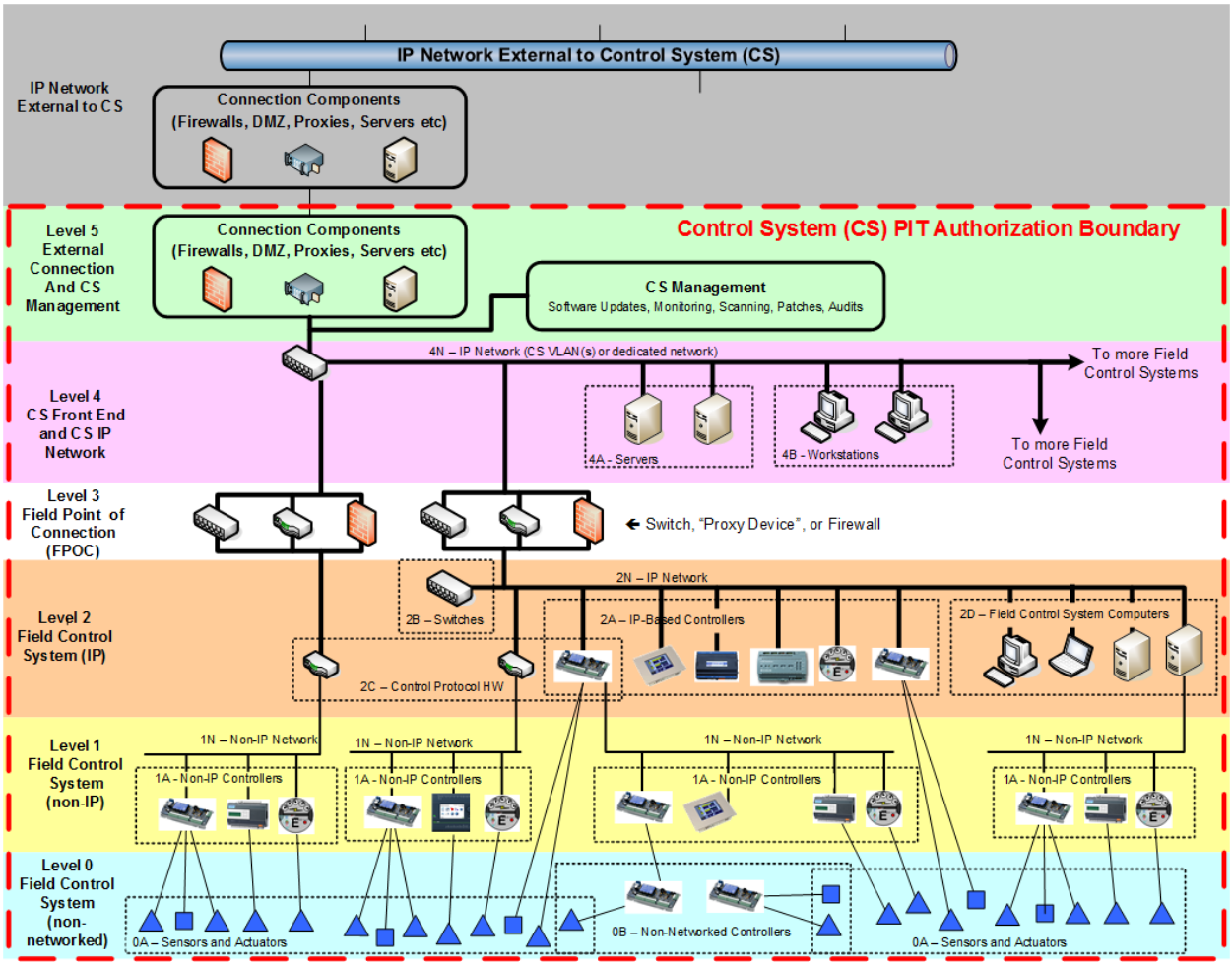


1.3 Control system architecture

The DoD has developed a “five-Level control system architecture” (Figure 2) as 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 B provides a more in-depth description of the five-Level control system architecture.

Figure 2. Five-level control system architecture.



1.4 Objectives of cybersecurity

Cybersecurity in the DoD is a method to establish protection of information with regards to confidentiality, integrity, and availability (CIA):

- *Confidentiality*. Ensuring that information is not disclosed to unauthorized individuals.
- *Integrity*. Ensuring that information or system components are not intentionally or unintentionally modified by unauthorized individuals, and that the information is accurate
- *Availability*. Ensuring that the system and its information is available whenever it is needed.

Note that for traditional IT systems confidentiality is the driving concern, while for FRCS availability and integrity are generally of greater importance. This distinction helps focus limited resources to activities that deliver desired outcomes.

1.5 Key resources

Although this guide mentions approaches for establishing secure systems through specific Security Controls, it does not provide the details of these methods. It is assumed that the reader will obtain help from appropriate experts for specification of security controls. Whether or not you desire to become a cybersecurity expert, it is important to know the resources that can help you understand the implementation of cybersecurity. Some key guidance websites, training opportunities, information sharing, and support assistance are listed below:

U.S. Army Corps of Engineers (USACE) Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX), 256-895-1153 (Program Manager), email: CSC-MCX@usace.army.mil, provides expert-level support to the USACE Military Programs Enterprise and external stakeholders on a cost-reimbursable basis. https://www.hnc.usace.army.mil/Portals/65/docs/PAO/Fact%20Sheets/2018%20Fact%20Sheets/Cybersecurity%20MCX%201809.pdf?ver=2018-09-17-155955-807

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (https://ics-cert.us-cert.gov/). Provides advisories, alerts and training related to many types of control systems (CS), although ICS-CERT currently focuses more on industrial and utility control system (systems using programmable logic controllers). Some of the training offered by ICS-CERT are:

Operational Security (OPSEC) for Control Systems (online)

Common ICS Components (online)

Cybersecurity Risk (online)

Introduction to Control Systems Cybersecurity (instructor led)

Intermediate Cybersecurity for Industrial Control Systems (instructor led)

ICS Cybersecurity (instructor led)

DoD Cyber Exchange (formerly known as Information Assurance Support Environment (IASE)) https://cyber.mil/

Provides guidance and links to a wide array of information about cybersecurity and the RMF process.

RMF Knowledge Service (https://rmfks.osd.mil/login.htm). The DoD's official site for RMF policy and implementation guidelines. A single authorized source for execution and implementation guidance, community forums, and the latest information and developments in the RMF.

Whole Building Design Guide (WBDG) (https://www.wbdg.org). Web-based portal providing government and industry practitioners up-to-date information on building-related guidance, criteria and technology from a 'whole buildings' perspective.

1.6 Online tracking systems

Registration in two online tracking systems is required as part of the RMF process.

Enterprise mission *Assurance Support Service (eMASS)* is the RMF process tracking system. Account registration: Each organization has a unique eMASS address. For the Army: https://army.emass.apps.mil/App/Home/Inbox

Army Portfolio Management System (APMS) tracks Army IT expenditures. https://cprobe.army.mil/enterprise-portal/web/apms.

1.7 Key personnel roles

Cybersecurity and RMF encompass several personnel roles with varying responsibilities. The following list is common for Army systems. Other components may differ slightly.

Information System Owner/System Owner (ISO/SO). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. An example would be an Energy Manager within a Directorate of Public Works (DPW) or the DPW Director. The SO is an appointed and required role for RMF. (Although the Energy Manager is often the effective system owner at many Army installations, this can be problematic since they may or may not have the authority necessary, e.g., fiscal, programmatic, etc., to direct or fulfil system owner duties.)

Information System Security Manager (ISSM). The ISSM is responsible for ensuring that cybersecurity is implemented and tracked in a system. The ISSM is an appointed and required role for RMF.

Organizational ISSM. System level.

Program ISSM. At the command level.

System Administrator (SA). The SA is responsible for ensuring that cybersecurity is implemented on the system using technical solutions (described later). The SA is an appointed and required role for RMF. This role can be filled locally to the *SO*'s organization or with an agreement through the local Network Enterprise Center (NEC), or service provider.

Security Control Assessor (SCA). The individual, group, or organization responsible for conducting a security control assessment. The Army identified an operational need to break the larger SCA role into four granular roles:

The *SCA-Validator (SCA-V)* has an appointed lead supported by a team that are officially designated to perform risk assessments on behalf of the SCA-Army (SCA-A). The risk assessment performed is a reimbursable expense that is to be paid by the SO's organization.

SCA-Representative (SCA-R) is a group of people known as functional leads (FL) who serve as a single point of contact for specified systems. The SCA-R works under the direct management of the SCA-A and provides the final risk assessment to the SCA-A.

The SCA-Army (SCA-A) makes the final recommendation (to authorize or not to authorize a system) to the Authorizing Official (AO).

The SCA-Organization (SCA-O) is an appointed position by the AO to act as the SCA-V, SCA-R, and SCA-A for systems that fall under the one of the alternate paths to addressing cybersecurity (Standalone Information System and Closed Restricted Network Assessment and Authorization; Operational Tactics, Techniques, and Procedures; and the RMF Assessment Only Operational Tactics, Techniques, and Procedures (TTPs) for the Army). The SCA-R at NETCOM will act in the auditor's role within the package approval chain (PAC) process in the Enterprise Mission Assurance Support Service (eMASS) when a SCA-O is appointed.

Authorizing Official (AO). A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. The AO is the person who grants the ATO for your system. For example, for IMCOM systems the Chief Information Officer (CIO)/G6 at HQ-IMCOM* is the AO.

1.8 Why RMF

RMF ensures that the risks associated with a system are properly understood and addressed before the system is *officially* allowed to operate. (In practice, since this is an unfunded mandate, it is presently an aspirational goal, and existing systems are not typically disabled pending authorization.)

RMF is required for any DoD system that processes, stores, transmits or receives DoD or component (e.g., Army, Navy, Air Force, etc.) information. Exactly what constitutes a "system" can be unclear. A basic rule of thumb is that, if you have a controller that is communicating on any kind of network (e.g., Ethernet, wireless, non-IP,† etc.), then the configuration is considered to be a system and RMF is required.

If you do not have a network (e.g., if the configuration uses only level 0 devices as defined in the five-level architecture, which do not use any form of digital protocol for communication), then RMF is not required.

* Headquarters, Installation Management Command (HQ-IMCOM)

† Internet Protocol (IP)

1.9 How does RMF apply to my system

If you are fielding a completely new system, you will need to go through the complete RMF process.

If you are expanding an existing system and not changing the impact rating of the system (not adding a critical component to a non-critical system), you likely do not need to do the whole RMF process. You may instead be able to add the components to the existing authorization using the Change Management Process (CMP) or using the Assess-Only process. Note there may be cases where the system will be considered to have changed sufficiently that a new authorization is required, but there is not guidance on this. Chapter 8 briefly describes the Assess-Only process.

If you are changing the impact rating of an existing system, you will likely need to do the whole RMF process (although you can leverage existing documentation for the requirements that are in common), or you may be able to obtain a separate authorization for the new components and then connect the two authorized systems with a connection agreement.

This guide focuses primarily on the implementation of a new system requiring an authorization and provides limited guidance on the expansion of an existing system. Many of the steps described here will apply to a more limited extent to the expansion of an existing system, so familiarity with the complete process will be helpful in expansions as well.

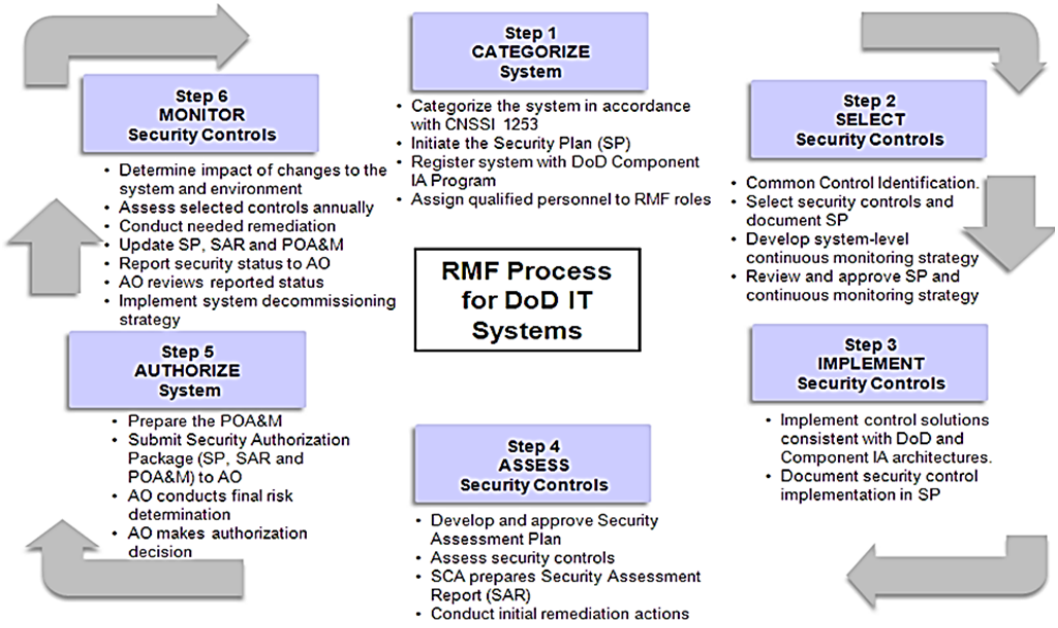
1.10 RMF process chart

Figure 3 graphically shows the six steps of the RMF process. The following chapters are organized to follow each step in the graphic. Note that these steps are described assuming a new authorization is required. They will not fully apply as described here when the Assess-Only process is allowed. Appendix A includes a checklist for tracking tasks to be completed through the RMF process.

1.11 Scope

Since cybersecurity methods evolve at a rapid rate, and website interfaces are continually updated, it is recognized that the presentation here represents only a snapshot in time. It is anticipated that as time passes this guide will need to become a living document with regular updates to adequately reflect current practice.

Figure 3. RMF process chart.



2 RMF Step 1: Categorize System

2.1 What is "categorization" and how do I know what my system is?

A system is categorized based on an evaluation of the *impact* associated with the loss of confidentiality (C), integrity (I), or availability (A) (generally written as CIA) on organizational operations, organizational assets, or individuals. The system impact is categorized as high, moderate. or low. This is sometimes referred to as the CIA level, CIA value, impact level, or security category.

Categorization will determine the appropriate security controls to be applied to your system. Step 1 of the RMF instructs us to categorize the system in accordance with Committee on National Security Systems Instruction (CNSSI) 1253. This instruction describes how CIA impact level is determined by the type of information on the system and mission criticality of the system. Rationales for system categorization will be required and may be supported by three approaches:

1. *Methodical System Review*. This is a "common sense" approach to determining impact ratings based on the mission and the relationship the control system has to the mission.
2. *IE&E Master List*. This list included "starting point" CIA impact ratings by control system type for three mission criticalities. The values here have generally (and for Utility Monitoring and Control System [UMCS], BCS, UCS more specifically) been determined through an application of the "common sense" methodical process defined here.
3. *NIST Guidance*. This is the "proper formal way" to determine impact ratings, but is not easily applicable to control systems. In practice, the approach used is to determine CIA using another approach first and then to confirm/document that impact rating determination using the NIST guidance.

2.1.1 System categorization definitions

Before defining the system categorization it is important to understand that is meant by loss of confidentiality (C), integrity (I), or availability (A), and what is meant by high, moderate and low impact.

The RMF considers three types of security breach:

1. *Loss of Confidentiality*. Information within the system is leaked to the outside.
2. *Loss of Integrity*. Information in the system is subject to unauthorized modification.
3. *Loss of Availability*. The system (or information in the system) is unavailable.

The RMF categorizes systems as LOW, MODERATE, or HIGH based on the potential impact of a security breach. The DoD definitions for LOW, MODERATE, and HIGH are given in FIPS-199* as modified in CNSSI 1253:†

> The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals [exceeding mission expectations.]
>
> The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries [exceeding mission expectations.]
>
> The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries [exceeding mission expectations.]

* Federal Information Processing Standards (FIPS)

† CNSSI amends the FIPS definitions to add the phrase "…exceeding mission expectations." to the end of the FIPS 199 definitions for each of LOW, MODERATE and HIGH.

One clarification is necessary to fully understand the above definitions, and that is: "When those definitions refer to 'the organization', which 'organization' are they talking about?" Loss of heating, ventilating, and air-conditioning (HVAC) at the Houston Marriott Hotel in August might be catastrophic to the local Marriott facility manager, but is hardly a significant blow to the United States, or even to the Marriott Corporation. RMF generally assumes that "Organization" refers to a high-level organization: A Major Army Command (MACOM), the Army, or all of DoD, not a local office.

2.1.2 System categorization based on methodical system review

2.1.2.1 Background

Ultimately, the goal of the cybersecurity "process" is to obtain the approval of the AO, who has the authority to grant an ATO. Because of the nature of the process, the AO has broad authority to approve any particular implementation of cybersecurity.

For an analogy of why this is, consider mechanical design of an HVAC system where systems are designed to specific criteria (design day environmental conditions). This criteria is a compromise between a system that is oversized for the need and a system that is sometimes under-sized. The criteria are well-established and nobody questions this tradeoff. Cybersecurity involves similar trade-offs, but (unlike mechanical design) the criteria is not well-established and the process allows the AO to determine the balance point between an over-secure* system and a system that still has some residual risk.

In almost all cases, loss of confidentiality of the information in the control system is of little or no consequence† and the impact of the control system is primarily due to loss of integrity or availability. Loss of integrity or availability relates to how these losses may impact the mission supported by the specific FRCS. Determination of impact for the control system is typically a two-step process:

> What is the impact of the mission? Will loss of the mission result in a LOW, MODERATE, or HIGH impact?
>
> How much will a loss of (integrity or availability of) HVAC controls impact the mission?

* Note: an overly secure system will likely most more and be harder to install, commission, and maintain.

† In the rare cases where it is of consequence, it is still generally much less important than integrity or availability.

This process will provide a rational ("common sense") starting point for determining criticality of an FRCS, but is not official policy. **Ultimately, system criticality is determined by Authorizing Official (in coordination with the system owner and based on input from the designer of the control system).**

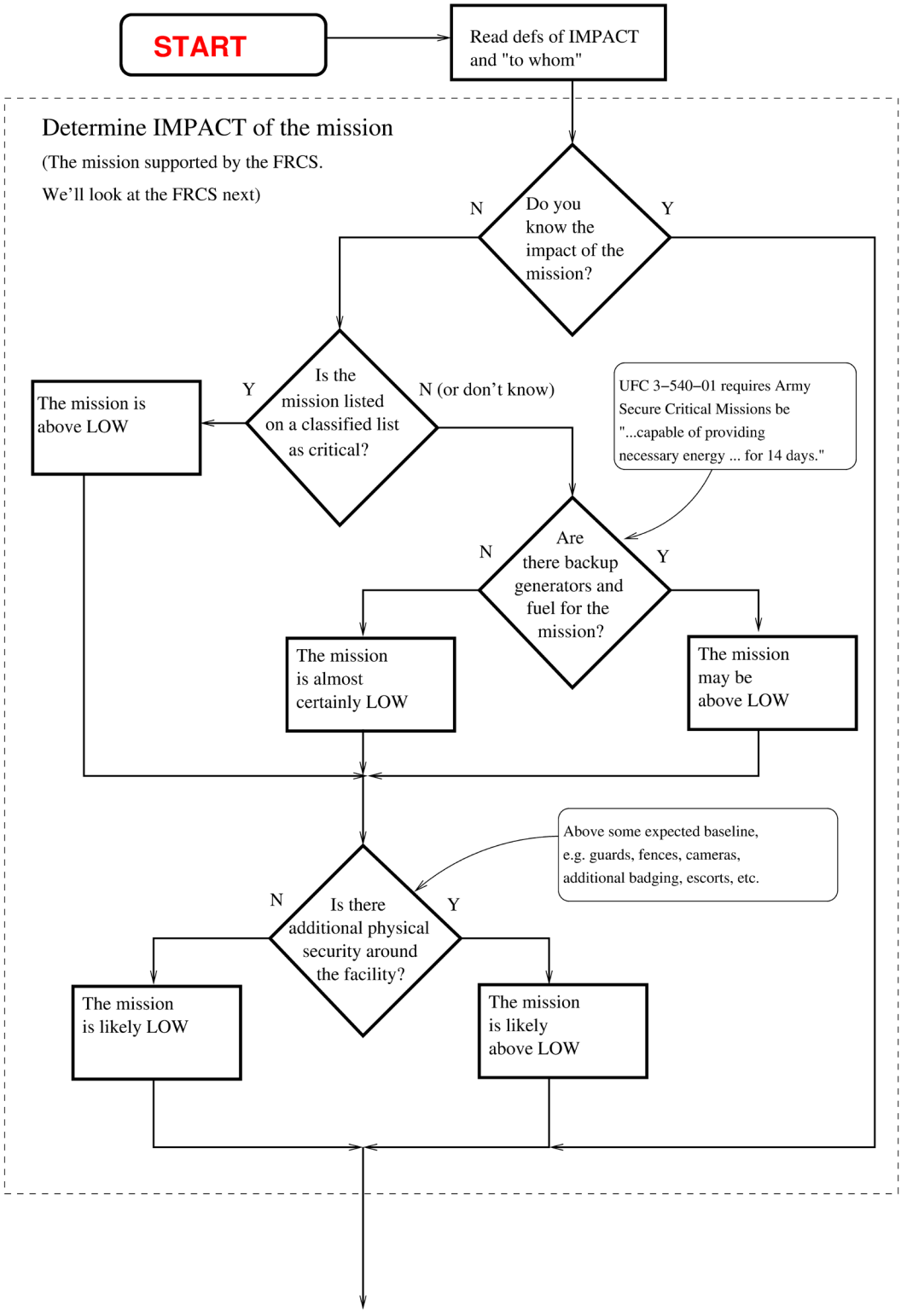
2.1.2.2 Impact of the HVAC control system

Ideally, the mission tenant will identify the mission impact, but this is often not feasible (mission tenants may not in fact know and frequently overstate their own importance). In cases where the mission impact is not known, or when the claimed mission impact seems exaggerated and confirmation is desired, the flow chart in Figure 4 may be helpful. The flowchart assumes that availability and integrity have the same impact rating, and disregards confidentiality. This chart relies on three observations:

> Critical mission facilities are often on a (classified) list of critical facilities.
>
> Critical mission facilities generally have a requirement for local backup generators. UFC 3-540-01, "Engine-Driven Generator Systems for Prime and Standby Power Applications" requires that "For Army Secure Critical Missions, the Army will reduce the risk by being capable of providing necessary energy and water for 14 days."
>
> Critical mission facilities generally have a requirement for physical security above and beyond what is typical on the installation.* This might include such things as additional fencing, cameras, security guards, additional badging, or requirements for escorts inside the facility. When electrical and mechanical infrastructure is outside the facility (e.g., a diesel generator outside the facility), there is typically a security fence surrounding the facility and the electrical / mechanical infrastructure.

* Note that while child development centers typically have additional security to protect the children from abduction, it seems unlikely that child development centers would be considered mission critical.

Figure 4. impact assessment flowchart.



Once the *impact of the mission* is known, the impact of the FRCS *on the mission* can be evaluated.

The first issue is whether the mission depends at all on the equipment controlled by the FRCS. A computer server room is clearly dependent on continuous cooling for operation while an outdoor training area is clearly not.

Another issue to be considered is "how long can the mission function before a loss of the controlled equipment will cause a mission failure?" For example, a computer server room might fail completely if it loses cooling for 30 minutes, while an office environment (even one performing a critical function) might continue to function for hours before their mission was impacted, and may be able to carry on indefinitely (with some reduced efficiency) without completely failing at their mission.

Finally, consider to what extent the controlled equipment relies on the FRCS for operation. For example, a lighting system controlled by an occupancy sensor that also has a manual on/off relies very little on the occupancy sensor for meeting mission goals.

The flowchart shown in Figure 5 may be helpful in deducing the connection between impact of the mission and impact of the FRCS. This chart embodies several concepts.

If the equipment controlled by the FRCS is critical, it likely requires the same level of backup power as the mission, which normally means local backup power generation.

If the equipment controlled by the FRCS is critical, there will likely be redundant equipment to allow for failure (e.g., mechanical) of a piece of equipment (e.g., broken belt, burned out bearing).

Are there local controls available that will allow staff (either installation Operations and Maintenance [O&M] staff or adequately trained mission staff) to restore operation of the equipment before the mission fails? Note that these manual controls might lead to reduced energy efficiency, but the key point is that the mission can continue with minimal disruption.

Can the O&M staff repair or restore system operation before the mission fails due to loss of the system?

The Integrity and Availability impact of the FRCS controls cannot be higher than the impact of the mission supported by the FRCS. FRCS rarely emphasize the impact of Confidentiality, but in cases where confidentiality is important the confidentiality impact rating of the FRCS impact may exceed the mission impact.

Figure 5. Deducing the connection between impact of the mission and impact of the FRCS.

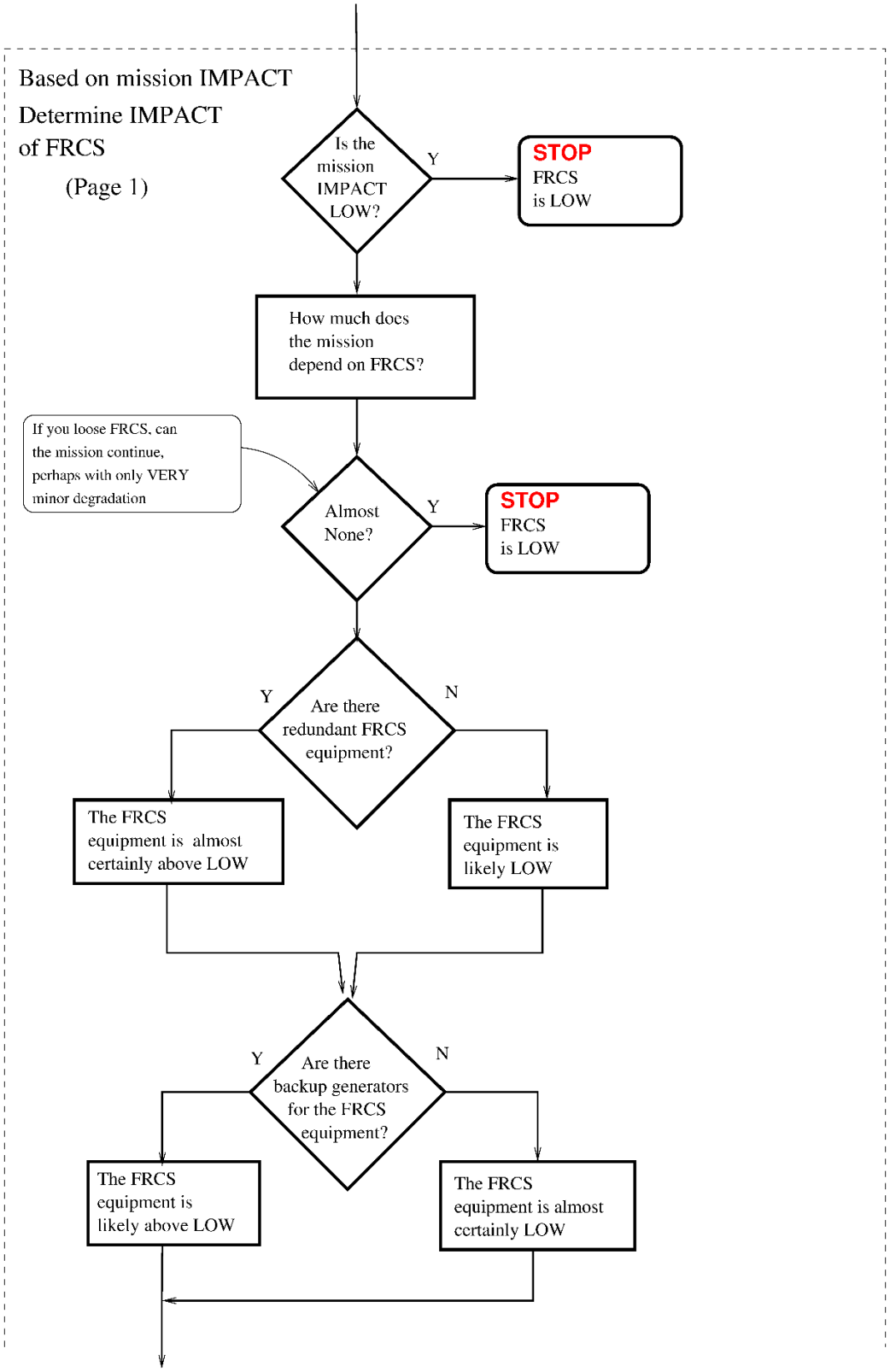
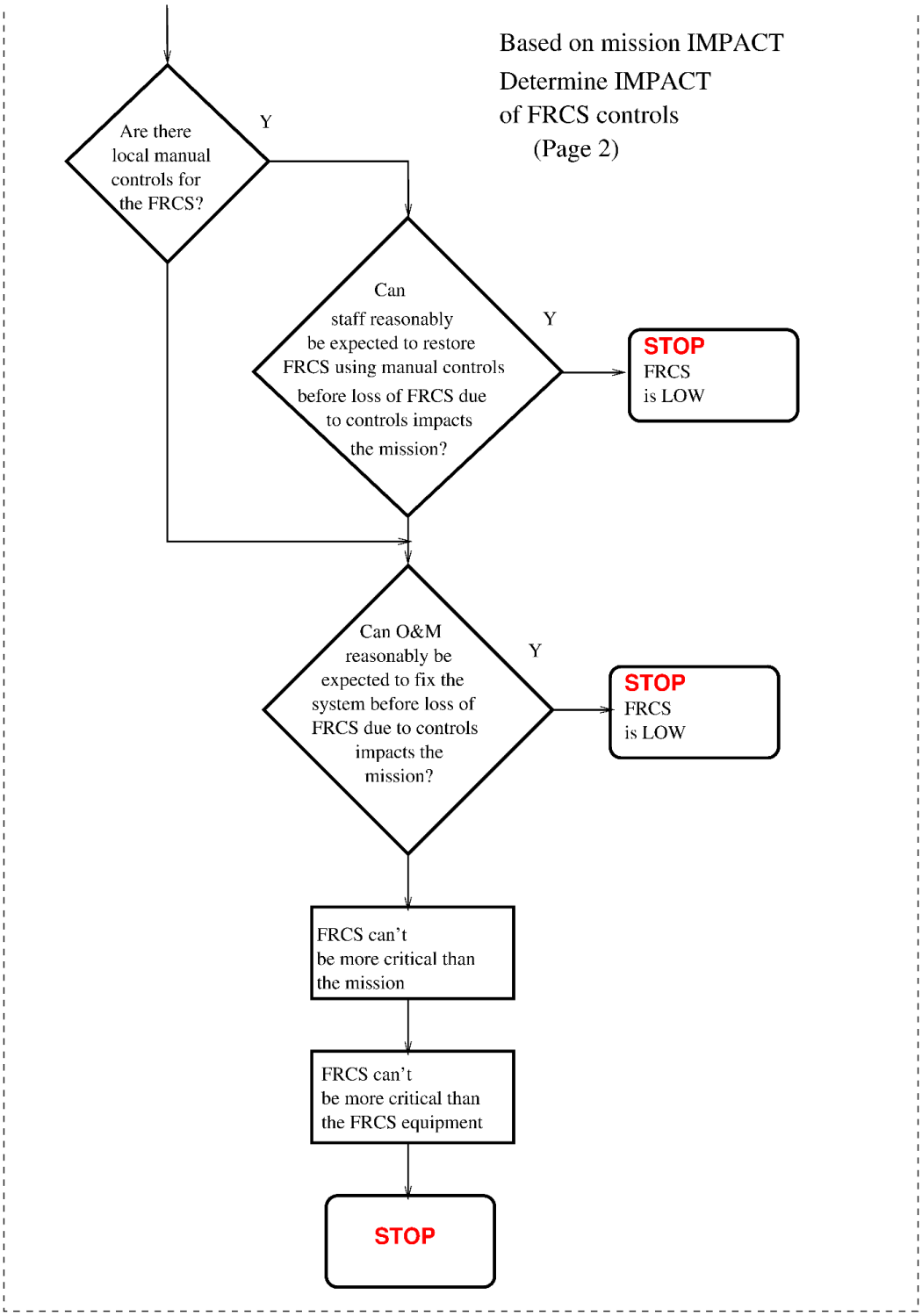


Figure 5. (Cont'd).



2.1.2.3 Addressing the critical control system

Several options for addressing a critical FRCS are suggested by the above drawing.

> Can manual controls be added to compensate for a compromised control system?
>
> Some critical facilities may be staffed 24/7. In this case, a local controls front end might be installed inside the facility and facility staff provided sufficient training to make basic adjustments to the system. Another option is to add local display panels (limited operator interfaces within the control system) in mechanical rooms, again with the intent of allowing onsite staff the ability to maintain system operation (perhaps in a degraded state, but sufficient to maintain basic mission capabilities).
>
> Can simple standalone backup systems be added to compensate for a failed (base-wide) control system? For example, for a data center, can a standalone CRAC* unit be added that would start based on a local thermostat and run independently of the base-wide system? Particularly in the case of a critical facility (which likely has redundant HVAC equipment), can the "normal" or "primary" unit be connected to the base-wide UMCS, while the "backup" or "secondary" unit operates in a standalone configuration with purely local controls?
>
> Some buildings may overall be non-critical, but have a small critical room or facility inside the larger building. Again, can a small standalone unit, such as a small DX† unit be added?

If the "standalone" system approach is used, this can (but not necessarily) mean that the "standalone" system cannot be monitored by the primary systems. Multiple strategies exist to allow for a lower impact system to monitor a higher impact system. Some of these strategies are described in UFC 4-010-06, *Cybersecurity of Facility Related Control Systems* (NFEC 2007).

2.1.3 System categorization based on Energy, Installations & Environment (EI&E) platform information technology (PIT) control system master list categorization

The EI&E Master List, available on the RMF Knowledge Service website, provides a *suggestion* for categorization dependent on system criticality, which is then broken down into system types. Note that these baseline categorization recommendations are NOT policy. **Ultimately. system criticality is determined by Authorizing Official (in coordination**

* Computer Room Air-Conditioning (CRAC) unit

† Direct Expansion (DX)

with the system owner and based on input from the designer of the control system).

> To find the Master List access the RMF Knowledge Service
> https://rmfks.osd.mil/login.htm
>
> Follow the instructions to Login to the RMF Knowledge Service
>
> Under RMF GENERAL, highlight IT, then, select PLATFORM IT.
>
> Look for the link titled ENERGY, INSTALLATIONS & ENVIRONMENT CONTROL SYSTEMS
>
> Read the Background
>
> Under KEY DOCUMENTS AND TOOLS click on EI&E CONTROL SYSTEM MASTER LIST (.XLSX)

Ensure that the EI&E CS Master List tab is selected. Column C reveals the following types of Facility Related Control Systems (FRCS)

> Building Control System (BCS)
>
> Utility Control System (UCS)
>
> UMCS.

Locate one of the system types listed above on the spreadsheet, and then reference Column F for the specific type of system you have. The UMCS is defined in Column F as a UMCS BUNDLED UCS AND/OR BCS. This means that your UMCS could incorporate different combinations such as a BCS (Heating, Ventilation, Air-Conditioning) along with a UCS (Central Plant Chilled Water System).

Columns H-P reveal three categories of mission criticality into which the facility/mission your system supports will fall. The DoD 5000.02 defines them as:

> *Mission Support*. Simply, not designated as mission essential or critical.
>
> *Mission Essential*. "…is basic and necessary for the accomplishment of the organizational mission. (designated by the DoD Component head)"
>
> *Mission Critical*. "…the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (designated by the DoD Component head)"

Assuming that the mission is (heavily) dependent on the FRCS, then the CIA values under the mission criticality for the facility/mission can be used as preliminary CIA values for the FRCS. Table 1 lists the values for a UMCS.

Table 1. UMCS system categorization based on mission criticality.

FRCS Type and Description		Preliminary Baseline C-I-A								
		Mission Support			Mission Essential			Mission Critical		
FRCS Type	System Name	C	I	A	C	I	A	C	I	A
Utility Monitoring and Control System (UMCS)	Utility Monitoring and Control System (UMCS)	L	L	L	L	M	M	M	H	H

Note that the CIA values for Mission Essential or Mission Critical facilities should be lower than shown on the Master List if the mission does not depend heavily on the FRCS.

NOTE: The EI&E Master List is not policy, rather guidance in helping you determine categorization. The focus on determining categorization is in the following instructions on the National Institute of Standards and Technology (formerly National Bureau of Standards) (*NIST*) Special Publication (SP) 800-60. For example, you may have a Physical Access Control System that does not nor should not rise to the suggested CIA impact categorization of MMH (for Moderate Confidentiality, Moderate Integrity, and High Availability Impact) as depicted in the Master List. Follow the next section and provide a clear concise categorization rationalization.

2.1.4 NIST SP 800-60, Vol. 2,-Rev. 1, Information Types

NIST SP 800-60, Volume II: *Appendices to Guide for Mapping Types of Information and Information System to Security Categories (NIST 2008)* is the goto document to help system owners determine the CIA values for the information processing types of their systems.

NIST SP 800-60, Table D-1, "Mission-Based Information Types and Delivery Mechanisms Mission Areas and Information Types" lists information type.

UMCS will most likely fall into information systems described in section D.7, "Energy." The information types in D.7 are:

Energy Supply

Energy Conservation and Preparedness (common information type for an Army UMCS)

Energy Resource Management

Energy Production

NIST SP 800-60, Table D-2 (summarized in Table 2, below) lists the anticipated CIA categorization for each of the above types. Note that UMCS fall in the Energy Conservation and Preparedness Information Type and has a baseline CIA level of Low-Low-Low.

Table 2. CIA categorization based on information type.

Information Type	Confidentiality	Integrity	Availability
Energy Supply	Low	Moderate	Moderate
Energy Conservation and Preparedness (includes UMCS)	Low	Low	Low
Energy Resource Management (does not include UMCS)	Moderate	Low	Low
Energy Production	Low	Low	Low

This is still not enough information for you to appropriately justify your CIA categorization. Go to NIST SP 800-60 section D.7 Energy, and review the definitions of the four types of Energy (as listed above) and determine what best fits your system. Select all information types that are applicable to your system. Make sure you look at the definitions, confidentiality, integrity availability and any special factors that could elevate the baseline CIA.

2.1.5 Required categorization rationale

When designating your CIA values in eMASS, the *SO* must also provide categorization rationale describing how they came to the CIA categorization determination. The categorization determination is one that is agreed upon between the SO and the AO. Described in a later section, the Package Approval Chain (PAC) consists of various RMF roles. The U.S. Army Network Enterprise Technology Command (NETCOM) operates in the Security Control Assessor-Representative (*SCA-R)*) and SCA-A (Army) roles. The *SCA-R)* and SCA-A will scrutinize the system categorization and ensure that the rationale supports the *SO*'s CIA claim.

Here is an example of why categorization rationale is important. Figure 6 shows a categorization rational submitted for Electrical Distribution System Disney Land.

Figure 6. Sample categorization rationale.

SYSTEM NAME: Electrical Distribution System Disney Land
ACRONYM: EDS-DL
APPLIED INFORMATION TYPES: Energy Production
CONFIDENTIALITY: Low
INTEGRITY: Low
AVAILABILITY: Low
CATEGORIZATION RATIONALE: (blank)

Upon NETCOM review the System Security Plan (SSP) was rejected with the following justification:

> "The system is being returned for the following reasons: (1) The Office of the Secretary of Defense for Energy, Installations and Environment (OSD EI&E) has issued categorization guidance for all DoD industrial control systems (ICS)/SCADA systems. The recommended categorization for Electrical Distribution Systems (EDS) is Moderate, Moderate, High. The information system owner (*ISO*) may recommend adjustments to these recommendation if justified, however, the information provided in the USAG* Disney Land record does not adequately justify deviating from these values. The ISO must either provide additional justification for lowering the potential impact values or alter the categorization."

By failing to provide sufficient categorization rationale months of work and planning for a Low, Low, Low baseline was threatened with CIA elevation.

The categorization rational was changed and the package was resubmitted with the following:

> CATEGORIZATION RATIONALE: USAG Disney Land is a Power Projection Platform, with category of Mobilization Force Generation Installation. The Minnie Mouse Depot (where the system is) is an Army Pre-Positioned Stock Site, not a critical facility PPP mission. The EDS system as named in eMASS and APMS is just a SCADA. The actual Electrical distribution system will operate with or without the SCADA. The SCADA monitors and can optimize the EDS but it DOES NOT deliver the energy supply.

* U.S. Army Garrison (USAG).

This well thought out categorization rationale saved the *SO* time and resources that would have been incurred due to the elevation of the CIA to Moderate, Moderate, High.

2.2 Army Portfolio Management System (APMS) registration

Before any system can receive an ATO through RMF, the system must first be registered in the APMS. APMS system description, and mission criticality must match exactly. This information can be changed and updated up until the system is submitted for the ATO. APMS is used for:

Army's feeder system to the DoD IT Portfolio Repository (DITPR) to support all Congressional, Office of Management and Budget (OMB), DoD and Army Reporting Requirements

Supports the Defense Business System (DBS) Certification and portfolio management processes

Supports Submission of the Army's Information Technology Budget

Army Data Center Consolidation Plan (ADCCP) Data Center Optimization and Closure Tracking.

The first step in APMS registration for you system is to obtain an APMS account (see Figure 7).

Navigate to APMS **https://cprobe.army.mil/login.htm?target=/enterprise-portal/web/apms**, you will most likely be redirected to the New Portal User screen.

Check PPBBOS-PLANNING, PROGRAMMING AND BUDGETING BUSINESS OPERATING SYSTEM (see pic below).

Click PROCEED TO REGISTRATION.

Fill out the form. For Echelon, select Army Command (ACOM) first and see if under ORGANIZATION you find yours.

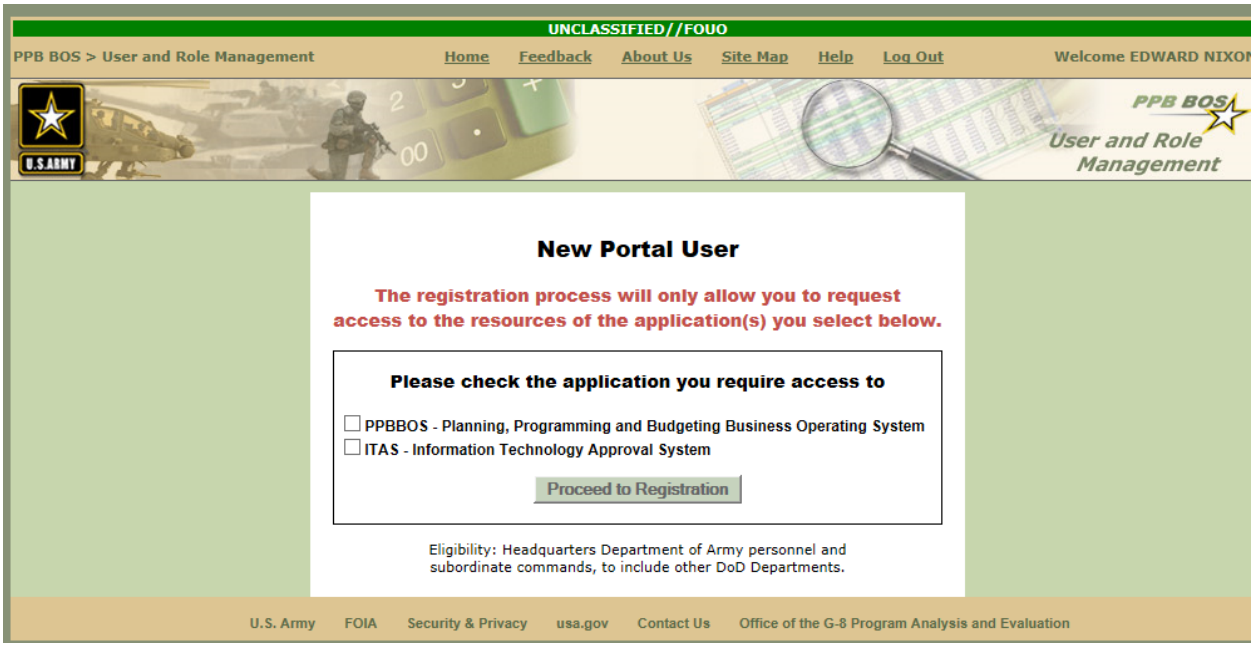
Once you have your APMS account, you can access the home screen to find all of the necessary APMS training and system registration information.

For further help contact APMS at:

Phone: 443-861-3712

Email: **usarmy.apg.cecom.mail.aitr-help@mail.mil**

Figure 7. APMS user registration screen.



2.3 Enterprise Mission Assurance Support Service (eMASS) account

eMASS is the RMF tracking system and the tool used to facilitate the following for RMF. Whereas APMS registration is IT system funding and tracking, an eMASS account supports the following RMF tasks:

System Security Plan (SSP)

Control Selection

Implementation Plan

Artifact Repository

Entering Test Results for all Control Correlation Identifiers (CCIs) (A CCI correlates to an assessment procedure [AP])

Plan of Action and Milestones (POAM)

Reports

Risk Assessment

Package Approval

Before you can have all the fun listed above, you must train and register for eMASS. If any other members of your staff will be responsible for uploading artifacts or supporting the RMF process, this is also a good time to have them train and register for eMASS.

RMF Overview/Training https://cprobe.army.mil/login.htm?target=/enterprise-portal/web/apms Provided by *NIST*

Defense Information Systems Agency (DISA) eMASS Training
https://cyber.mil/training/enterprise-mission-assurance-support-service-emass-5-5-2-cbt

(Select Enterprise Mission Assurance Support Service (eMASS). For location, select ONLINE)

eMASS Account Request https://army.emass.apps.mil/App/Home/Inbox (If more than one registered PKI certificate is displayed, highlight the PKI identity certificate that shall be used to access eMASS.)

Each organization will have specific requirements to approve the New User Registration request. Common documents are a completed DD2875, eMASS Training certificate and DOD Annual Cyber Awareness Challenge.

2.4 eMASS system registration

Initial eMASS registration (see Figure 29) is fairly simple and most likely you will not have all of the information required, however, many of the fields that are unknown can be initially populated with "TBD" (to be determined).

Upon Logging in to eMASS https://army.emass.apps.mil/App/Home/Inbox, Click on the NEW SYSTEM REGISTRATION LINK

Figure 8. eMASS registration screenshot.

2.4.1 Registration Step 1

System Registration will consist of four modules. Fields with a * are required. If you are unsure what to put, simply type TBD.

Tables 3 to 5 list steps you take to accomplish System Registration with some relevant comments.

Table 3. APMS Step 1, registration guidance.

Step 1-System Overview	Field Selection/Sample Entries	Comment
*Registration Type	Assess and Authorize	See Chapter 7 for Assess-Only guidance.
*System Name	Disney Land Utility Monitoring and Control System	This must match your APMS entry.
*System Acronym	UMCS-DL	This must match your APMS entry.
*Information System Owner		This is your Installation name (e.g., USAG Italy).
*Version/Release Number	1.0	Think "System Version."
*System Type	Platform IT	If your system is a Control System, then select Platform IT.
*System Life Cycle/Acquisition Phase		Determine what best fits your system in relation to your system development/sustainment.
National Security System		Mouse over the icon "i" to see the description.
Financial Management System		Mouse over the icon "i" to see the description.
Reciprocity System	Checked	Mouse over the icon "i" to see the description.
*System Description		This must match your APMS entry.
* DITPR ID		If APMS has not given you this # use a placeholder such as DA000000.
DoD IT Registration Number		Mouse over the icon "i" to see the description.

Table 4. APMS Registration Step 2, guidance.

Step 2- Authorization Information	Field	Comment
*Security Plan Approval Status	Not Yet Approved	This field should be changed once you receive the System Security Plan (SSP) approval in later steps.
*Authorization Status	Not Yet Authorized	Unless you have an ATO, IATT.
Need Date		Not a required field but the Operational-need-date of the ATO.
* RMF Activity	Initiate and plan cybersecurity Assessment Authorization	Look at choices. Where in the process are you at. If beginning choose field suggested here.
Terms/Conditions for Authorization		Unsure of the value of this during initial registration. Not a required field.

Table 5. APMS registration step 3 guidance—package approval chain (PAC)/control approval chain/view only role.

Step 3-Roles Package Approval Chain	Field	Comment
* *ISO*/Program Manager (PM)		This is reserved for the person(s) designated as Information System Owner (ISO) or PM.
*Organizational *ISSM*		The local ISSM responsible for the system.
*Program ISSM		Will be someone at your headquarters level. (e.g., IMCOM ISSM).
* *SCA-R)*	SCA-R	If your system is an Army system, then NETCOM will be the SCA-R.
* SCA-A	SCA-A	If your system is an Army system, then NETCOM will be the SCA-A.
*AO		Choose the AO designated for your Command (e.g., for IMCOM choose IMCOM AO).
STEP 3-ROLES Control Approval Chain		
*ISO/PM/ISSO		Select your ISO/PM/ISSO (Information System Security Officer) as in the Package Approval Chain.
SCA-V		This can be left blank unless you have already determined the SCA-V.
STEP 3-ROLES View Only Role		Anyone you want to have the capability to “view” the system record with no edit rights.
STEP 3-ROLES Auditor Role		Use only if a particular Auditor group is to be assigned.

3 RMF Step 2: Select Security Controls

3.1 Security controls

Per the RMF Knowledge Service, "Controls are safeguards/countermeasures prescribed for information systems to protect the CIA of information that is processed, stored, and transmitted by the systems; and to satisfy a set of defined security requirements."

There is a broad range of control types. For example, controls can include: passwords, physical barriers, encryption schemes, firewalls, training, software vulnerability patches, and data backups. Controls define the physical, administrative, and technical requirements your system must meet to be considered compliant. Systems may not be able to meet every intent of the control and must be *Risk Accepted* by the AO.

> Controls are deemed Common, Hybrid, or System-Specific (to be discussed later).
>
> Controls can be Tailored IN or OUT to reflect system-specific circumstances
>
> Controls are further broken down into assessment procedures, or compliance procedures, called Control Correlation Identifiers (CCIs)

The Controls for RMF are derived from the *NIST* SP *800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (NIST 2014).

The appropriate controls to be applied to your system are based on the CIA determination you made earlier. For example, if the CIA determination was LOW, LOW, LOW, then the controls designated as LOW impact for confidentiality, integrity, and availability from NIST SP 800-53A will be applied.

An excellent way to discover the Controls by family, or by a combination of CIA with various impact values is through the RMF Knowledge Center:

> Access the RMF Knowledge Center: https://rmfks.osd.mil/login.htm
>
> Under RMF General highlight SECURITY CONTROLS and select SECURITY CONTROLS EXPLORER.
>
> Choose the individual Control Family or All Control Families.
>
> Choose the Impact rating for CIA
>
> Select the first control you see, which will most likely be Access Control AC-1, and review the text for each of the following:

Control Text

Supplemental Guidance

References

Security Categorization

Implementation Guidance and Assessment Procedures

Reveal the CCIs, to be discussed in a later section.

3.2 Tailoring

The RMF allows SOs and *ISSM*s to review the baseline control set (control set determined by applying the impact level to confidentiality, integrity and availability) and Tailor In or Out controls. This is not a license to cut out the hard stuff. Rather, if the SOs and ISSMs analyze their systems and control set and appropriately determine those that are Not Applicable (NA), and they can provide sufficient justification as to why, then the finalized control set can be sent through eMASS and approved by the AO. Table 6 lists example steps for tailoring out controls.

Table 6. Example steps for Tailoring out controls.

Control	Control Text	Statement Of Non-Applicability
AC-18	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wires access: and b. Authorizes wireless access to the information system before allowing such connections.	The XYZ UMCS does not incorporate wireless access to any components of the system. Wireless IS NOT authorized for the system.
AC-5	The organization: a. Separates [Assignment: organization-defined duties of individuals]; b Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	The *NIST* 800-82 ICS Overlay allows the control to be set to Not Applicable for Control Systems.

If the system implements a technology or service that has an associated control not in the baseline, then the *SO* and ISSM should tailor in the Control. See section 3.2, “Overlays.” Applying an overlay may add to or subtract from the baseline control set. An example of tailoring in a control would be applying privacy controls if your system contains anything defined as personally identifiable information (PII).

3.2.1 Common (inherited)

NIST 800-37 defines a common security control as "A security control that is inherited by one or more organizational information system(s)."

The DoD CIO identifies common security controls (called Tier 1 common controls) that are satisfied by existing DoD policy and guidance. DoD information systems (ISs) and Platform IT Systems (s) may be automatically compliant with Tier 1 common controls. You will see these in eMASS when you apply the Army Policy Record (to be discussed later).

Every control that your system can inherit will result in fewer controls that you must prove compliance with. There are many factors that determine whether or not your system receives any inheritance.

> Do you have a Service Level Agreement (SLA) with a network provider such as the NEC to provide system administration for any parts of your system such as servers and or workstations? If so, then then the network provider or NEC can automatically make a listing of inheritable controls that you can associate your package to. Note: The SO will need to work actively with the NEC to establish an SLA for the specific system under consideration.
>
> The network providers or NECs may or may not automatically make a listing of inheritable controls. If they do not, then you or the *ISSM* for the system must determine per the SLA which controls are inheritable and then "manually" associate the determined inheritable controls in eMASS.
>
> Is/are your server(s) located in the network provider or NEC's facility? If so, then your system will be able to inherit certain controls that pertain to physical and environmental requirements.
>
> Is your system standalone and solely managed by you/ *ISO*? Your system most likely would not have any controls to inherit.

Ask yourself this question, "Is any portion of my systems security, operation or maintenance the responsibility of someone outside of my organization?" If the answer is "yes," then some controls may be that entity's responsibility and can be marked as "inherited" for your system.

3.2.2 Hybrid

NIST 800-37 defines a Hybrid Security Control as "A security control that is implemented in an information system in part as a common control and in part as a system-specific control."

3.2.3 System-specific

A system-specific control is a security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

3.2.4 Control families

Controls are organized into family groups (Table 7) that indicate the major subject or focus areas to which an individual security control is assigned.

Table 7. Control families.

Identifier	Subject Family
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 Authentication
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 Service Acquisition
SC	System and Communication Protection
SI	System and Information Integrity

3.2.5 Control Correlation Identifiers (CCIs)

A Low, Low, Low system without any tailoring or overlays applied generally will have a baseline of approximately 310 controls. Each control will have at least one or more CCI that reveals the Implementation guidance and Assessment procedure to make the Overall Control Compliant. For example, for AC-19 to be compliant, the CCIs listed in Table 8 must be satisfied.

Table 8. Control correlation identifiers.

Control	CCI	CCI Description (Guidance and Procedure)
AC-19	CCI-000082	The organization establishes usage restrictions for organization controlled mobile devices.
	CCI-002325	The organization establishes configuration requirements for organization controlled mobile devices.
	CCI-002326	The organization establishes connection requirements for organization controlled mobile devices.
	CCI-000083	The organization establishes implementation guidance for organization controlled mobile devices.
	CCI-000084	The organization authorizes connection of mobile devices to organizational information systems.

In the above example, to satisfy the AC-19 control, five CCIs must be deemed compliant. If a single CCI is non-compliant, then the whole control is deemed non-compliant.

3.3 Overlays

An overlay is a set of security controls applied during the tailoring process. The overlay may:

Complement and further refine the control baseline.

Make the control baseline more or less stringent.

Add or subtract controls from the baseline.

Overlays have several advantages

Overlays that subtract controls from a baseline are listed as Not Applicable in the Security Plan.

Personnel are not required to create a POAM (see section 6.2 for POAM) entry for controls deemed NA.

Overlays can simplify the tailoring process.

3.3.1 Current available overlays selectable in eMASS

Cross Domain Solutions (CDS)

Space Platform

Intelligence (FOUO)*

Classified Information

Privacy

* For Official Use Only (FOUO)

3.3.2 *NIST* 800-82 ICS overlay

The NIST SP 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security* (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf) is a key document for applying Cybersecurity and RMF to Control Systems. Since FRCSs are a subset of ICSs, it is highly recommended that *ISO*s, and *ISSM*s read the NIST SP 800-82 in its entirety.

NIST SP 800-82, Appendix G, Table G-1 "Security Control Baselines," summarizes the *ICS Overlay*. Figure 9 shows a sample of the NIST table, in which AC-4, AC-5, AC-6, AC-10, AC-11, and AC-12 are "not selected" for a Low Categorized system. In essence, those controls were tailored out by the overlay.

Figure 9. Security control baselines.

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3**
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	**AC-5**	**AC-5**
AC-6	Least Privilege	Not Selected	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control	Not Selected	Not Selected	**AC-10**
AC-11	Session Lock	Not Selected	**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination	Not Selected	**AC-12**	**AC-12**
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	**AC-17**	**AC-17 (1) (2) (3) (4)**	**AC-17 (1) (2) (3) (4)**
AC-18	Wireless Access	**AC-18**	**AC-18 (1)**	**AC-18 (1) (4)** (5)

Source: NIST SP 800-82, Appendix G, Table G-1.

As of the date of this manual, the ICS Overlay HAS NOT been added to eMASS to be selected, however this does not preclude SOs from using the Overlay.

There is an easier way to determine your baseline control set using the ICS Overlay than by manually processing the table in *NIST* SP 800-82.

Access the RMF Knowledge Service https://rmfks.osd.mil/login.htm

Under RMF GENERAL, highlight IT, then, PLATFORM IT.

Look for a link titled ENERGY, INSTALLATIONS & ENVIRONMENT CONTROL SYSTEMS, then click it.

Under KEY DOCUMENTS AND TOOLS click on NIST SP 800-82 R2 ICS OVERLAY SECURITY CONTROLS (.XLSX)

Upon opening the spreadsheet, select the 2nd tab labeled CONTROLS BY SELECTED CIA values, then:

Select your CIA values

Review the FINAL CONTROL SET (After Overlay is Applied)

Review the COMMENT OUT THESE CONTROLS

Review the ADD THESE CONTROLS

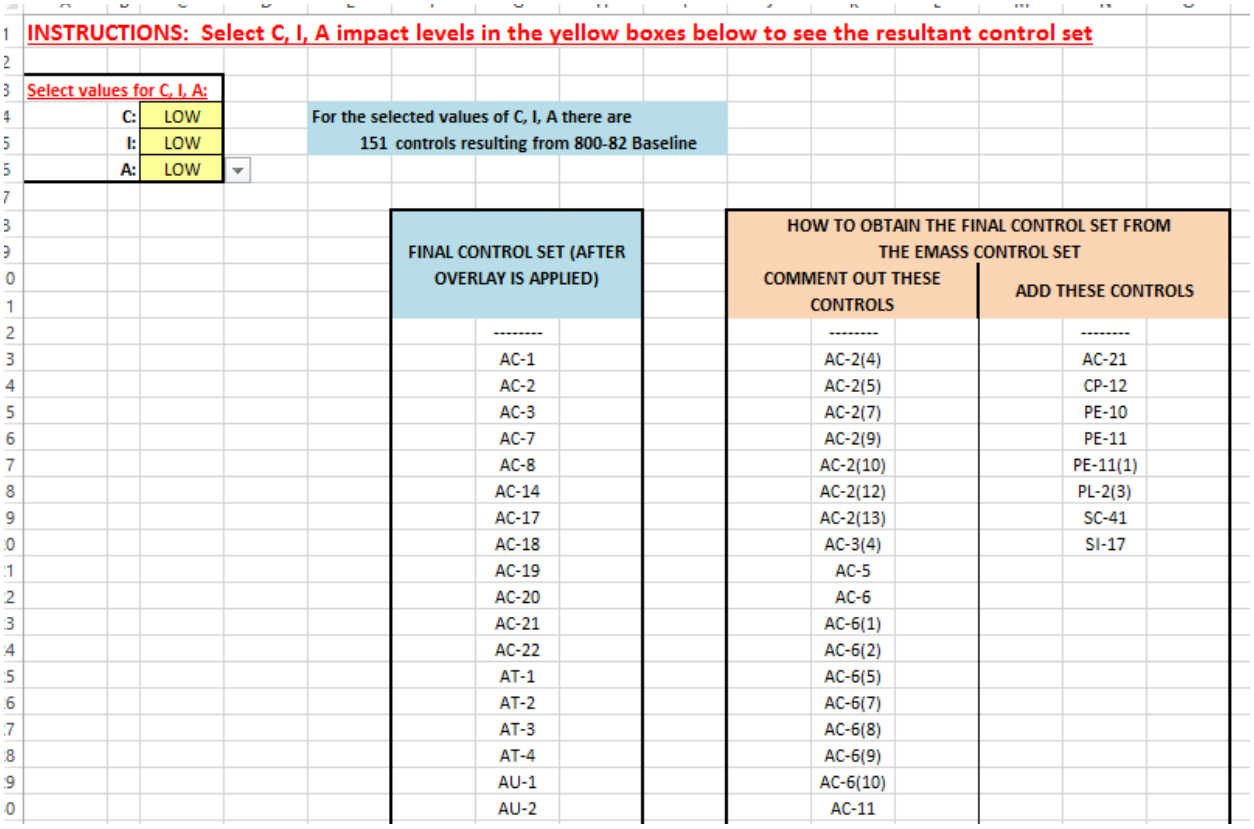
The COMMENT OUT THESE CONTROLS section is important. You can use this to fill out your implementation plan in eMASS by selecting them as NA, and using the *NIST* 800-82 ICS Overlay as justification for the NA designation.

Figure 10 shows an example of a CIA of LOW, LOW, LOW revealing the final control set, the controls to comment out, and the controls to add.

3.4 Implementation plan (eMASS)

The Implementation Plan's purpose is often misunderstood, even from the days of the Department of Defense Information Assurance Certification and Accreditation Program (DIACAP). The Implementation plan SHOULD NOT be the place where control compliance is assessed. Rather, the Implementation Plan should simply be used by the *SO* and *ISSM* to denote "where" they believe the system is in relation to control compliance. Simply put, are the controls Implemented, Planned, Inherited or Not Applicable? The comments section should be used for rationale as to "why" a control was set to Not Applicable or to document any deviation from implementation guidance.

Figure 10. Control set example.



INSTRUCTIONS: Select C, I, A impact levels in the yellow boxes below to see the resultant control set

Select values for C, I, A:

C: LOW
I: LOW
A: LOW

For the selected values of C, I, A there are 151 controls resulting from 800-82 Baseline

FINAL CONTROL SET (AFTER OVERLAY IS APPLIED)	HOW TO OBTAIN THE FINAL CONTROL SET FROM THE EMASS CONTROL SET	
	COMMENT OUT THESE CONTROLS	ADD THESE CONTROLS
---------	---------	---------
AC-1	AC-2(4)	AC-21
AC-2	AC-2(5)	CP-12
AC-3	AC-2(7)	PE-10
AC-7	AC-2(9)	PE-11
AC-8	AC-2(10)	PE-11(1)
AC-14	AC-2(12)	PL-2(3)
AC-17	AC-2(13)	SC-41
AC-18	AC-3(4)	SI-17
AC-19	AC-5	
AC-20	AC-6	
AC-21	AC-6(1)	
AC-22	AC-6(2)	
AT-1	AC-6(5)	
AT-2	AC-6(7)	
AT-3	AC-6(8)	
AT-4	AC-6(9)	
AU-1	AC-6(10)	
AU-2	AC-11	

Go to your systems record in eMASS. Under the CONTROLS tab, click on IMPLEMENTATION PLAN. There are two ways to populate the Implementation Plan.

Click on each Control Acronym and enter the information individually.

Download the Implementation Plan Template.

It is highly recommended to download the template. The instructions for populating the template will be the same as doing it directly in eMASS.

3.4.1 Exporting the implementation plan template

Under the CONTROLS Tab (Figure 11), select LISTING.

Under CONTROL ACTIONS click on IMPORT/EXPORT

On the right under CONTROL INFORMATION, choose EXPORT ALL

Save this file. You will build your Implementation Plan from this file, then do a bulk upload to have it populated in eMASS.

Figure 11. Exporting implementation plan screenshot.

3.4.2 Populating the implementation plan template

The template reveals all the fillable fields under the BLUE IMPLEMENTATION PLAN heading. However, depending on the IMPLEMENTATION STATUS you choose for each control, it will have different required fields. For the following, fill in the appropriate fields on the template under IMPLEMENTATION PLAN

3.4.2.1 Planned or Implemented

If you know the control is PLANNED, meaning, it is applicable and you know that the control has not been implemented then enter following:

Implementation Status: Planned

Security Control Designation: Select COMMON, SYSTEM-SPECIFIC, or HYBRID (See earlier section on Controls for definitions) Hint: if the control is inherited then select common. If it is a combination of inherited and system-specific select HYBRID.

Estimated Completion Date: When the control is expected to be implemented/was implemented

3.4.2.2 Inherited or manually inherited

If the control is provided by another entity such as a NEC …

Implementation Status: Inherited

Common Control Provider: Identify the source of the Inheritance, DoD, COMPONENT or

Security Control Designation: If Inherited then select COMMON.

Estimated Completion Date: Enter current date.

3.4.2.3 Not Applicable

If you have deemed that the control is Not Applicable either because of the application of *NIST* 800-82 as an overlay or for another reason (i.e., it is being "tailored out" for a some reason).

Implementation Status: Not Applicable

Justification: Enter a thorough justification as to why the control is deemed NA. For example, if the control us deemed NA through the application of NIST 800-82 as the overlay: "The control is not applicable because the control is not in the ICS Baseline (NIST 800-82, derived from NIST 800-53A)."

Security Control Designation: If the control is NA, then most likely you will choose System Specific or Hybrid.

Estimated Completion Date: Enter current date.

3.4.3 System-level continuous monitoring strategy (eMASS)

While populating the Implementation Plan for your system, you are required to fill out the System-Level Continuous Monitoring Strategy (SLCMS). This in itself can be a source of confusion and frustration. Step 6 of the RMF process is Continuous Monitoring. Continuous Monitoring requires that the system maintain an acceptable level of security. Continuous Monitoring means that the *SO* actively assesses the security of the system. (See section 6.2 "Recurring activities")

According to NIST 800-37, it is up to the SOs to determine the frequency with which security controls are monitored. This is subjective. So how do we determine this? Read the following sections and read each control to make your best assessment. Remember, you must be able to justify the rationale behind the monitoring frequency for each control.

The *NIST* 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information System and Organizations." Provides insight into determining some of the requirements. This is not entirely straight forward and easy to apply as each system is different. Continuous Monitoring requirements should be determined based on the following:

Security Control Volatility. Volatile security controls are assessed more frequently. An example of volatile controls are the Configuration Management family. System configurations on workstations and servers can change frequently and therefore open the system up to exploit if not monitored and

mitigated frequently. On the other hand, controls in the Personnel Security family such as PS-2, Position Categorization and PS-3, Personnel Screening are not volatile in many organizations and could be reviewed on a yearly basis rather than monthly, etc…

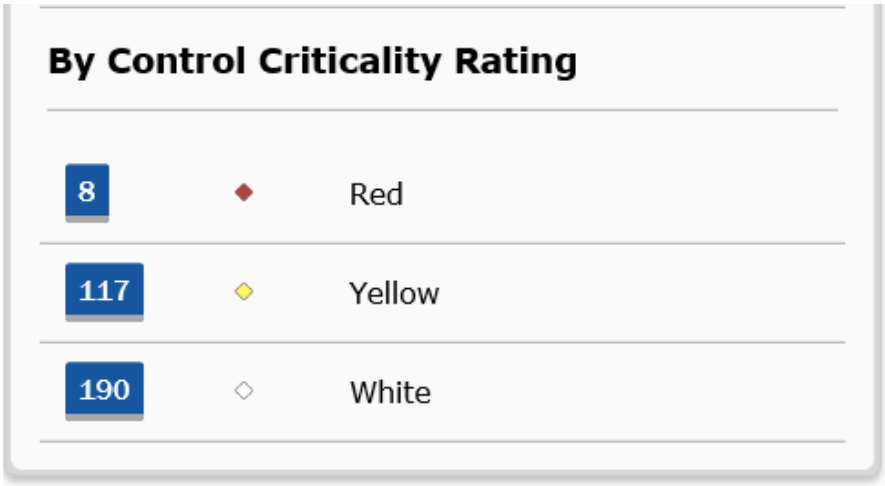
System Categorization/ Impact Levels. High impact categorized systems controls would be monitored more frequently that Low impact categorized systems.

A standalone BCS categorized as a LOW, LOW, LOW would be considered a LOW impact system.

A system categorized as a MODERATE, MODERATE, HIGH would require the availability controls to be monitored at a higher frequency since the impact to availability is HIGH.

Security Controls or Specific Assessment Objects Providing Critical Functions. Controls that provide critical functions such as log management server, firewalls and malicious code protection should have more frequent monitoring. In eMASS under the Controls tab find the graphic "By Control Criticality Rating," click on the Red Controls [see Figure 12]. These are controls that should be monitored more frequently than Yellow or White. This coding is automatically set in eMASS based on a typical IT system and this determination may not be appropriate for an FRCS. In particular, it does not differentiate between a workstation and a controller.

Figure 12. Control criticality rating count.



Security Controls with Identified Weaknesses. Findings from the RMF assessments are documented in the Risk Assessment section of eMASS. If they have not been mitigated in the POAM – the "how are we going to fix things" document), they are still considered a risk or a weakness and would require a greater frequency of monitoring. However, LOW or VERY LOW impact weaknesses identified would still not require the monitoring frequency that weaknesses deemed MODERATE or HIGH would.

Organizational Risk Tolerance. The AO for a particular system may have a low tolerance for risk and require systems to monitor the controls on a more frequent basis.

Threat Information. Current credible threats, known exploits and attacks can require certain controls to be monitored more frequently. If physical breaches to fences or buildings are common in a general area, then physical security controls may need to be monitored at a higher frequency to ensure that security is maintained.

Vulnerability Information. Vulnerabilities are often identified in software applications. Therefore, if a company like Microsoft sends out patches once a month, then specific technical controls may need to be monitored monthly.

Risk Assessment Results. The third party assessor known as the Security Control Assessor-Validator (*SCA-V*) is responsible for assessing Army systems and will provide their findings in relation to non-compliant controls in the Risk Assessment section of eMASS. As a part of the assessment, non-compliant controls will be rated as seen in the graphic below. The Residual Risk Level (see Figure 13)can be used to aid the *SO* in determining the monitoring frequency.

Figure 13. Risk assessment summary.

Risk Assessment Summary

Security Control Distributions expand

Control Acronym	Status	Severity	Relevance of Threat	Likelihood	Impact	Residual Risk Level
AC-1	NCO	Low	Moderate	Low	High	Low
AC-2	NCO	Low	Moderate	Low	High	Low
AC-2(1)	NCO	Very Low	Moderate	Very Low	High	Low
AC-2(2)	NCO	Low	Moderate	Low	High	Low
AC-2(3)	NCO	Very Low	Moderate	Very Low	High	Low

Reporting Requirements- DoD, Army, and Federal Information Security Management Act (FISMA), may specify certain reporting requirements. For example, FISMA requires the following to be reported annually. Controls relating to the following could be set to an annual basis.

Contingency Plan Test

Security Control Test

Subset of controls each year

Security Review

Baseline control set

3.4.3.1 System-Level Continuous Monitoring (SLCM) in eMASS

Below are the fields within the Implementation Plan in eMASS for the SLCMS and a description of what the field is looking for. Following the de-

scription of the fields, Figure 14 shows the current Army guidance for populating these fields. (Use the Implementation Plan Template as described above. Upload all as a single IMPORT.)

> *Criticality*: Indicate the criticality of monitoring the Control as Red, Yellow, or White. Explain what drives the criticality for monitoring. For example, the categorization of the system, the nature of the operations, the type of environment (e.g., volatile or hostile), the sensitivity of the information, the nationality of the users/operators, etc. can drive the criticality.
>
> ******NOTE***: Army eMASS may automatically populate this field for you.
>
> *Frequency*: Indicate the frequency with which the Control is monitored. Explain what drives the frequency in the SLCM* comments field. The value of "constantly" may only be appropriate for high impact systems, and for functions most critical to sustaining the cybersecurity posture. For example, one may need a constant awareness of the fact the firewall between the Non-Secure Internet Protocol Router Network (NIPRNet) and the Internet is up and running (i.e., the access control lists have not been compromised and are not letting through traffic from attackers). Automated tools may be the only means to achieve "constant" monitoring. A particular security control may state a value such as how often passwords are to be changed, however that does not necessarily correlate to what the frequency of monitoring for that control should be. For example, Security Control CP-9, Information System Backup, requires data backups, and the CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems, assignment value is "at least weekly or as defined in the contingency plan." However, would not necessarily want to confirm each week that a user had performed the weekly backup. Rather, it may be sufficient to confirm on a monthly or a quarterly basis, depending on the system categorization. Availability of information on the backups is more critical for a system categorized at HIGH for Availability than it is for a system categorized at LOW for Availability; therefore, higher categorized systems should have backups performed more often.
>
> *Method*: Indicate the method of monitoring the Control. Explain what drives or limits the method of monitoring in the SLCM comments field. The method often depends on the criticality and frequency of monitoring. Automation may be the only realistic means to monitor a large set of the technical security controls on a very frequent basis. Conversely, it may be sufficient to use manual means to monitor the management type of security controls (e.g., are policies and procedures – the dash-1 Controls such as AC-1 – published and current?). The availability of continuous monitoring tools often constrains the method. For legacy, mission, or disconnected (from the DoD Information Network) systems, there are not likely many automated tools readily available, at least not those centrally managed by *DISA* or United States Cyber Command [USCYBERCOM]). As such, the method may be manual, and the procedures used to assess the security control before system authorization might need to be used to continuously monitor; that is, the ISSO or SCA runs those assessment procedures periodically.
>
> *Manual*: Often selected for management type of security controls or when no automation is available, feasible, or affordable.

* System-Level Continuous Monitoring (SLCM)

Semi-automated: Selected for controls that cannot yet be fully automated or where it is most feasible to monitor some aspects manually.

Automated: Often selected for higher criticality or frequency; assumes the organization has resources to implement automation.

Reporting: Provide a short narrative explaining who reports what to whom by when. The reporting mechanism may vary depending on the criticality of the security controls. Examples of reporting mechanisms/actions are provided below, reflecting the urgency.

Red Security Controls: via telephone or high-priority email, the system-level *ISSM* reports the situation immediately and directly to the AO, while keeping the cybersecurity chain of command informed of status and response actions; if time permits, an authorization/connection decision recommendation is provided to the AO.

Yellow Security Controls: via telephone or email, the system-level ISSM reports to the cybersecurity chain of command, and after appropriate (but not prolonged) investigation into the severity/urgency of the situation, the AO is advised and provided an authorization/connection decision recommendation.

White Security Controls: system-level *ISSM* resolves the situation in due course, keeping the cybersecurity chain advised via email or normal tracking tools (e.g., eMASS); the AO is contacted for an authorization/connection decision only if the risk cannot be reduced back to the accepted level in a reasonable time.

Tracking: Provide a short narrative explaining how security controls found to be non-compliant or ineffective will be tracked. The system's POAM may be used to track the least critical Controls, but updating the POAM and conveying such updates to authorities can be a somewhat lethargic process. The POAM is not usually dynamic enough to track fast actions associated with identifying, analyzing, and correcting the more critical security controls in real time. More responsive methods of reporting and tracking are necessary for real-time risk management. Such methods may not be readily available for legacy, mission, or disconnected systems; therefore, specialized tools may need to be developed. If so, centralized solutions are desirable and should be developed and managed at the organizational level (i.e., higher than a single program office).

SLCM Comments: Provide a short narrative further explaining any other details not appropriate for the other columns. For historical and analysis purposes, it is often necessary to provide a rationale for why values were set as they were for criticality, frequency, method, reporting, and tracking. The SCA will need this information when determining if the SLCMS is in synch with the Security Assessment Plan (SAP). The AO will need this information when deciding whether to approve the SLCMS.

Figure 14. Army guidance on SLCMS population.

NOTE: AS OF April 23, 2018. ARMY GUIDANCE ON SLCMS POPULATION
Current Army guidance is to populate the new required fields as follows:
CRITICALITY:
This will be populated with the Control Criticality Rating.
For White security controls use “CRWG White Criticality Control”
For Yellow security controls use “CRWG Yellow Criticality Control”
For Red security controls use “CRWG Red Criticality Control”
FREQUENCY - Select “Undetermined”
METHOD - Select “Undetermined”
REPORTING - Use “Reporting is undetermined.”
TRACKING - Use “Tracking is undetermined.”
SLCM Comments – Use “No additional SLCM comments

3.5 Implementation plan bulk upload

Once your Implementation Plan is completed on the template, perform a bulk upload.

Go to your systems record in eMASS

Under the CONTROLS tabs click on LISTING

Under CONTROL ACTIONS click on IMPORT/EXPORT

On the right side under CONTROL INFORMATION browse for your Implementation Plan Template

For Import Type Select IMPLEMENTATION PLAN

Click UPLOAD

3.6 System security plan approval (eMASS)

At this point you should have the initial registration for your system in eMASS and some preliminary fields/artifacts populated or uploaded in the Artifacts section.

Implementation Plan completed

Categorization Complete with Information Types and Rationale for Categorization

Hardware and Software List

Generally the hardware list will only consist of components down to level 1 non- IP components such as chillers, boilers and other non-IP controllers.

Software list should include all software loaded on the system.

Privacy impact Assessment (PIA) DD Form 2930

National Security System Identification Checklist (See Page 10 of the NIST 800-59)

Network Diagram (see section 3.3.2 Network/Topology Diagrams)

Data Flow Diagram (see section 3.3.2 Network/Topology Diagrams)

Your AO representatives may require more or less of the above listed. Generally, this is all you need to obtain the SSP approval to begin populating your test results.

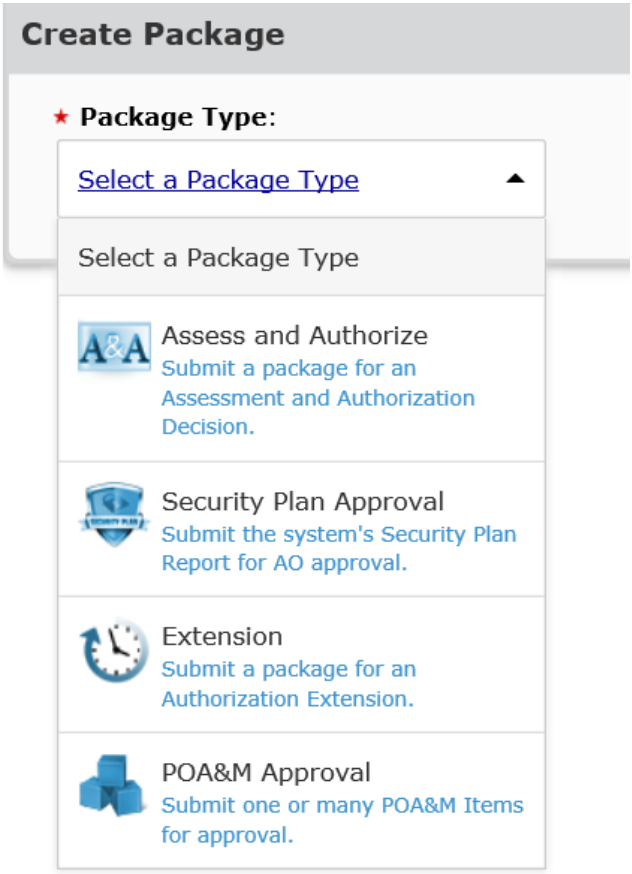
The purpose of submitting your SSP for approval is to have the AO concur with your CIA categorization and stated control set. To submit the SSP do the following:

Go to the eMASS record of the system you wish to submit for approval

Click on the PACKAGE tab

Under Package Type select the drop down and choose SECURITY PLAN APPROVAL (see Figure 15)

Figure 15. Security plan approval screenshot.



The package will go up the Package Approval Chain to the AO. The AO's signature is an approval of your stated control baseline and categorization. If the designated personnel disagree with any of the elements submitted, they may reject the package with explanation of what needs to be corrected before proceeding any further.

4 RMF Step 3: Implement Security Controls

By this point the Implementation Plan has been completed and you know the control set for your system. The implementation of security controls are accomplished in a couple of ways. The first is through some technical configuration, a setting such as the system requiring and enforcing passwords to be a minimum of 15 characters. Technical configuration of the control system components can and should generally be required of the installing contractor for new systems. For technical configuration of legacy systems or for items outside of the responsibility of the installing contractor, the services of a security engineer may be required. The *CSC-MCX* can provide or assist in procuring these services.

UFC 4-010-06 identifies controls that can be incorporated into control system design and made requirements for the installing contractor. Unified Facilities Guide Specification (UFGS) 25 05 11 provides specification language to the installing contractor to meet many of these controls.

The second is through a non-technical means such as defining a policy or a physical solution. An example would be a policy that the organization specifies requiring all users must use a 15 character password. This policy makes users of the system aware of the requirements. The system owner's organization is ultimately responsible for these items, although an outside security engineer can support the development of policies and other support (e.g., contractor or the installation security organization) may be required to support physical solutions. The CSC-MCX can provide security engineering and/or assist in procuring these services.

When entering the test results (to be discussed later) for your system, proof of the implementation of security controls may be found in written policy and procedures or through scans verifying compliance.

4.1 Inheritance

The RMF Knowledge Service does an excellent job explaining Common Controls or Inherited Controls.* Click on the link here to read more in depth about inherited controls. Between the DoD Tier 1 and Army Policy Record, an IT sys-

* https://rmfks.osd.mil/rmf/General/SecurityControls/Pages/CommonControls.aspx

tem is able to inherit up to 409 CCIs spanning 25 Controls. To take advantage of this you must apply the Army Policy Record to your system in eMASS. To apply the Army Policy Record:

Go to the systems record in eMASS

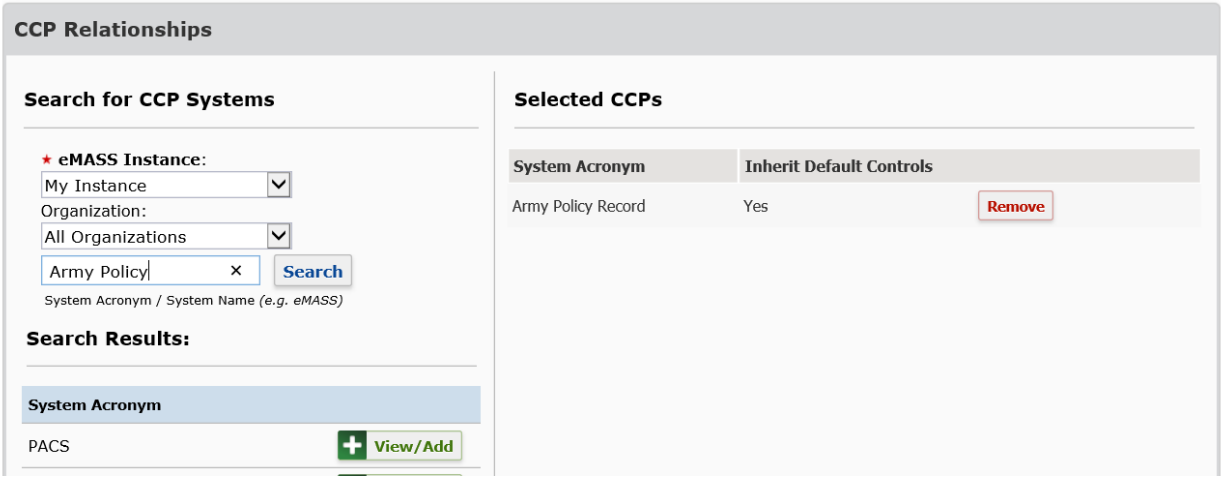
Highlight the MANAGEMENT tab and click on ASSOCIATIONS (INHERITENCE)

Click on MANAGE COMMON CONTROL PROVIDERS

In the SEARCH FOR CCP SYSTEMS box type in ARMY POLICY (see Figure 16) and click Search

Once you see it below, click VIEW/ADD

Figure 16. CCP relationships screenshot.



Now test results for all Controls/ CCIs listed in the Army Policy Record will show Compliant for your system. Note that this compliance assumes the implementation of the common controls and inherited controls is in accordance with the DoD Tier 1 and Army Policy Record requirements. Standard IT components of the control system (computers, some IP network hardware etc.) will meet these requirements but other components (particularly controllers) will not be able to fully implement them

Systems that operate on a network managed by someone else can receive more inheritance. Also, if your servers and/or equipment are housed within a data center not controlled by you then there are other physical security controls that can be inherited. For example, if your servers are housed in the Redstone Arsenal Network Enterprise Center (RNEC) server room then your system can inherit certain physical security controls. If your system operates on their network and receives boundary defense,

Host Bases Security System (HBSS), patching, etc… then you can inherit even more controls. (see section 2.1.2 Common (Inherited)

First step would be to follow the same process as you did to associate the Army Policy Record. Find the local NEC's record and see if they have made specific controls inheritable.

There are many instances where the local NECs or network provider have not made their controls inheritable. Nevertheless, if you know that another entity is responsible for a particular control, mark it as INHERITED and sufficiently explain why in the comments section of the CCI.

4.2 Technical control implementation

Many legacy systems or brand new systems will have very few security controls applied. The DoD and Army mandate certain settings and configurations for various operating systems (OS), applications and network devices. This is also called system-hardening. System-hardening can be performed by applying the Army Gold Master (AGM) OS image or through the application of Security Technical Implementation Guides (STIGs).

Sections 3.2.1 through 3.2.3 are technical solutions to IT using Windows or Unix based OSs or network devices commonly found on the *DISA* Approved Products List (APL). FRCS components generally do not have an applicable STIG or an AGM and therefore must implement security in a different way. Section 3.2.4 will cover FRCS components.

4.2.1 Army Gold Master (AGM)

The AGM Program develops baseline configurations for commonly used desktop and server environments within U.S. Army IT networks. The AGM Program baseline is intended to be the initial configuration that Army IT personnel will use to develop local configuration baselines.

Installing the AGM, or the AGM with a local configuration baseline (local NEC additions) can be a giant leap forward in securing your system if it is installed on your server and workstations versus applying security off of a base OS install, or out-of-the box configuration.

If your system is to be Public Key Infrastructure (PKI) enabled (used with a CAC) and run on the local network providers network (e.g., NIPRNET),

then most likely your system will be required to receive the AGM with the network provider's configurations. Again, this will save time and money in hardening the system.

If your system is to operate in a purely standalone mode or the use of field devices (laptops) that are never connected to the network, then the AGM would not be required, yet still would be preferred with some tweaks to allow it to operate without PKI enabled (e.g., uses username and password instead of CAC).

Contact your local network provider, or NEC on how to obtain a copy of the AGM for your system.

4.2.2 Secure Content Automation Protocol (SCAP)/Security Technical Implementation Guides (STIGs)

The SCAP is a software tool that assesses a particular OS and associated applications/software tools that are run on the system for compliance with specific mandated standards called STIGs. If an entity such as the NEC maintains your system, then they would be the ones to apply the SCAP and STIGs.

For example, a basic control system may include a Windows 10 workstation connected to a Programmable Logic Controller (PLC) and then to some level 1 or 0 components (as defined in the 5-level architecture). To appropriately assess the system, you need to know the applications/software running on the workstation that have an applicable STIG/benchmark, for example:

Windows 10 OS

Adobe Acrobat Reader

Microsoft Internet Explorer

Microsoft .net

Microsoft Structured Query Language (SQL)

Internet Information Services (IIS)

APACHE

In this case, to assess the system appropriately you would need to download the SCAP Compliance Checker (SCC) Tool for Windows OS, then the SCC Benchmarks (the STIGS) for Adobe Acrobat, Internet Explorer, and Microsoft .Net, which are the parameters used to check the system. Each of these will produce a score revealing how well the particular application is secured.

You will also download the STIG Viewer and import the results from the SCAP and the STIG Benchmarks. The SCAP performs all of the Automated Checks. Once imported into the STIG Viewer you will notice there are some checks that SCAP did not perform called "Not Reviewed" also called manual checks. The *SA* will be required to go through each manual check independently to assess whether it is a finding or not. Within each checklist there are several tabs for each check. The CCI tab can be used to correlate a particular checks compliance or non-compliance with the test results in eMASS.

It is out of the scope of this document to teach SCAP, STIGS and the STIG Viewer, however, Click below on an excellent YouTube resource that explains it all. There are also links to the IASE *DISA* site to find the SCAP tools and STIGs.

Video Tutorial - Assessment and Remediation using SCAP Tool https://www.youtube.com/watch?v=Q8F1Bh-fU1I&index=3&list=PLu2VX3M94wM2V5fb27jL-bxjE-NQpaFgG

PDF Tutorial* **-** Getting Started with the SCAP Compliance Checker and STIG Viewer https://www.dcsa.mil/portals/91/documents/ctp/tools/SCAP_Compliance_Checker_and_STIG_Viewer_Job_Aid.pdf

Site Content

SCAP Content and Tools https://cyber.mil/stigs/downloads/

STIGS https://cyber.mil/stigs/downloads/

4.2.3 STIG deviations list

A part of the RMF process is for a third party validator to assess your system. This validator will review the STIGs applied or not applied to the system. It is imperative that any required STIG check that cannot be applied to a system is documented with justification as to why it cannot be applied. This STIG deviation list can be loaded into the artifacts section of eMASS and have a corresponding POAM entry for each STIG deviation so that the AO can grant a "risk accepted."

Also, continuous monitoring will be a requirement for all systems accredited under RMF. SCAP scans will be a requirement. Again, it is imperative to document and justify any deviation to a STIG requirement for Risk Acceptance by the AO.

* Portable Document Format (PDF)

4.2.4 Assured Compliance Assessment Solution (ACAS)

The ACAS is an integrated software solution that provides automated network vulnerability scanning, configuration assessment, and network discovery. ACAS consists of a suite of products to include the Security Center, Nessus Scanner, and the Nessus Network Monitor (formerly the Passive Vulnerability Scanner), which is provided by *DISA* to DoD Customers at no cost. DISA's Cyber Development (CD) provides program management for the Enterprise ACAS offering as well as help desk support and training.

For FRCSs that will communicate using installation campus area networks (ICANs) managed by local NECs, ACAS scans will mostly likely be automatically performed as part of their ongoing overall network management and can be provided to you for upload into the systems eMASS record.

NOTE: The ACAS solution provides the required automated network vulnerability scanning, configuration, assessment, application vulnerability scanning, device configuration assessment, and network discovery. ACAS generates reports. ACAS is different than SCAP in that SCAP does not check for vulnerabilities such as missing security patches and OS updates.

ACAS is mandated for DoD use. For more information on ACAS visit the *DISA* ACAS Site (https://www.disa.mil/Cybersecurity/Network-Defense/ACAS)

4.2.5 FRCS component hardening

Most FRCS components do not have a vendor specific STIG or AGM for security hardening. Hardening of these types of devices can also hinder their functionality. Nevertheless security must be a consideration and measures should be taken where possible and noted where they cannot. Below are some ways to implement security in FRCS components and devices.

4.2.5.1 Factory defaults

Just like a Linksys router used in a home network, many FRCS components that support accounts are shipped with a default username and password. Oftentimes these defaults are not changed and give an attacker easy access to the device. Ensure that all devices using accounts and passwords are changed from default settings to the most secure settings allowed by each device.

4.2.5.2 Physical security

The most common security mitigation to devices that cannot implement technical security controls is simply restricting access to them. A control system network device in a locked cabinet with proper key control restricts unauthorized access and or modification to such devices. Unauthorized access can be determined by physical destruction or absence of a key from key control.

4.2.5.3 Generic STIGs

While the following is not vendor specific or necessarily a perfect fit, they can be used to manually assess devices and apply security where feasible. *SCA-V*s, sometimes will (rightly or wrongly) assess a Field Point of Connection (FPOC) by manually reviewing compliance with the following:

If the device is a network management device e.g., control system firewall, Ethernet switch, network device, Zigbee (Institute of Electrical and Electronics Engineers [IEEE] 802.15.4) gateway device, or IP-based controller etc., navigate to https://cyber.mil/stigs/downloads/?_dl_facet_stigs=network-perimeter-wireless%2Cnetwork-infrastructure. Look for the Network Device Management SRG STIG (Security Requirements Guide Security Technical Implementation Guide).

Another option would be to manually apply, where feasible the Network Other Devices STIG.

If the device contains an embedded OS navigate to https://cyber.mil/stigs/downloads/?_dl_facet_stigs=operating-systems to apply the General Purpose Operating System SRG.

If the device or technology hosts a web interface, navigate to https://cyber.mil/stigs/downloads/?_dl_facet_stigs=app-security%2Cweb-servers and apply the Web Server SRG.

4.2.5.4 Vendor specific security hardening guides

While this may not apply to most legacy FRCS components, many vendors are providing security best practices or hardening guides for newer devices. Research vendors sites for their recommended hardening guides.

4.2.5.5 Patching

FRCS components may have vulnerabilities that require patching/updating the component. Keeping up with vendor specific patches and firmware updates can help ensure that risk to vulnerabilities is kept low. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (https://ics-cert.us-cert.gov/) provides information specific to FRCS components vulnerabilities and even how and where to obtain patch remediation. However, note that ICS-CERT is industrial control system focused on does not have much information for a typical BCS.

4.3 Developing policies and procedures (artifacts)

As stated before, the implementation of security controls can also be accomplished through an organization defining policies and procedures for a system or having other artifacts such as network diagrams, hardware and software list. All of these artifacts are stored in eMASS as evidence of security control implementation.

4.3.1 Control family documents

How security controls are addressed in the test results section of eMASS is extremely important. There will be a third party assessor, the *SCA-V* who will validate the compliance or non-compliance of every CCI. You can make their job easy or hard. If you make them search through endless artifacts to determine compliancy, chances are, they may miss some.

By developing Control Family Documents, all Controls and CCIs for each family are contained in their own document.

There are 18 Control Families (see section 2.1.5 Control Families), which means 18 separate documents.

The following is an example of an entry in The Identification and Authentication (IA) Control Family Document of three Security Controls and 25 CCIs being addressed by a single section of the document.

9. AUTHENTICATOR MANAGEMENT (IA-5), PASSWORD-BASED AUTHENTICATION (IA5(1), AUTHENTICATOR FEEDBACK (IA-6)
The National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4 identifies many forms of individual authenticators that can be used on an information system. The authenticator used primarily for the XYZ System is account identifier(s) and password(s). The Account Manager is responsible for assigning and monitoring the account(s) and password(s) as explained in the Account Management section of the Access Control Policy **CCI-001980, CCI-000176, CCI-001984, CCI-001986, CCI-001998, CCI-001982, CCI-001981, CCI-001990, CCI-002041, CCI-001985.** Implementation of password policy, for all accounts, will be directly managed by the System Administrator (SA) with oversight provided by the system CCB **CCI-002042**. All privileged and non-privileged user account passwords will consist of 14 characters **CCI-000205**. For components (e.g., PLC's, RTU's, and Human Machine Interface (HMI)'s) that cannot meet the password requirements, the strongest password that is technically feasible will be applied. The general rules for password strength are as follows **CCI-001544:**
Passwords must have at least 2 uppercase, 2 lowercase, 2 numbers, and 2 special characters **CCI-000192, CCI-000193, CCI-000194, CCI-001619**
Cannot contain four consecutive alphabetic characters in any order (AAaa or AbCa)
Cannot contain repetitive characters (AA, ==, bb,44)
For new passwords, at least 50% of the minimum password length must be changed **CCI-000195**
Cannot use any of the prior 5 passwords **CCI-000200, CCI-000181** It is XYZ System policy that all passwords are obscured when being entered to avoid password exploitation **CCI-000206**. All personnel with account access to the control system are required to complete DoD and Army mandated training on password usage and protection **CCI-002365, CCI-001621**. In most cases, vendors and integrators will program control system components and software with well-known and easily discoverable passwords to make installation of the component or software easier. These are considered as factory set or default passwords. The risk to the system if these factory passwords are not changed is significant. The ISSM is responsible for ensuring that all factory set or vendor/integrator default passwords for the system are changed and meet the criteria above within 30 days of new component or software deployment **CCI-001989**. As the Account Manager, the SO or ISSM maintains a current list of all accounts on the system as well as the individual username(s) for those accounts (please refer to the Account Management section of the Access Control Policy). This document is sensitive and for official use only and must be stored properly on an encrypted hard drive or locked in a safe for paper copies **CCI-000183.**

Again, creating Control Family Documents addresses all of the security controls and CCIs in a clean and verifiable fashion.

Other plans that will be required and may not necessarily be a Control Family Document are:

Continuity of Operation Plan (COOP)

Configuration Control Board (CCB) Charter

Incident Response Plan (IRP)

4.3.2 Network/topology diagrams

A Network Diagram is a required artifact that represents your system, its accreditation boundary, internal and external connections graphically.

Army systems are to follow *DISA* Topology Standards. The following describes the required information for different devices.

4.3.2.1 Servers

Server Function

Web Server

SQL Server

Application Server

Operating System

Current Service Pack Version

Complete IP Address

4.3.2.2 Workstations/laptops

Workstation/Laptop

Operating System

Current Service Pack Version

Complete IP Address

4.3.2.3 Routers/switches/firewalls

Router/Switch/Firewall

Manufacture/Model

Software/Firmware Version

Complete IP Address

4.3.2.4 Various IP-based control system components

These are the level 2 devices (as defined in the 5-level architecture, see Appendix B)

Manufacture/Model

Software/Firmware Version

Complete IP Address

4.3.2.5 Various non-IP-based control system components (networked)

These are the level 1 devices (as defined in the 5-level architecture, see Appendix B)

Manufacture/Model

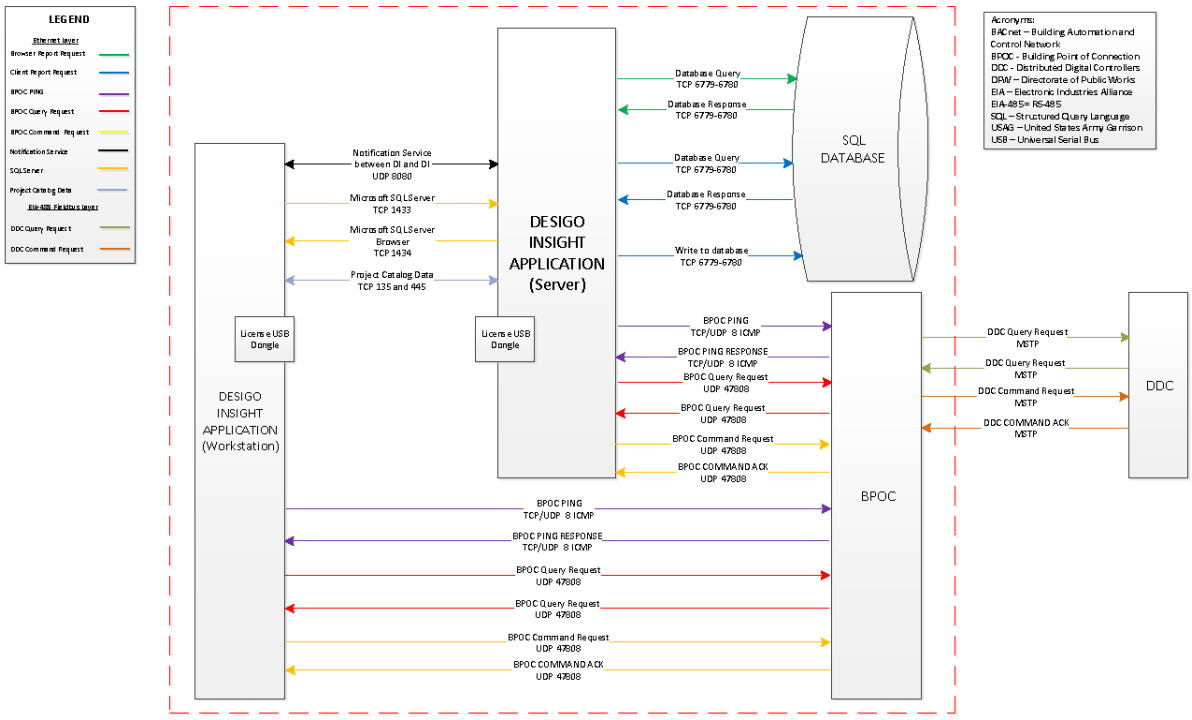
NOTE: Not required to represent all quantities, rather a representation and total #

4.3.3 Data flow diagram

The Data Flow Diagram is to be a visual representation of the ports, protocols and services used. It should depict the way traffic flows within the system along with any external connections.

Figure 17 schematically shows an actual UMCS that underwent the RMF (note that BPOC [Building Point of Common Connection] as used in the figure is an outdated term and has been replaced with FPOC).

Figure 17. Data flow diagram.



4.3.4 Hardware and software lists

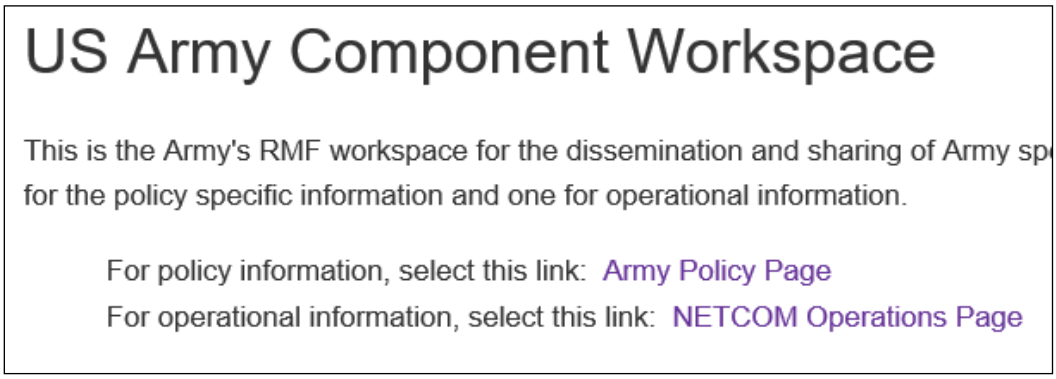
You must account for all of the Hardware (HW) and Software (SW) within the system boundary. A HW/SW template can be found on the NETCOM Operations page as described below. Generally, the hardware list will only

consist of components down to level 1 non-IP components such as chillers, boilers and other non-IP controllers. To access:

Go to the Knowledge Service **https://rmfks.osd.mil/rmf/Pages/default.aspx**

Highlight the COLLABORATION Tab, then COMPONENT WORKSPACES and select U.S. ARMY COMPONENT WORKSPACE (see Figure 18).

Figure 18. Component workspace screenshot.



Click on NETCOM OPERATIONS PAGE

Click on U.S. ARMY DOCUMENT LIBRARY, click on the TEMPLATES folder.

Download and save the HWSWList_Template

4.3.5 Ports, Protocols, and Services Management (PPSM)

The PPSM program ensures that Internet Protocols, Data Services, and associated Ports used in DoD information systems, applications, and boundary protection devices are cataloged, controlled and regulated.

Every system is required to register the Ports, Protocols and Services used within the system.

DISA offers an excellent training library for understanding and registering PPSM. Click on the link below and look for PPSM:
https://disa.mil/network-services/Enterprise-Connections/Mission-Partner-Training-Program

4.4 Uploading artifacts to eMASS

Up to this point, we have covered the required artifacts for RMF. These artifacts reveal compliance with controls and CCIs. The Artifact section of eMASS acts as a repository for required artifacts and updates to artifacts. It is important to know the controls and CCIs that are satisfied by each artifact before uploading. See “Associate Controls/CCIs to Artifacts” for details.

It is imperative upon adding a new artifact to eMASS that you identify any CCIs that are satisfied by the artifact.

Access system eMASS entry

Click on Artifacts, then ADD ARTIFACT

Under ASSOCIATE CONTROLS and/or APs

On the drop down, select the control family the document relates to, be sure to check INCLUDE Aps, and click SEARCH

Under ARTIFACT INFORMATION

Enter the name of the artifact

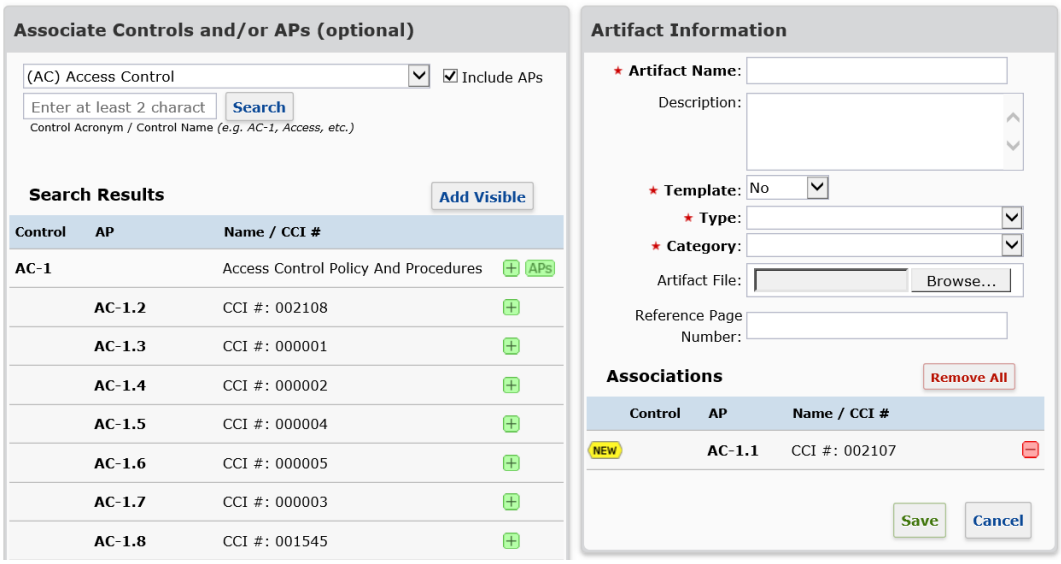
Answer TEMPLATE, TYPE and CATEGORY

Browse for file … but DO NOT HIT SAVE YET

On the left hand side you will see the Controls, and the CCIs under each control (see Figure 19).

Click the green PLUS sign for every CCI that should be associated with the Artifact. If all the CCIs under a particular control are relevant, just click the plus sign next to the overall control.

Figure 19. Associate controls screenshot.



In the above screenshot, I clicked the PLUS sign next to AC-1.1 and it was transferred to the rights side under ASSOCIATIONS.

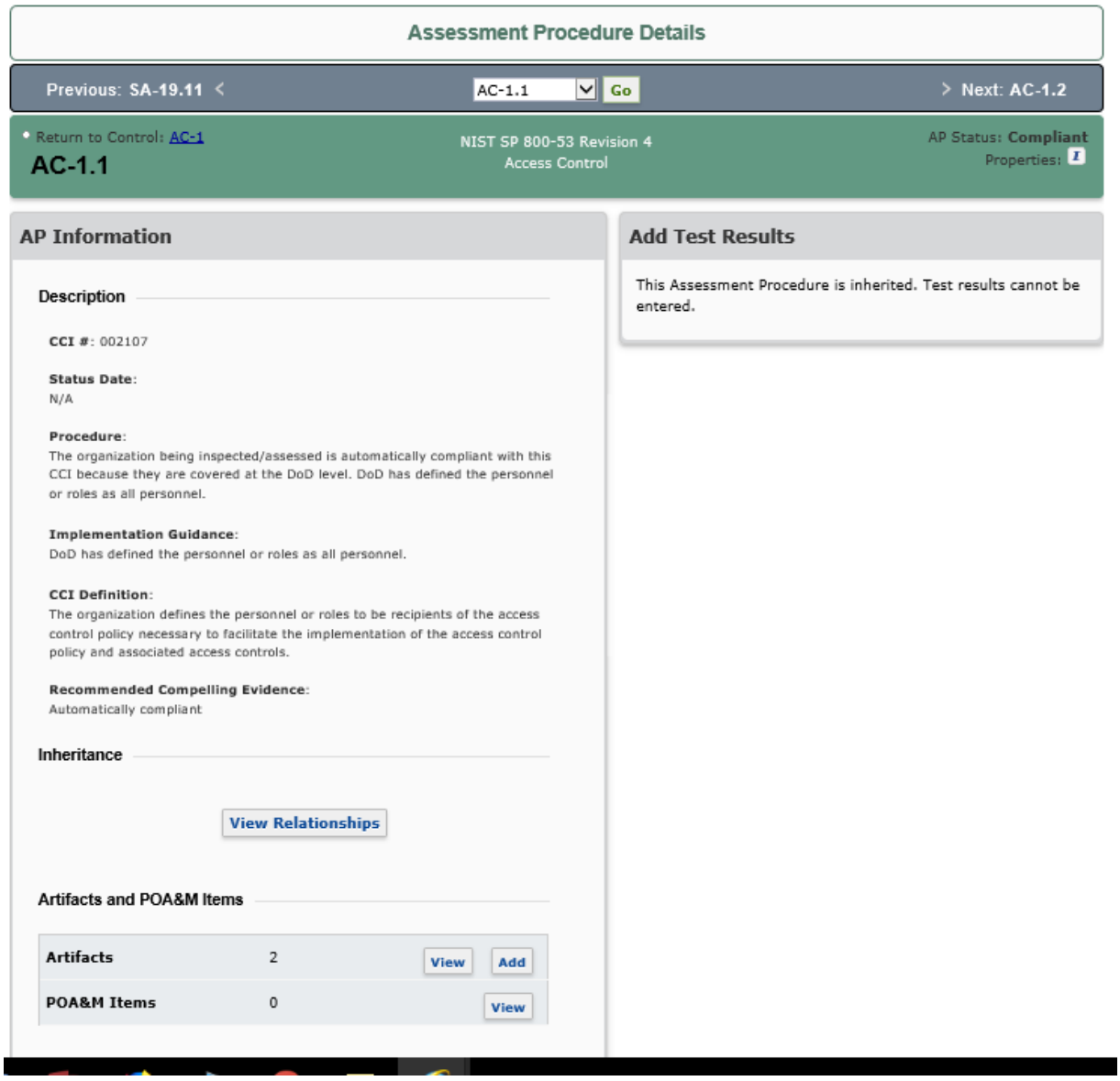
Continue selecting all applicable CCIs

Select another control family if more apply to the particular artifact.

Once complete click SAVE

When you navigate to the CONTROLS section and select AC-1.1, you will see that an Artifact is tied to this Control/CCI (see Figure 20). The Assessor can click VIEW to see all artifacts associated with the selected CCI.

Figure 20. Assessment procedure details screenshot.



The process of association of CCIs to artifacts should happen for every CCI, whether it be a policy, procedure, screenshot or scans.

4.5 Entering test results (self-assessment) in eMASS

At this point you have accomplished the following:

Categorized your system

Selected your controls

Implemented your controls

Developed/Associated artifacts

Now you will perform the Self-Assessment, meaning, you will enter the test results for each Control/CCI into eMASS. Performing the Self-Assessment is your declaration of the Compliance, Non-Compliance, or Non-Applicability of the controls and a statement to support each determination.

There are TWO ways to perform the Self-Assessment (entering the test results); manual, and bulk upload.

4.5.1 Manual

Select the CONTROLS Tab, then LISTING

On the right side, you will see the controls family groups.

Expand the **first** control family (e.g., AC)

Expand the **first** control to reveal the CCIs (e.g., AC-1)

Click on the first CCI (e.g., AC-1.3 CCI:000001)

NOTE: If the control is INHERITED then you cannot enter a Test Result (see Figure 21)

Enter Status

Compliant

Non-Compliant

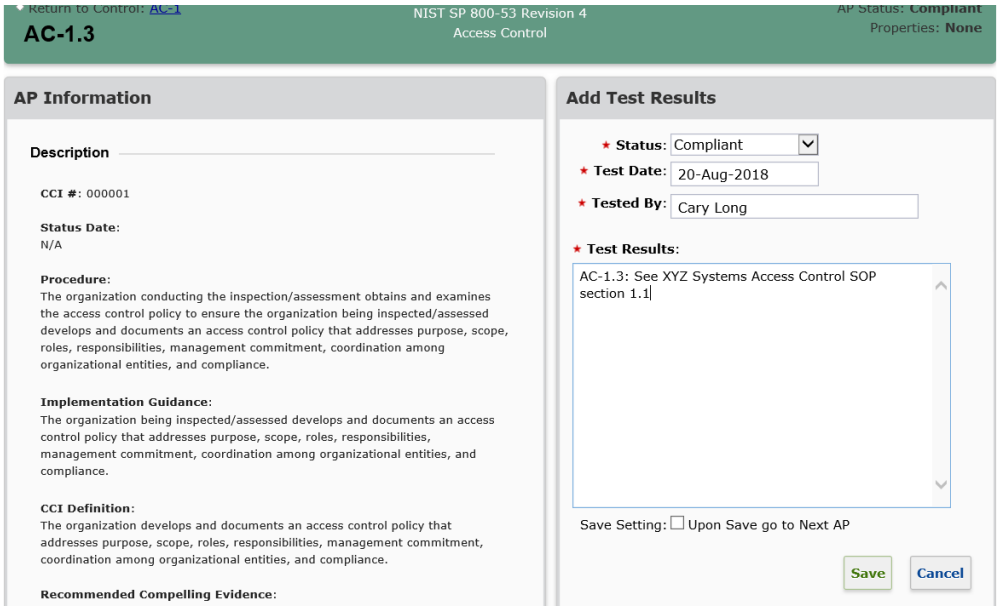
Not Applicable

Enter Test Result

This should be a description of “how” the control has been made compliant or “why” the control is Not Applicable.

Click SAVE

Figure 21. Access control.



Continue this process for every CCI that you want to enter a Test Result for. Subsequent updates/revisions will be displayed in the TEST RESULT HISTORY at the bottom.

EXAMPLE COMPLIANT TEST RESULT:

AC-1.3: See XYZ Systems Access Control Standing Operating Procedure (SOP) section 1.1

EXAMPLE NOT APPLICABLE TEST RESULT:

This CCI is not applicable because the control is not in the ICS Baseline (NIST 800-82, derived from the NIST 800-53A).

4.5.2 Bulk upload

The Bulk Upload option allow you to work offline using excel then, upload ALL Test Results at one time.

Select the CONTROLS Tab

Under Control Actions click IMPORT/EXPORT

Under TEST RESULTS/EXPORT click EXPORT ALL

Then SAVE or OPEN the file

Read the Instructions tab, then the Example tab

Under the TEST RESULT IMPORT tab, all of the Controls/CCIs will be listed.

Any Inherited Controls will have information already populated under the LATEST TEST RESULTS columns

For all other CCIs (ones to be made Compliant or Not Applicable) enter the Test Result in the ENTER TEST RESULTS HERE columns (should be in blue).

When you are ready to upload all or a portion of the Test Results do the following:

In eMASS go back to CONTROLS/LISTING, then click IMPORT/EXPORT

Under TEST RESULT/Import, Browse the file to upload

Upload

If there are errors, it will let you know. You can make corrections directly at that point or exit, correct the spreadsheet, and then attempt to Import again.

NOTE: If you only upload a portion of the Test Results, ensure that you go back and EXPORT ALL as you did above to obtain a fresh Test Result bulk upload spreadsheet. Previously entered Test Results will now show up in the LATEST TEST RESULTS columns. You will only enter NEW Test Results in the updated Blue Section of the template.

5 RMF Step 4: Assess Security Controls

5.1 Security Control Assessor (SCA)

The SCA role as defined by the NIST SP 800-37 is "an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security…of an information system."

What does that mean? This is a group that will verify what you say is compliant with your system. They will determine the level of risk associated with your system and make their recommendation to your AO as to whether or not to grant an ATO, or a Denial of Authority to Operate (DATO).

For the Army, this group is broken down into four different roles.

SCA-Army (NETCOM)

SCA-Representative (NETCOM)

SCA-Validator

SCA-Organization

For the purposes of this training we will focus on the SCA-V and *SCA-O*.

5.2 SCA-V

The SCA-V team are DoD reimbursable (you pay for their services) organizations that are appointed by the Army to be the official validator for Army systems. SCA-V estimates are dependent upon the size and complexity of your system but a typical range is $45,000 to $75,000. Again, the size and complexity of your system will be the determining factor. For a full description of the SCA-V and associated activities go to the RMF Knowledge Center and access the NETCOM Tactics Techniques and Procedures (TTP).

Log in to the Knowledge Center

Highlight COLLABORATION/Component Workspaces

Click U.S. ARMY COMPONENT WORKSPACE

Look for and click NETCOM OPERATIONS PAGE

Click on U.S. ARMY DOCUMENTS, then click TTPs

Find SCA-V TTP

5.2.1 The SCA-V team mission

Conducts comprehensive assessments of the management, operational, and technical security controls implemented within or inherited by your system.

Determines the overall effectiveness of the controls.

Provide an assessment of the severity of weaknesses or deficiencies discovered in your system and its environment of operation.

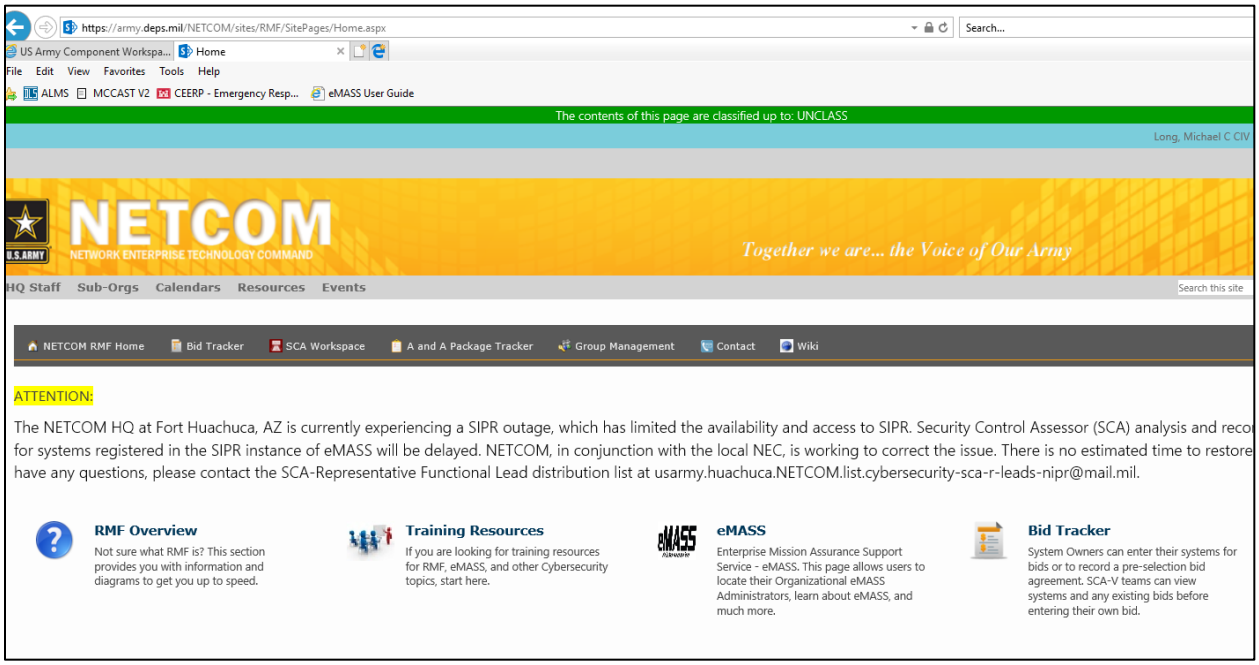
Recommends corrective actions to address any identified vulnerabilities.

5.2.2 How to obtain a SCA-V

The Bid Tracker is the primary application to submit for bids by the Army approved SCA-Vs. It is best to seek bids and secure a SCA-V within 6 months of the operational-need-date of an ATO. Generally, I recommend determining when the system will be ready for an assessment and securing a SCA-V as soon as possible. Waiting until 6 months out may reduce the pool of bidders due to already being booked up.

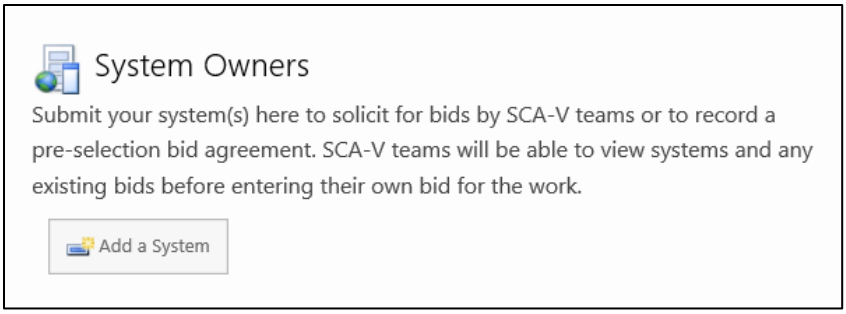
The Bid Tracker can be accessed via NETCOM's RMF Portal (see Figure 22). Upon entering the site look for the Bid Tracker.

Figure 22. NETCOM's RMF portal.



Click on ADD A SYSTEM (see Figure 23), and enter all required information

Figure 23. Validation bids.



NOTE: If you already have a SCA-V in mind and want to reach out to them directly, you can bypass the bid process through the Bid Tracker. If you choose this route, you must still go into Bid Tracker and ADD A SYSTEM. There will be a section where you can click that you have already obtained a SCA-V and DO NOT need any subsequent bids.

5.2.3 SCA-V preparation

No later than 20 working days before the onsite assessment, the Test Results should be completed and all controls submitted to the SCA-V in eMASS

Approximately 20-30 days in advance of the assessment, the team lead for the SCA-V will host a Technical Readiness Review (TRR) with the *SO* or designated point of contact (POC).

The TRR addresses the readiness to proceed with the validation, gather logistics (i.e., SMO Code,* physical address, etc…)

The TRR permits time to ensure that questions related to the validation have been addressed.

Updated Scans (SCAP, ACAS/NESSUS) should be run and loaded into the eMASS artifacts section.

5.2.4 Submitting the control set to the SCA-V

Before the SCA-V comes to perform the onsite assessment, the controls must be pushed to them in eMASS. This usually happens about 30 days before the onsite assessment or at the time of the TRR.

To push the controls for review:

Click on the CONTROLS tab

Under LISTING tab click on BULK Processing

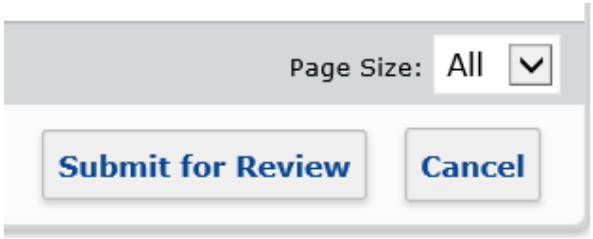
Click on SUBMIT FOR REVIEW tab (see Figure 24)

* Sample Management Office (SMO)

Just for fun click RESET (next to filter) to ensure that all filters are removed

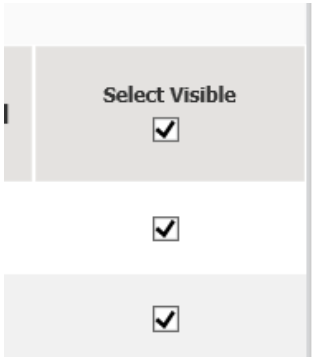
Scale to the bottom and ensure that page size is set to ALL.

Figure 24. Submit for review screenshot.



Go back to the top and click SELECT Visible (see Figure 25), to select ALL of the controls.

Figure 25. Select visible controls.



Scale to the bottom and click SUBMIT FOR REVIEW button.

At this point the controls are in the hands of the SCA-V. You should not be adding any more Test Results until the SCA-V releases the controls back to you after they populate the risk assessment.

5.2.5 SCA-V onsite assessment

First day onsite, a formal In-Brief will occur to address what to expect during the assessment.

Ensure that all appropriate personnel are available for the assessment (*SA*, *SO*, *ISSM*)

Ensure that physical access to all systems and components within the boundary are accessible

A daily informal hot-wash to review any significant events of the day and/or address any necessary schedule adjustments.

On the final day of the assessment, an Out-Brief will be presented to any/all stakeholders onsite to address preliminary observations identified during the effort.

5.2.6 How the SCA-V validates the controls/ CCIs

To be found compliant, each security control must be:

Known: Personnel are aware of the requirement and internal processes to meet that requirement.

Documented: Information and processes are recorded, kept up to date, and are readily available to allow for consistent application.

Implemented: Validation confirms the known and documented process are the same and consistently applied across the environment.

Technical Validation Methods. Note than many of these apply only to the standard IT components of a control system and will not be applicable to the actual controllers (Architecture level 2 or below) where other means (e.g., as-built submittals from construction) will need to be used instead.

Automated and manual testing will be conducted on hosts and devices using approved automated tools (i.e., SCAP, ACAS/NESSUS, etc…)

Manual STIG reviews

Manual data collection and subsequent data analysis.

Non-Technical Validation Methods

Data collection

Test scenarios

Personnel interviews

Physical inspection

Observation

Documentation (Artifacts) reviews

May take place before, during and after onsite assessment

5.2.7 SCA-V post assessment

The SCA-V has 30 working days to submit final deliverables to NETCOM via eMASS. Generally, the findings and risk matrix will be loaded in the artifact section of eMASS.

All controls/CCIs will become Compliant Official, Non-Compliant Official or Not Applicable Official. (CO, NCO, NAO)

The risk assessment will reveal all Non-Compliant controls to be used by the system personnel for POAM development.

5.3 Deliverables

Out-brief

Security Assessment Report (SAR): shows the status of the package at the time the assessment is complete.

SCA-V Recommendation Memorandum

Risk Assessment Workbook: See the Risk Assessment section in eMASS

Any Technical Data collected and analyzed during the assessment

6 RMF Step 5: Authorize System

At this point the SCA-V has completed their assessment and your system is ready to begin the Authorization process. This chapter describes how to submit to get the ATO for the system.

6.1 Risk assessment

The SCA-V will populate the risk assessment tab in eMASS. The risk assessment will detail all of the findings by the SCA-V, particularly the non-compliant ones. The non-compliant controls will be detailed at the control level, meaning there may be one or more CCIs that were deemed non-compliant, however it is only represented at the control level in the risk assessment section. Each finding will reveal the severity, relevance of threat, likelihood, impact and residual risk. The SCA-V will detail the finding in the vulnerability summary and then provide a recommendation under the recommendation column. Oftentimes the SCA-V will list each CCI that failed for each control in the vulnerability summary. To view log into eMASS:

Under the CONTROLS tab click on RISK ASSESSMENT

Use the FILTER to select only the NON-COMPLIANT controls

These findings will become the basis of your POAM, a key artifact informing the AO how and when the open risks will be made compliant

6.2 Plan of Action and Milestones (POAM) development

If there are any Not Applicable or Non-Compliant controls then you must complete and submit a POAM during the package submission step. The systems *ISSM*/O or *SO* will complete the POAM.

The POAM will list all of the Not Applicable and Non-Compliant controls. The Not Applicable controls will be automatically added by eMASS. Generally you will create a POAM entry for each Non-Compliant control in the Risk Assessment, however, some Commands may have you create an entry down to the CCI level.

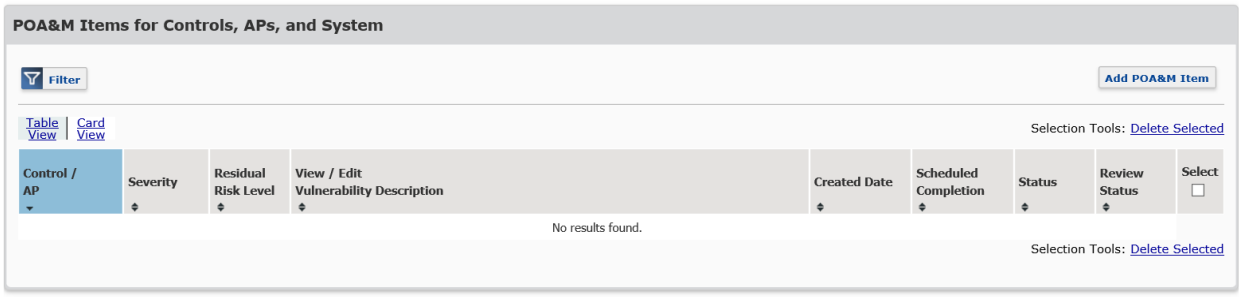
To add a POAM item for a Non-Compliant control:

If possible, open a second instance of your eMASS record and click on the CONTROLS tab, then select the RISK ASSESSMENT tab. This will allow you to see all of the non-compliant controls identified by the SCA-V (at the control level).

In eMASS click on the POAM tab

Under POA&M ITEMS FOR CONTROLS, APs, and SYSTEM (see Figure 26), Click ADD POA&M Item

Figure 26. POAM items for controls, SPs, and system.



Click on EDIT ASSOCIATION

Look at the RISK ASSESSMENT results and find the first non-compliant control

For example use AU-1

In the Search Box type in AU-1

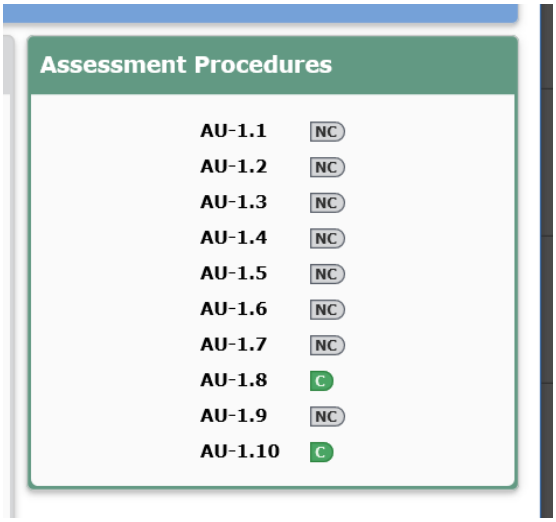
Here you need to know which APs were non-compliant. (APs have a corresponding CCI #)

To identify the non-compliant APs go to the second instance of eMASS where you see the RISK ASSESSMENT.

Under the CONTROL ACRONYM column, click on the first non-compliant control.

Under ASSESSMENT PROCEDURES (see Figure 27) you will find each AP that was non-compliant.

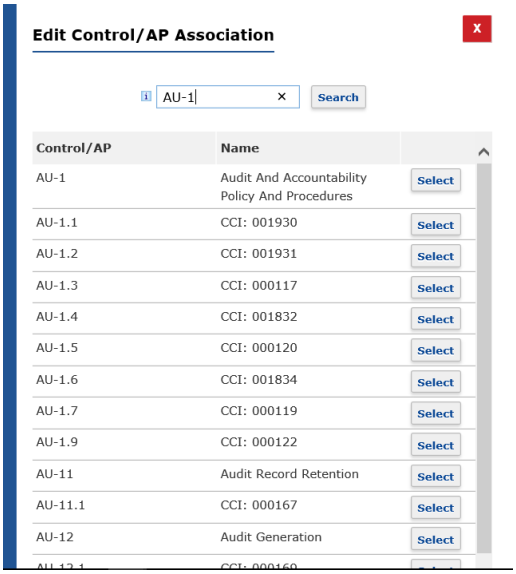
Figure 27. Assessment procedures.



Go back to the POAM instance of eMASS and select all of the non-compliant APs in the EDIT CONTROL/AP ASSOCIATION

In this example (Figure 28), you would select AU-1.1, AU-1.2, AU-1.3, AU-1.4, AU-1.5, AU-1.6, AU-1.7, AU-1.9.

Figure 28. Edit control/AP association.



Now your new POAM entry is associated to a non-compliant control.

Populate all of the * required fields

If the control has been made COMPLIANT, select COMPLIANT. Otherwise choose ONGOING or RISK ACCEPTED.

The VULNERABILITY DESCRIPTION can be copied and pasted from the Risk Assessment page.

SOURCE IDENTIFYING VULNERABILITY

Could be from the SCA-V assessment, Monthly/Quarterly Scans, or whatever.

SCHEDULED COMPLETION DATE will be the date it was made compliant or a future date.

Enter a description of how/when it will be completed, or justification for Risk Acceptance.

You will REPEAT this process for each entry in the Risk Assessment page.

NOTE: For each POAM item you made COMPLIANT, go back to the CONTROLS page, find the Control/AP and add a new TEST RESULT changing it to COMPLIANT with the supporting artifact or comment for verification. It will now show up as COMPLIANT UNOFFICIAL (CUO).

6.3 Control status update

For every POAM item where you listed the entry as COMPLIANT, you must go back to the CONTROLS page and mark the Control/AP compliant.

Click on the CONTROLS Tab

Find the CONTROL (e.g., AU-1)

Click the + sign to show all of the APs under AU-1

Find the AP(s) that are NC that you made COMPLIANT and enter a new TEST RESULT for each one.

Make sure you insert the correct comments on how the Control/AP has been made compliant.

Select the Values for SEVERITY, RELEVANCE of THREAT, and IMPACT as seen in the risk assessment. (Likelihood and Residual will auto-populate)

Follow these procedures for any new POAM entry that you make Compliant, or any control that has become Non-Compliant.

6.4 Package submission for Assess and Authorize (A&A)

Before submitting your package for an ATO, ensure that the following are complete:

A POAM entry for every Non-Compliant, Risk Accepted, and Not Applicable

All POAM items made Compliant are updated in the CONTROLS page.

To submit the package for ATO:

Click on the PACKAGE tab (do not choose the drop down choices)

Click on ASSESS AND AUTHORIZE

Enter the Package Name (e.g., YOUR SYSTEM NAME-Assess and Authorize)

Enter any Comments

Click INITIATE WORKFLOW

6.5 Package approval chain (PAC)

The Package Approval Chain reveals the roles that the package will go through for approval or rejection on its way to the AO. Remember, most likely you are in the *ISO*/ PM role or the Organizational *ISSM* role.

If you submitted the Package as the ISO/PM, you will have to go back in and then APPROVE and forward the Package to the Organizational ISSM.

Each subsequent role will review the package for completeness and accuracy. If there are any issues, the reviewer may approve or reject the package. If the package is rejected, it will be sent back to the previous PAC for them to correct or reject back to the beginning.

For the Army, the PAC and expected duration for review/approval at each step are as follows:

ISO/PM- 1 day

Organizational ISSM- 5 days

Program ISSM- 5 days

SCA-R)- 9 days

SCA-A- 5 days

AO- 5 days

The expected duration for package review and approval is predicated on the package not being returned for rework. Even if the package is perfect, schedules, workloads and other factors can extend these review timeframes and oftentimes do.

For the Army, NETCOM operates in the SCA-R and SCA-A role. Once your package is approved and recommendation made, it is sent to the AO.

6.6 Authorization decision

After you submit your package, the approvals at each PAC can be tracked as follows:

Hover over the PACKAGE tab and select PACKAGE STATUS

If you do not see anything this could be good, or could be a problem:

Hover over the PACKAGE tab and select HISTORICAL PACKAGE LISTING

You will either see that the Assess and Authorize submission was RETURNED for Rework or that an ATO was granted.

If the ATO was granted click on the VIEW button under the word ACTION

You will see the AO's comments about the ATO.

If the package was returned, click on the VIEW button to see why. Make all corrections and resubmit.

Hopefully your package does not receive the dreaded Denial of Authority to Operate (DATO). If so, follow the instructions and make the necessary corrections in the DATA comments section.

Look in the ARTIFACTS tab. The ATO Decision Document should be uploaded.

7 RMF Step 6: Monitor Security Controls

RMF brought us more than just 4 times the number of controls to assess compared to previous assessment requirements, it brought us the concept of continuous monitoring. The goal is for a system to continually assess the security safeguards in place to better protect the systems. Your ATO can be in jeopardy if you do not perform the activities in the Recurring Activities section below.

7.1 Impact changes to the system and environment

Your system accreditation was a snapshot in time. Most likely the next day something changed. Either a new patch came out or you may have changed or added a component. These types of things can impact the security of the system:

New workstation, laptop, or database not originally assessed in the accreditation

New components introduced into the system not originally assessed in the accreditation

Field Controllers

Field Point of Connection (FPOC)

Switches/Routers

Control System Application

Wireless Communication

Connecting to another network or system

Integration of a critical facility

Operating System (OS) upgrade

Removal of a boundary fence

All of the above can have impacts on the security of the system. The changes do not necessarily mean that the system must undergo another accreditation, however, they must be looked at to determine if there is a significant impact to the system. This is where your Configuration Management Plan comes into play.

7.2 Recurring activities

The AO, and Program ISSM will be looking at recurring activities to ensure that the system is being maintained and monitored appropriately. Until the

DoD defines the SLCM, it is up to you to implement the topics below for your AO to be confident in continuing to accept the risk of your system(s).

7.2.1 Scans

Earlier in this document SCAP and ACAS were discussed. One or more of your controls addressed the scanning of your system. In that control you defined the frequency to which you will perform various scanning and remediation of findings to your system. For continuous monitoring, you will upload the scan results into eMASS. From these scans, eMASS will populate findings and create an Actions list. Any findings will need to be converted to a POAM entry.

How to import a scan:

Click on the ASSETS tab
Click on IMPORT SCAN
Select Scan Type
ACAS: ASR/ARF
ACAS: NESSUS
DISA STIG Viewer: CKL
DISA STIG Viewer: CMRS
eEye Retina
Policy Auditor
SCAP Compliance Checker
Then click on IMPORT

7.2.2 Assess selected controls annually

FISMA requires the following to be reported annually and the controls associated with the following could be set to an annual basis.

Contingency Plan Test
Security Control Test
Subset of controls each year
Security Review
Baseline control set

7.2.3 Conduct remediations

Any findings through the reviews or periodic scans will need to be entered in the POAM and remediated to seek Risk Acceptance from the AO. Remediations for some findings cannot be applied, in doing so, the system or component may not function properly. Keep a deviations list and load into the Artifacts section of eMASS.

7.2.4 Update eMASS

The Program *ISSM* and AO have the ability to monitor the systems eMASS entry. If they do not see any activity in eMASS, they can issue a DATO. Therefore it is important to update eMASS with scans, POAM findings and fixes, and updates to any of the policies and procedures associated with the system.

7.2.5 POAM update submission

There will be a defined frequency to which the POAM must be reviewed. Upon uploading new scans into the ASSETS tab, you create the POAM entries for each finding.

Depending on the frequency defined, you must submit your POAM to the AO for approval. To do this perform the following:

Click on the PACKAGE tab

Click on the POAM Approval

Complete the appropriate * Required Items

Click on INITIATE WORKFLOW

***__NOTE__: Every ATO granted has an Authorization Termination Date (ATD). This is the date by which you should have your new ATO granted. RMF allows the AO the option to extend an ATO at the time of the ATD up to one year. Some may allow this and some may not. If you have any hopes of getting an ATO extension without having to go through another SCA-V assessment, ensure that your system remains in a secure state and eMASS is kept up to date.

7.3 Decommission the system

IT systems normally have a limited life span due to the rapid changes in technology. A control system may last for 15 years or more. When a *SO* determines they no longer want to maintain a system or the systems purpose is no longer needed, the system owner will decommission the system.

In section 1.2 and 1.3 you created an APMS record and an eMASS record. The SO will need to follow the procedures for decommissioning the system prescribed by APMS

Once you have deleted the system in the respective databases begin the turn in process of the decommissioned components.

8 Assess-Only

NETCOM has established a TTP for the Assess-Only process. To access the Assess-Only TTP, see steps listed in section 3.6.1 to access NETCOM's operations page. Instead of clicking on the SCA-V TTP find and click on the NETCOM RMF ASSESS-ONLY TTP.

When the Assess-Only process was released, it was widely thought that Closed Restricted Networks (CRN) and standalone systems could bypass RMF. This is not the case.

Per the TTP, "The purpose of this TTP document is to provide operational procedures for approving Army IT that DOES NOT rise to the level of an IS."

Platform IT () that does not rise to the level of a system is also known as "IT below the system level." The Assess-Only process applies to IT below the system level. Per the TTP, "IT below the system level is assessed for the purpose of being accepted and connected into an existing computing environment (i.e., an IS or system with an authorization)." In essence, the Assess-Only process allows for the inclusion of IT below the system level with an existing FRCS that already has an ATO.

The TTP depicts an Assess-Only determination process (see Figure 29) to help determine if a new eMASS record should be created or if the items to be assessed should be reflected in an existing eMASS record.

It would be very difficult to teach Assess-Only in the same manner as was done in this document for general RMF. Therefore, it is imperative that you read the entire TTP. Appendix E within the TTP establishes a process (Assess-Only Triage) in which a *ISO* can submit a request to determine if qualifies under the Assess-Only process or if the full Assess and Authorize must take place.

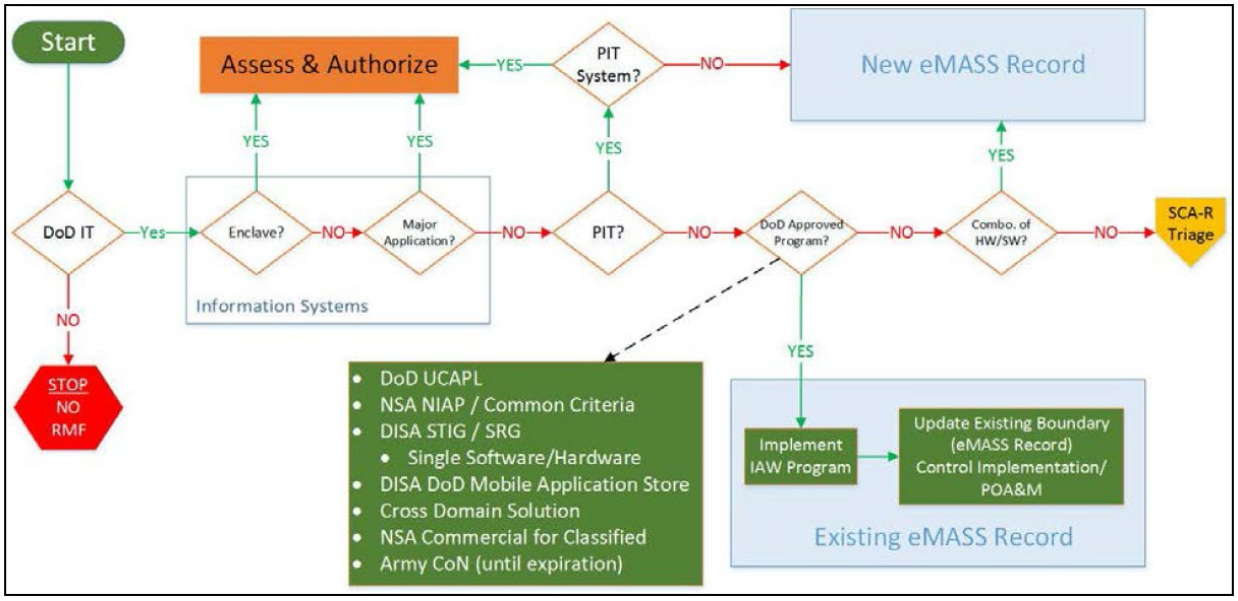
If it has been determined that you can use the Assess-Only process for a particular to be used, what does that gain you?

Uses the *SCA-O* role, which will replace the SCA-A, *SCA-R)*, and SCA-V.

A reduced set of controls to assess.

No APMS requirement

Figure 29. Assess-Only determination process.



In essence, the Assess-Only bypasses the requirement to use a SCA-V and the package does not go through NETCOM for approval. RMF still applies, however, it is somewhat a reduced process.

In issue to overcome would be the appointment of the SCA-O role. This appointment is made at the command level. The SCA-O must be qualified to perform the roles of the SCA-A, SCA-R, and SCA-V.

Another consideration is to know when to simply use the CMP for your system to add a component already accredited in your system, or to use the Assess-Only process.

9 Standards and Criteria

The inclusion of cybersecurity in the design and construction process is addressed in UFC 4-010-06 and in UFGS 25 05 11. The scope of these documents are specific to addressing controls that can be covered by designers and installers, and therefore help meet cybersecurity requirements but are not themselves a full RMF solution for control systems.

Appendix A:- RMF Checklist

This checklist can provide the *SO* and *ISSM*s for any system a solid foundation for tracking tasks to be completed through the RMF process. This list is *NOT all inclusive* and should be viewed as a living document to be tailored as new requirements may arise.

Cybersecurity Requirements	To Be Completed By	Determination
Register System APMS		
Register System eMASS		
Categorize System (in eMASS)		
Secure SCA-V (Bid Tracker or direct)		
Develop/Acquire Tenant Security Plan (to include Inheritable Controls) (If Applicable)		
Develop/Acquire Service Level Agreement (to include Inheritable Controls) (If Applicable)		
eMASS Determine/Assign Roles (*ISO/* PM, CAC, AO, SCA-V, Org ISSM, etc…)		
eMASS Account-Information System Owner (ISO)		
eMASS Account-Information System Security Manager *(ISSM*)		
eMASS Account/Access for Contractor		
eMASS Package Approval Chain-Assign as group *SCA-R)* (For Army Systems)		
eMASS Package Approval Chain-Assign as group SCA-A (For Army Systems)		
System Design	To Be Completed By	Determination
Acquire IA Training for IA Personnel		
Appoint ISO		
Appoint ISSM		
Appoint ISSO		
Determine *Authorizing Official* (AO)		
Determine Configuration Control Board (CCB) Members		
Determine if Standalone, Closed Restricted Network (CRN) or Networked		
Determine Program ISSM (in eMASS)		
Develop Acceptable Use Policy (AUP)		
Develop Authorized Users List		
Develop CCB Charter and Change Request Form		
Develop Contingency Plan		
Develop COOP Plan		

Cybersecurity Requirements	To Be Completed By	Determination
Develop Data Flow Diagram		
Develop Group Account Tracking List		
Develop HBSS Waiver (If applicable)		
Develop HW List		
Develop Incident Response Plan		
Develop Network Diagram		
Develop Physical Access List		
Develop PKI Waiver (If applicable)		
Develop Policies and Procedures for Access Control AC		
Develop Policies and Procedures for Audit and Accountability (AU)		
Develop Policies and Procedures for Awareness and Training (AT)		
Develop Policies and Procedures for Configuration Management (CM)		
Develop Policies and Procedures for Contingency Planning (CP)		
Develop Policies and Procedures for Identification and Authentication (IA)		
Develop Policies and Procedures for Incident Response (IR)		
Develop Policies and Procedures for Maintenance (MA)		
Develop Policies and Procedures for Media Protection (MP)		
Develop Policies and Procedures for Personnel Security (PS)		
Develop Policies and Procedures for Physical and Environmental Protection (PE)		
Develop Policies and Procedures for Planning (PL)		
Develop Policies and Procedures for Program Management		
Develop Policies and Procedures for Risk Assessment (RA)		
Develop Policies and Procedures for Security Assessment and Authorization (CA)		
Develop Policies and Procedures for System and Communications Protection (SC)		
Develop Policies and Procedures for System and Information Integrity (SI)		
Develop Policies and Procedures for System and Services Acquisition		

Cybersecurity Requirements	To Be Completed By	Determination
Develop Port Protocols and Services (PPP) Determination/Registration		
Develop Privacy Impact Assessment (PIA) DD 2930		
Develop SW List		
Document CCB Minutes		
Test Contingency Plan		
Select Security Controls	To Be Completed By	Determination
Determine Control Set		
Determine Supplemental Controls/Overlay		
Populate Implementation Plan (in eMASS)		
Develop System-Level Continuous Monitoring Strategy (in eMASS)		
Finalize Control Set		
Submit System Security Plan for approval in eMASS		
Implement Security Controls	To Be Completed By	Determination
Apply appropriate STIGs to system		
Obtain Licensing for ACAS Server		
Develop STIG deviations List		
Scan/Fix Process		
Upload system documentation to eMASS		
Address Controls/ CCIs and Tie to Artifacts		
Assess Security Controls/Third Party Validator	To Be Completed By	Determination
Develop Security Assessment Plan		
Push Controls to SCA-V in eMASS		
Prepare site for Validation team		
Host Validation Team		
Provide SMO Code and Site Security POC to SCA-V		
Upload Scans/Checklists in eMASS 30 days before SCA-V		
Collaborate with Validation team to receive results from validation scan		
Apply any necessary Scan/Fixes resulting from Validation Team		
Prepare system POA&M		
Upload/Populate POA&M into eMASS		
Prepare any final system documentation		
Apply any necessary Scan/Fixes resulting from Validation Team		

Cybersecurity Requirements	To Be Completed By	Determination
Submit RMF Package for Assess and Authorize in eMASS		
Authorize System	To Be Completed By	Determination
Receive Decision from AO		
Authority to Connect Process	To Be Completed By	Determination
Request ATC		

Appendix B: Five-Level FRCS Architecture

Source: Appendix E to UFC 4-010-06 19, *Cybersecurity of Facility Related Control Systems* (NFEC 2017).

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

APPENDIX E 5-LEVEL CONTROL SYSTEM ARCHITECTURE

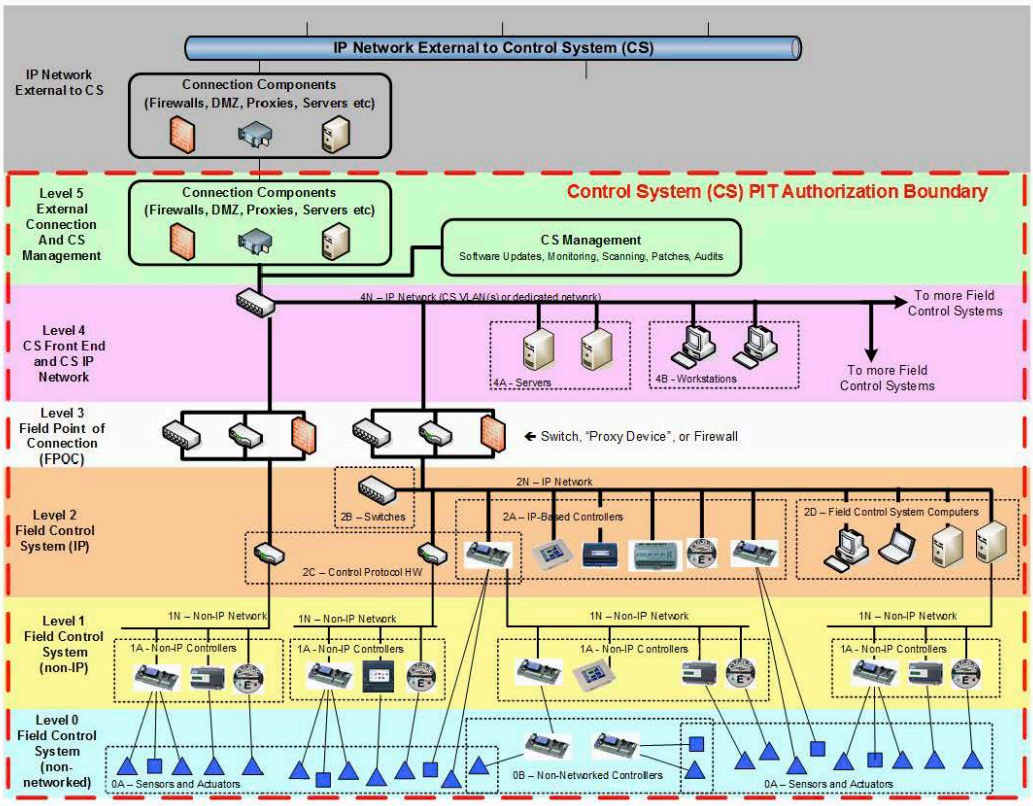
E-1 INTRODUCTION

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.

Bibliography

DoD (U.S. Department of Defense). 2017. DODI 8510.01. Subject: Risk Management Framework (RMF) for DoD Information Technology (IT). Washington, DC: DoD.

———. 2014. DODI 8500.01. Subject: Cybersecurity. Washington, DC: DoD.

NFEC (Naval Facilities Engineering Command). 2017. *Cybersecurity of Facility Related Control Systems*. Unified Facilities Criteria (UFC) 4-010-06 19. Washington, DC: U.S. Army Corps of Engineers (USACE), NFEC (Preparing Activity), Air Force Civil Engineer Center (AFCEC), https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf

NIST (National Institute of Standards and Technology). 2015. *Guide to Industrial Control Systems (*ICS*) Security*. NIST SP 800-82, Rev. 2, Washington, DC: U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

———. 2014. *Assessing Security and Privacy Controls in Federal In-formation Systems and Organizations*. NIST Special Publication (SP) 800-53A. Washington, DC: U.S. Department of Commerce, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

———. 2008. *Volume II: Appendices to Guide for Mapping Types of Information and Information System to Security Categories*. NIST SP 800-60, Vol. 2, Rev. 1. Washington, DC: U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Acronyms and Abbreviations

Term	Definition
A&A	Assess and Authorize
AC	Access Control
ACAS	Assured Compliance Assessment Solution
ACOM	Army Command
ADCCP	Army Data Center Consolidation Plan
AGM	Army Gold Master
ANSI	American National Standards Institute
AO	Authorizing Official
AP	Assessment Procedure
APL	Approved Products List
APMS	Army Portfolio Management Solution
ARF	Assessment Results Format
ASR	Assess Summary Reporting
AT	Awareness and Training
ATC	Authority to Connect
ATD	Advanced Technology Demonstration
ATO	Authority To Operate
AU	Audit and Accountability
AUP	Acceptable Use Policy
BCS	Building Control System
BPOC	Building Point Of Common connection
CA	Security Assessment and Authorization
CAC	Common Access Card
CCB	Configuration Control Board
CCI	Control Correlation Identifier
CCP	Common Control Provider
CD	Cyber Development
CDS	Cross Domain Solution
CERL	Construction Engineering Research Laboratory
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CM	Configuration Management

Term	Definition
CMP	Change Management Process
CMRS	Continuous Monitoring and Risk Scoring
CNSSI	Committee on National Security Systems Instructions
CO	Compliant Official
COOP	Continuity of Operation Plan
CP	Contingency Planning
CRAC	Computer Room Air-Conditioning
CRN	Closed Restricted Network
CS	Control System
CSC-MCX	Control System Cybersecurity Mandatory Center of Expertise
CUO	Compliant Unofficial
DATO	Denial of Authority to Operate
DBS	Defense Business System
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITPR	DoD IT Portfolio Repository
DoD	U.S. Department of Defense
DoDI	Department of Defense Instruction
DPW	Directorate of Public Works
DX	Direct Expansion
EDS	Electrical Distribution System
EI&E	Energy, Installations and Environment
ERDC	U.S. Army Engineer Research and Development Center
ERDC-CERL	Engineer Research and Development Center, Construction Engineering Research Laboratory
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FL	Functional Lead
FOUO	For Official Use Only
FPOC	Field Point of Connection
FRCS	Facility Related Control System
HBSS	Host Bases Security System
HQ-IMCOM	Headquarters, Installation Management Command
HVAC	Heating, Ventilating, and Air-Conditioning

Term	Definition
HW	Hardware
IA	Identification and Authentication
IASE	Information Assurance Support Environment
IATT	Interim Authorization to Test
ICAN	Installation Campus Area Network
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ID	Identification
IE&E	Installations, Energy and Environment
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMCOM	U.S. Army Installation Management Command
IP	Internet Protocol
IR	Incident Response
IRP	Incident Response Plan
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISO/PM	Information System Owner or Program Manager
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITTP	Installation Technology Transition Program
MA	Maintenance
MACOM	Major Army Command
MMH	Moderate Confidentiality, Moderate Integrity, and High Availability Impact
MP	Media Protection
N/A	Not Applicable
NA	Not Applicable
NAO	Not Applicable Official
NCO	Not Compliant Official
NEC	Network Enterprise Center
NETCOM	U.S. Army Network Enterprise Technology Command
NIPRNET	Non-Secure Internet Protocol Router Network

Term	Definition
NIST	National Institute of Standards and Technology
NSN	National Supply Number
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OPSEC	Operations Security
OS	operating system
PAC	Package Approval Chain
PDF	Portable Document Format
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
	Platform Information Technology
PKI	Public Key Infrastructure
PL	Planning
PLC	Programmable Logic Controller
PM	Program Manager
POAM	Plan of Action and Milestones
POC	Point of Contact
PPBBOS	Programming and Budgeting Business Operating System
PPP	Public Private Partnership
PPSM	Ports Protocol and Services Management
PS	Personnel Security
RA	Risk Assessment
RMF	Risk Management Framework
RNEC	Redstone Arsenal Network Enterprise Center
SA	System Administrator
SAP	Security Assessment Plan
SAR	Security Assessment Radar
SC	System and Communication Protection
SCA	Security Control Assessor
SCA-A	Security Control Assessor-Army
SCADA	Supervisory Control and Data Acquisition
SCA-O	Security Control Assessor-Organization
SCAP	Secure Content Automation Protocol

Term	Definition
SCA-R	Security Control Assessor-Representative
SCA-V	Security Control Assessor-Validator
SCC	SCAP Compliance Checker
SF	Standard Form
SI	System and Information Integrity
SLA	Service Level Agreement
SLCM	System-Level Continuous Monitoring
SLCMS	System-Level Continuous Monitoring Plan
SMO	Sample Management Office
SO	System Owner
SOP	Standing Operating Procedure
SP	Special Publication
SQL	Structured Query Language
SRG	Security Requirements Guide
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SW	Software
TBD	To Be Determined
TR	Technical Report
TRR	Technical Readiness Review
TTP	Tactics, Techniques, and Procedures
UCS	Utility Control System
UFC	Unified Facilities Criteria
UFGS	Unified Facilities Guide Specification
UMCS	Utility Monitoring and Control System
UMCS-DL	Disney Land Utility Monitoring and Control System
USACE	U.S. Army Corps of Engineers
USAG	U.S. Army Garrison
USCYBERCOM	United States Cyber Command
WBDG	Whole Building Design Guide

Index

REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
10/01/2019	Final Technical Report (TR)	

4. TITLE AND SUBTITLE

An Army Guide to Navigating the Cyber Security Process for Facility Related Control Systems: Cybersecurity and Risk Management Framework explanations for the Real World

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT

6. AUTHOR(S)

Michael Cary Long, Joseph Bush, Stephen Briggs, Tapan Patel, Eileen Westervelt, Daniel Shepard, Eric Lynch, and David Schwenk

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Engineer Research and Development Center (ERDC)
Construction Engineering Research Laboratory (CERL)
PO Box 9005,
Champaign, IL 61826-9005

8. PERFORMING ORGANIZATION REPORT NUMBER

ERDC/CERL SR-19-5

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Headquarters, U.S. Army Corps of Engineers (HQUSACE)
441 G St., NW
Washington, DC 20314

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

This work was reimbursably funded under the HQUSACE Standards and Criteria Program, via Military Interdepartmental Purchase Request (MIPR) 11268080, "A1040-FY19 TSG [Tech-nology Standards Group] Oversight of ITTP."

14. ABSTRACT

Personnel who maintain Facility Related Control Systems (FRCS) of any type are required to implement cybersecurity to attain and maintain an Authority to Operate (ATO) on their respective systems. This document is a guide for installation personnel owning and operating control systems to assist in addressing the cybersecurity process for FRCS in the Army through the Risk Management Framework (RMF) approach, which encompasses six steps. This manual walks the reader through the administrative aspects of each step.

15. SUBJECT TERMS

Computer security, Cyberspace--Security measures, Facility management, Military bases--Risk management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (include area code)
Unclassified	Unclassified	Unclassified	SAR	118	