****
USACE / NAVFAC / AFCEC / NASA **UFGS-25 08 11.00 20 (November 2020)**

Preparing Activity: NAVFAC

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated July 2021
****

SECTION TABLE OF CONTENTS

DIVISION 25 - INTEGRATED AUTOMATION

SECTION 25 08 11.00 20

RISK MANAGEMENT FRAMEWORK FOR FACILITY-RELATED CONTROL SYSTEMS

11/20

-- End of Section Table of Contents --

****
USACE / NAVFAC / AFCEC / NASA **UFGS-25 08 11.00 20 (November 2020)**

Preparing Activity: NAVFAC

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated July 2021
****

SECTION 25 08 11.00 20

RISK MANAGEMENT FRAMEWORK FOR FACILITY-RELATED CONTROL SYSTEMS
11/20

****
NOTE: This guide specification covers the Navy requirements to support the Risk Management Framework (RMF) Authority to Operate (ATO) Process for Facility-Related Control Systems.

Adhere to UFC 1-300-02 Unified Facilities Guide Specifications (UFGS) Format Standard when editing this guide specification or preparing new project specification sections. Edit this guide specification for project specific requirements by adding, deleting, or revising text. For bracketed items, choose applicable item(s) or insert appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be submitted as a Criteria Change Request (CCR).

To download UFGS Forms, Graphics, and Tables, go to: http://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/forms-graphics-tables
****

****
Note: Facility-Related Control Systems (FRCS) are a subset of control systems that are used to monitor and control equipment and systems related to DoD real property facilities (e.g., building control systems, utility control systems, electronic security systems). This section includes Risk Management Framework (RMF) requirements to be included on DOD projects which has a facility-related control system requiring an Authority To Operate (ATO). This Section does not provide general requirements for a control system,

nor are the requirements in this section sufficient to procure a control system. This section also does not repeat requirements from UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS or other technical sections.

The use of UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS does not necessarily make this specification applicable.

Only use this specification on control systems which are obtaining a new ATO.

If an installation obtained a J&A to procure specific equipment based on an existing authorization, this specification is not needed. Instead include the make/model of equipment referenced in the J&A on the plans and include configuration settings into the technical specifications to match the existing authorization. Where equipment is procured and configured to match an existing authorization, a memo for the record (MFR) to the existing authorization is needed ILO performing a new authorization.

Refer to UFC 4-010-06, "Cybersecurity for Facility-Related Control Systems" for requirements on incorporating cybersecurity into control system design and for general information on the RMF process as it applies to control systems. Assistance for control system cybersecurity is available from the following Service organizations:

Navy: Naval Facilities Engineering Command, Command Information Office (CIO)

Marine Corps: Contact Navy POC for Marine Corps POC information

Many designer selections in this Section will require coordination with the project site, System Owner, Information System Security Manager (ISSM), Authorizing Official (AO) or a subject matter expert in the specific control systems being installed.

****

PART 1 GENERAL

This specification includes the contract requirements to to support the Government in obtaining an Authority To Operate (ATO) following the Department of Defense Risk Management Framework process.

This Section does not provide technical requirements for a control system, nor are the requirements in this section sufficient to procure a control system. This section must be used in conjunction with other technical control system specifications and UFGS 25 05 11 CYBERSECURITY FOR FACILITY RELATED CONTROL SYSTEMS.

1.1 CONTROL SYSTEM APPLICABILITY

****

NOTE: List each control system requiring an authorization and the corresponding impact rating categorization (Confidentiality-Integrity-Availability) of Low, Moderate, or High. Typical systems to consider are utility monitoring control systems, building control systems, lighting control systems, UPS control systems, generator control systems, and SCADA systems.

****

This section applies to the following control systems:

a. [Building DDC System] [_____] with a categorization of [Low-Low-Low] [Moderate-Moderate-Moderate] [_____].

[b. [_____] Control System with a categorization of [Low-Low-Low] [Moderate-Moderate-Moderate] [_____].

][c. [_____] Control System with a categorization of [Low-Low-Low] [Moderate-Moderate-Moderate] [_____].

]## 1.2 RELATED REQUIREMENTS

All Sections containing facility-related control systems (FRCS) or control system components as identified in paragraph CONTROL SYSTEM APPLICABILITY are related to the requirements of this Section. Review all specification sections to determine related requirements.

1.3 REFERENCES

****

NOTE: This paragraph is used to list the publications cited in the text of the guide specification. The publications are referred to in the text by basic designation only and listed in this paragraph by organization, designation, date, and title.

Use the Reference Wizard's Check Reference feature when you add a Reference Identifier (RID) outside of the Section's Reference Article to automatically place the reference in the Reference Article. Also use the Reference Wizard's Check Reference feature to update the issue dates.

References not used in the text will automatically be deleted from this section of the project specification when you choose to reconcile references in the publish print process.

****

The publications listed below form a part of this specification to the extent referenced. The publications are referred to within the text by the basic designation only.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

NIST FIPS 201-2	(2013) Personal Identity Verification (PIV) of Federal Employees and Contractors
NIST SP 800-82	(2015; Rev 2) Guide to Industrial Control Systems (ICS) Security

U.S. DEPARTMENT OF DEFENSE (DOD)

DOD 8510.01	(2020; Change 1-2020) Risk Management Framework (RMF) for DoD Information Technology (IT)
DODI 8551.01	(2014) Ports, Protocols, and Services Management (PPSM)

1.4 DEFINITIONS

1.4.1 Assured Compliance Assessment Solution (ACAS) Scans

Automated vulnerability scanning and risk assessment tool mandated for use in DOD to identify security compliance and secure configuration of connected devices.

1.4.2 Authority To Operate (ATO)

The Authority granted by an organization's Authorizing Official (AO or FAO), which indicates the system has undergone the first five steps of the RMF process and has been assessed and deemed to be at an acceptable level of risk to allow connection to other Authorized systems, (any limitations to this connectivity will be documented within the RMF package). Retention of a system's Authorization status is contingent upon successful completion of all conditions as documented in the ATO package, as well as lifecycle compliance with Step 6 of the RMF; "Continuous Monitoring".

1.4.3 Control Correlation Identifier (CCI) or Security Control

Each Security Control is broken down into individual Assessment Procedures (AP's), to enable more granular assessment of the compliance status of a given control, (e.g. AC-1 is broken out into AC-1.1, AC-1.2, AC-1.3); each of these is assigned a CCI number and is individually assessed and tracked for compliance.

1.4.4 Enterprise Mission Assurance Support Service (eMASS)

A web-based application for the cybersecurity management of system information, which provides automated capabilities for documentation and tracking in support of Authorization within the Risk Management Framework Process.

1.4.5 Functional Authorizing Official (FAO) or Authorizing Official (AO)

Signature authority for granting an Authority to Operate (ATO) and the responsible individual for accepting risk imposed by the implementation and operation of systems in their AOR. The AO is exclusively accountable for organizational cybersecurity risk exposure corresponding to all IT under their cognizant authority. The AO makes an authorization decision based on all the artifacts related to the activities within the RMF

process and in accordance with the AO's cybersecurity risk tolerance. This risk tolerance accounts for the probability of a breach to confidentiality, integrity, and availability of information and the potential impact that breach would conceivably have.

1.4.6 Information System Owner (ISO) or System Owner (SO)

Has overall ownership of the system and is involved in the design, development, and cybersecurity implementation of the system, ensuring that the system is maintained and tracked throughout its lifecycle.

1.4.7 Information System Security Manager (ISSM)

Government-appointed Command Information Office Representative with overall responsibility for the cybersecurity of a program, organization, system, or enclave; and is accountable to the system Program Manager/Information System Owner. Often the ISSM/Information System Security Officer (ISSO) will delegate execution of tasks to other RMF team members, however accountability remains with the ISSM/ISSO. During sustainment, the ISSM/ISSO will be solely responsible and report to the PM/ISO. As their responsibilities are mandated by Department of Defense instruction, ISSM's are generally designated in writing by Senior Command Leadership (SYSCOM CIO, Base Commander)

1.4.8 Information System Security Engineer (ISSE)

The ISSE (contractor) is responsible for developing and maintaining the cybersecurity architecture of a program, organization, system, or enclave.

1.4.9 Risk Management Framework (RMF)

The process mandated by DOD 8510.01 for the management of cybersecurity risk across the DOD enterprise; the RMF leverages a risk-based approach for the formal Authorization of IT systems and services. The RMF implements and enforces a tailored set of security controls, focused on security as an integral part of a system’s overall lifecycle.

1.4.10 Security Assessment Plan (SAP)

A plan developed by the SCA / Validator which provides the specific test objectives for the security controls assessment, identifies the personnel, procedures and tools to be used, identifies any 'exceptions' to the plan, and documents 'false positives' [and][or] misleading reports discovered during testing.

1.4.11 Security Assessment Report (SAR)

A report produced by the SCA/Validator which documents the residual risk of the non-compliant security controls after the risk assessment work is completed. The SAR provides a summary of the vulnerabilities, interconnected systems, rationale for aggregated risk, and a recommendation to the FAO/AO regarding an Authorization decision.

1.4.12 Security Content Automation Protocol (SCAP)

An assessment methodology which leverages specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation of IT and computing systems. SCAP may be used to enumerate security-related software and configuration issues. SCAP scan data may

also be uploaded into a STIG viewer utility to assist in automating STIG checklist processing for those technologies that offer this functionality.

1.4.13 Security Control Accessor - Validator (SCA-V)

A Government-assigned independent third party which assesses and validates that the system has correctly implemented the approved security control baseline. To determine the overall effectiveness of the security controls, the SCA performs an independent, comprehensive assessment of the management, operational, and technical controls employed within or inherited by a system. To perform the SCA function in the most efficient manner, the Navy will utilize SCA Liaisons and Validators to assist with SCA responsibilities.

1.4.14 Security Plan (SP)

Includes essential operational, architectural, and functional information about the system. This plan is generated by eMASS from the information provided during eMASS registration process and is updated whenever pertinent information about the system is entered or changed. The SP is a living document which can be exported and downloaded in real time from eMASS.

1.4.15 Security Technical Implementation Guidance (STIG)

Standard security protocols and procedures that provide a methodology for secure configuration of computing, networking, software and control system assets. STIG checklists may be utilized as tools for determining compliance with a given set of security controls.

1.5 ADMINISTRATIVE REQUIREMENTS

1.5.1 Coordination

****

NOTE: This subpart deals with coordination requirements for the contractor, and does not indicate coordination that must be done by the designer/specifier. In addition to the normal project coordination, authorization for wireless use, alternate account lock permissions and devices with multiple IP connections may be impacted by site (or Service) policies and need to be coordinated with the appropriate Government representatives before authorization is provided.

****

Coordinate the execution of this Section with the execution of all other Sections related to control systems as indicated in the paragraph RELATED REQUIREMENTS.

1.6 SUBMITTALS

****

NOTE: Review Submittal Description (SD) definitions in Section 01 33 00 SUBMITTAL PROCEDURES and edit the following list, and corresponding submittal items in the text, to reflect only the submittals required for the project. The Guide Specification

technical editors have classified those items that require Government approval, due to their complexity or criticality, with a "G." Generally, other submittal items can be reviewed by the Contractor's Quality Control System. Only add a "G" to an item if the submittal is sufficiently important or complex in context of the project.

For Army projects, fill in the empty brackets following the "G" classification, with a code of up to three characters to indicate the approving authority. Codes for Army projects using the Resident Management System (RMS) are: "AE" for Architect-Engineer; "DO" for District Office (Engineering Division or other organization in the District Office); "AO" for Area Office; "RO" for Resident Office; and "PO" for Project Office. Codes following the "G" typically are not used for Navy, Air Force, and NASA projects.

The "S" classification indicates submittals required as proof of compliance for sustainability Guiding Principles Validation or Third Party Certification and as described in Section 01 33 00 SUBMITTAL PROCEDURES.

Choose the first bracketed item for Navy, Air Force, and NASA projects, or choose the second bracketed item for Army projects.
****

****
NOTE: All submittals in this Guide Specification require Government approval and must have a "G" designation.

Government review of submittals in this Section impact Cybersecurity, and must be coordinated with the appropriate Cybersecurity experts to ensure appropriate review and the identification of issues or concerns that may affect the cybersecurity posture of the system or the ability of the system to receive an RMF authorization. Cybersecurity Experts are in the following organizations:

Army: Control System Cybersecurity Center of Expertise, Huntsville Engineering and Support Center

Navy: Naval Facilities Engineering Command, Command Information Office (CIO)

Air Force: Civil Engineer Maintenance, Inspection, and Repair Team (CEMIRT) ICS Branch, Tyndall AFB

Marine Corps: Contact Navy POC for Marine Corps POC information
****

Government approval is required for submittals with a "G" or "S" classification. Submittals not having a "G" or "S" classification are [for Contractor Quality Control approval.][for information only. When used, a code following the "G" classification identifies the office that will review the submittal for the Government.] Submit the following in accordance with Section 01 33 00 SUBMITTAL PROCEDURES:

SD-01 Preconstruction Submittals

Authorization Strategy Plan; G[, [_____]]

SD-05 Design Data

Control System Security Controls; G[, [_____]]

Security Plan; G[, [_____]]

Ports, Protocols, And Services Management Registration Form; G[, [_____]]

SD-06 Test Reports

ACAS Vulnerability Reports; G[, [_____]]

Security Technical Implementation Guide Checklists; G[, [_____]]

SCAP Report; G[, [_____]]

ISSE Checklist (Step 3); G[, [_____]]

ISSE Checklist (Step 4); G[, [_____]]

SD-07 Certificates

Information Assurance Technical Level II/Security Plus; G[, [_____]]

1.7 QUALITY CONTROL

1.7.1 Certifications

****
NOTE: If there are contractor qualification or certification requirements related to the control system, specify those in the control system specification. If there are contractor qualifications or certifications specifically related to risk management framework they can be specified here.
****

Submit the Information Assurance Technical Level II/Security Plus certification for the Information System Engineer (ISSE) for the project. The ISSE is required to have a background check and be able to obtain a Common Access Card (CAC). The background check and ability to obtain a CAC are necessary to perform the eMASS requirements in this section. The ISSE is also responsible for developing and maintaining the cybersecurity architecture for all control systems. In addition to requirements in this

section the ISSE will perform the following duties:

a. Overseeing the development of all facility-related control system's cybersecurity solutions.

b. Identifying the security control baseline set and any applicable overlays and tailoring.

c. Construction Quality Control for Risk Management Framework submittals in this section and section 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

d. Obtain and maintain an eMASS account. The Government will initially set up eMASS records and authorization packages. Manage the authorization packages and eMASS records for all facility-related control systems as identified in paragraph CONTROL SYSTEM APPLICABILITY.

e. Lead the security control selection, security control implementation, self assessment, and testing efforts.

f. Work with the Government to complete the Security Assessment Plan.

g. Attend the Cybersecurity Commissioning Construction Coordination Meeting.

h. Attend the RMF Step 2 Checkpoint Meeting.

1.8 CYBERSECURITY DOCUMENTATION

1.8.1 Authorization Strategy Plan

Provide the Authorization Strategy Plan to include a narrative on the overall authorization approach for each control system identified in paragraph CONTROL SYSTEM APPLICABILITY. The narrative will outline the different anticipated leveraged authorizations, connections to the control system platform enclave, describe the process as outlined in paragraph RISK MANAGEMENT FRAMEWORK, and include how the RMF steps integrate with the overall construction schedule.

PART 2 PRODUCTS

****

NOTE: Specify representative spare parts to be provided to the Control Systems Test Bed, EXWC in Port Hueneme, CA if devices need additional testing performed by the government. This is normally not needed.

****

[2.1 SPARE PARTS

Provide one representative extra spare part for each ethernet capable Level 1 and Level 2 device in the control system.

] [Not used.]

PART 3 EXECUTION

3.1 RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (RMF) is a 6 step process adopted by the DoD to manage risk operating Facility-Related Control Systems. The following paragraphs identify construction requirements to support the Government in obtaining an Authority To Operate (ATO) for the control systems identified in paragraph CONTROL SYSTEM APPLICABILITY. Requirements for Steps 1 through 4 are below. RMF Steps 5 and 6 are performed by others and not part of this contract.

3.1.1 RMF Step 1: Control System Categorization

RMF Step 1, Control System Categorization is completed during the design phase of the control system. Control system categorization is listed by control system in paragraph CONTROL SYSTEM APPLICABILITY.

3.1.2 RMF Step 2: Security Control Selection

****

NOTE: RMF Step 2: Security Control Selection: Append the initial list of tailored security controls developed during design as outlined by UFC 4-010-06 to the end of this specification such that the contractor can complete RMF Step 2.

****

The security controls selected for a FRCS are initially developed during design, but the final list of security controls necessary to obtain an ATO cannot be determined without considering the specific equipment make/model/firmware selected for this contact.

3.1.2.1 Tailor Control System Security Controls

In eMASS, initiate the Security Control Selection Workflow. Next, take the initial list of security controls appended to this specification and complete tailoring the list based on specific equipment selected for this contract in accordance with NIST SP 800-82 and NIST FIPS 201-2.

3.1.2.2 Security Assessment Plan

In eMASS, initiate the Security Assessment Plan (SAP) Workflow. Track development and approval of the SAP by the Government. Provide information as necessary to complete the SAP.

3.1.2.3 Security Plan

In eMASS, initiate the Security Plan (SP) Approval Workflow. Track the review of the SP by the Government.

3.1.2.4 Ports, Protocols, And Services Management Registration Form

Obtain a Ports, Protocols, and Services Management Registration Form from https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-08-11-00-20 and fill it out with project specific information following DODI 8551.01.

3.1.2.5 RMF Step 2 eMASS Uploads

Upload the following artifacts into eMASS:

a. Cybersecurity Riser Diagrams from UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

b. Completed Control System Inventory Report from UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

c. Completed Cybersecurity Interconnection Schedule from UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

d. Ports, Protocols, and Services Management Registration Form

e. Control System Cybersecurity Documentation from UFGS 25 05 11 CYBERSECURITY FOR FACILITY-RELATED CONTROL SYSTEMS.

3.1.2.6 RMF Step 2 Checkpoint Meeting

Attend the RMF Step 2 Checkpoint Meeting.

3.1.3 RMF Step 3: Implement Controls

3.1.3.1 Security Control Implementation

In eMASS, initiate the Security Control Implementation Workflow.

3.1.3.2 Security Testing

Execute the Security Assessment Plan (SAP)

3.1.3.3 ACAS Vulnerability Scans

Conduct ACAS vulnerability scans. Generate summary and detailed ACAS Vulnerability Reports in accordance with NAVFAC FRCS AA ACAS Scan Policy Settings.

Remediate/Mitigate all discovered findings, especially high risk prior to RMF Step 4.

Generate and upload the scan summary and detailed vulnerability list into eMASS as an artifact.

Map ACAS vulnerability findings to the most appropriate CCI in the security control baseline. Upload ACAS Scan results as an artifact to eMASS Asset manager at the AP/CCI Level and add justifying statements for any non-compliance.

3.1.3.4 Security Content Automation Protocol (SCAP) Report

Complete the SCAP XCCDF XML and SCAP Report PDF/HTML files

3.1.3.5 Security Technical Implementation Guide Checklists

Apply the Security Technical Implementation Guide Checklists (STIGs) as identified in the Security Assessment Plan.

Utilize Security Content Automation Protocol (SCAP) Scans to supplement

the STIG checklist where applicable.

Map STIG findings to all CCIs identified for that particular finding according to the STIG guidance. Fully document the CKL files. Utilizing Asset Manager to import the checklists into eMASS.

3.1.3.6 POA&M

Document open (non-compliant remaining findings in the Plan of Action and Milestones (POA&M) within eMASS either manually or through the use of Asset Manager in eMASS.

3.1.3.7 ISSE Checklist (Step 3)

Complete the NAVFAC FRCS RMF Step 3 and 4 ISSE Checklist.

3.1.3.8 RMF Step 3 eMASS Uploads

Upload the following artifacts into eMASS:

a. SCAP benchmark XCCDF XML and SCAP Report (utilizing Asset Manager)

b. Fully documented STIG Checklists (utilizing Asset Manager)

c. ACAS Scans/reports (utilizing Asset Manager)

d. ISSE Checklist (Step 3)

3.1.4 RMF Step 4: Validate Controls

3.1.4.1 Security Control Accessor - Validator (SCA-V) Site Assessment

Ensure the control system(s) are ready for an assessment.

Schedule the Validator site assessment coordinating the schedules of the Validator and all control system subject matter experts.

Ensure supplier/installer and other control system subject matter experts are available at the discretion of the validator to support the assessment.

3.1.4.2 Security Assessment Workflow

Re-initiate the Security Assessment Plan Workflow in eMASS.

Submit all security controls in eMASS for Validator review.

3.1.4.3 ISSE Checklist (Step 4)

Update previously submitted NAVFAC FRCS RMF Step 3 and 4 ISSE Checklist and upload it into eMASS.

3.1.4.4 Validation Findings

Remediate/mitigate Validator findings and update the Security Assessment Report (SAR) and POA&M accordingly.

-- End of Section --