



**Facility-Related Control System
Risk Management Framework
Self-Assessment Tool
R-SAT**

User Guide

Prepared for:
Federal FRCS System Owners and other Stakeholders

December 10, 2019
Revised June 2020

Table of Contents

Introduction	1
Purpose	1
Scope	1
R-SAT Overview	2
Structure	2
Form Layout	2
Informational Popups and Alerts	2
System Information Form	3
Optional Entries (green cells)	3
Required Entries (orange cells)	4
Security Categorization Form	5
Buttons	5
Optional Entries (green cells)	6
Required Entries (orange cells)	6
Control Information Form	7
Popup Alerts	7
Buttons	8
Update Form	8
Export Data	8
Auto-filled Fields	10
Optional Entries (green cells)	12
Required Entries (orange cells)	13
eMASS Import Errors	14
Test Results Form	15
Popup Alerts	15
Buttons	16
Update Form	16
Export Data	17
Auto-filled Fields	18
Baseline Control Summary	20
Security Policies & Procedure Templates	21

Implementation Instructions: System Specific Requirements List _____	21
Implementation Instructions: ISSM Checklist _____	21
Appendix 1: References _____	22
Appendix 2: Acronyms _____	23

Revision History

Revision	Date	Name	Description
1.0	12/2019	IPERC	Initial Draft
2.0	06/2020	IPERC	Additional text added to address the addition of read-only fields in eMASS templates supported by RSAT

Introduction

Purpose

This User Guide provides an orientation, including relevant definitions and processes, to the Facility-Related Control Systems (FRCS) RMF Self-Assessment Tool (referred to herein as R-SAT). R-SAT has been developed to support an RMF Self-Assessment and facilitate entries into the Enterprise Mission Assurance Support Service (eMASS) through some process automation. R-SAT and this User Guide offer structured steps with brief instructions to guide the User through the RMF Self-Assessment.

R-SAT objectives include:

- **Cost Savings** through use of widely-available application (Microsoft Excel)
- **Time Savings** through automated generation of baseline RMF information
- **Guidance** for FRCS system owners inexperienced with RMF

Scope

R-SAT is designed specifically for Federal and DoD System Owners performing a FRCS RMF Self-Assessment, but other FRCS stakeholders may find it useful. This guide describes use of R-SAT and RMF Steps 1-3 but does not serve as a replacement for RMF requirements, guidance or training. A basic understanding of the RMF process is assumed. R-SAT facilitates RMF steps 1-3 for a FRCS by creating several forms. The data from these forms can be exported directly into eMASS templates. The databases within R-SAT are populated using references listed in Appendix 1.

User Guide sections step through use of R-SAT, beginning with an Overview (Instructions tab), then each of the user input and instructional tabs:

1. System Information Form
2. Security Categorization Form
3. Control Information Form
4. Test Results Form
5. Baseline Control Summary Form

An additional Section within this User Guide is included for ***Security Policies & Procedure Templates*** (optional documentation supported by R-SAT features).

R-SAT Overview

R-SAT was developed with funding through an Environmental Security Technology Certification Program (ESTCP) demonstration project. The most recent version of R-SAT is available on the ESTCP website.¹

Structure

R-SAT was developed as a Microsoft Excel-based template, including an extensive set of customized macros in order to execute automated aspects and perform various functions. Given this integration with Microsoft Excel, R-SAT Users need to satisfy that application's relevant licensing and minimum computing requirements.

R-SAT is structured using a familiar tab-based Excel workbook layout. R-SAT's workbook tabs include:

- Instructions - blue tab – quick start guide
- Date Entry Forms - four orange tabs – user input and autofill processes
- Informational Form – yellow tab – information summary
- Databases (hidden) - five green tabs – supporting form functions

Supplemental documents external to R-SAT include:

- eMASS Templates – spreadsheets exports from eMASS populated by R-SAT for eMASS import
- Security Policy & Procedure Documents (optional) - to address organizational policy requirements

Form Layout

All of the Forms are designed with a consistent color-coding format in order to make R-SAT easier to use. The color coding indicates the source and criteria of data:

- Orange cells indicate required User entry; data is used by R-SAT for auto-fill of other fields.
- Green cells indicate optional User entry; data may be helpful for RMF documentation.
- Grey cells indicate data fields that are not in applicable given the current entries in other R-SAT fields; the color of these data fields may change based on information entered by User.

Note: Users should not add or delete rows in R-SAT forms. Forms may be copied into external Excel files for modification. Additionally, the User should not modify the hidden sheets (database tables).

Informational Popups and Alerts

As Users navigate through R-SAT, popup menus may appear with informational text to inform or alert the User of input considerations or actions that should be taken. These popup menus and alerts are shown and described in Form instructions for where they appear in R-SAT. This includes a description of how to troubleshoot import errors of R-SAT populated templates in eMASS.

¹ <https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity>

System Information Form

The System Information Form is an offline repository where data that is useful during eMASS System Registration (RMF Step 0) can be collected for manual entry into eMASS at a later date.

RMF Step 0: Collect System Information and Identify Key Roles				
RMF Team Members and Contact Information The list of personnel assigned to the RMF roles for the system being assessed				
Role	Name	Organization	Email	Phone
Auditor				
ISO/PM				
Program ISSM				
SCA-R				
SCA-A				
AO				
User Rep (eMASS View Only)				
Organizational ISSM				
Organizational ISSO				
Estimated Date of Self Assessment Submission	1-Dec-2019			
DoD Component Information		DoD Activity		
DoD Component		DoD Activity		
System Information				
eMASS Registration Field	User Entry			
System Name				
System Acronym				
Version / Release Number				
DITPR ID				
System Type				
FRCS Type (based on FRCS Master List)	Microgrid Control System (MCS)			
System Description				
Hardware / Software / Firmware				
Information Flows / Paths				
Interconnected Information Systems and Identifiers				
System Authorization Boundary				
System Enterprise and Information Security Architecture				
Network Connection Rules				
Encryption Techniques				
Cryptographic Key Management Information				

Optional Entries (green cells)

RMF role requirements are defined in DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT) (Reference (c)). System Information fields are defined on the eMASS Step-by-Step Instructions Document² on the SERDP-ESTCP Portal.

² <https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Registering-FRCS-in-eMASS-DITPR-SNaP-IT/eMASS-Step-by-Step-Instructions>

Required Entries (orange cells)

- **ISO/PM:** Enter the name of the Information System Owner/Project Manager performing the self-assessment. This data will auto-fill the eMASS Test Result Export form (column J) as “Tested By” for auto-filled Control Correlation Identifiers (CCIs).
- **Estimated Date of Self-Assessment Submission:** Enter the date, when the self-assessment is to be submitted to the Validation Team in eMASS. This date will auto-fill the Control Information Form (column H) for auto-filled CCIs.
- **DoD Component:** The DoD Component is the entity that has authorization responsibility for the system (example: Department of Navy). This entry is auto-filled on R-SAT forms to identify the Responsible Entity applicable to Component policies (Tier 2).
- **System Name:** This data will be auto-filled on the top of R-SAT forms.
- **FRCS Type:** Select the type of FRCS from this drop-down from the FRCS Master List.³ This selection will populate related Information Type(s) from the FRCS Master List to use in the Security Categorization Form. The autofill function is described in more detail in the **Security Categorization Form** section.

Note: Each time the FRCS System Type (System Info Form drop-down) is changed, the Information Types, Provisional Impacts, and Justifications (if completed) on the Security Categorization Form are cleared and repopulated to corresponding values based on the FRCS Master List.

³ <https://www.serdp-estcp.org/serdp-estcp/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/EI-E-RMF-FRCS-Master-List-Current>

Security Categorization Form

System Categorization is RMF Step 1. This form will auto-fill Information Types⁴ identified in the FRCS Master List as being applicable to the FRCS Type selected in the System Info Form drop-down. The Provisional Impact Levels for each Information Type are also populated. R-SAT will calculate the aggregate and overall Security Impact Levels (Low, Moderate or High) for Confidentiality, Integrity and Availability (CIA). The Overall System Impact Level is the “high water mark” of the Security Impact Levels and will be used to build the security baseline on subsequent R-SAT forms. This form does not import data into the eMASS system. The Security Categorization is required to complete the system registration in eMASS.

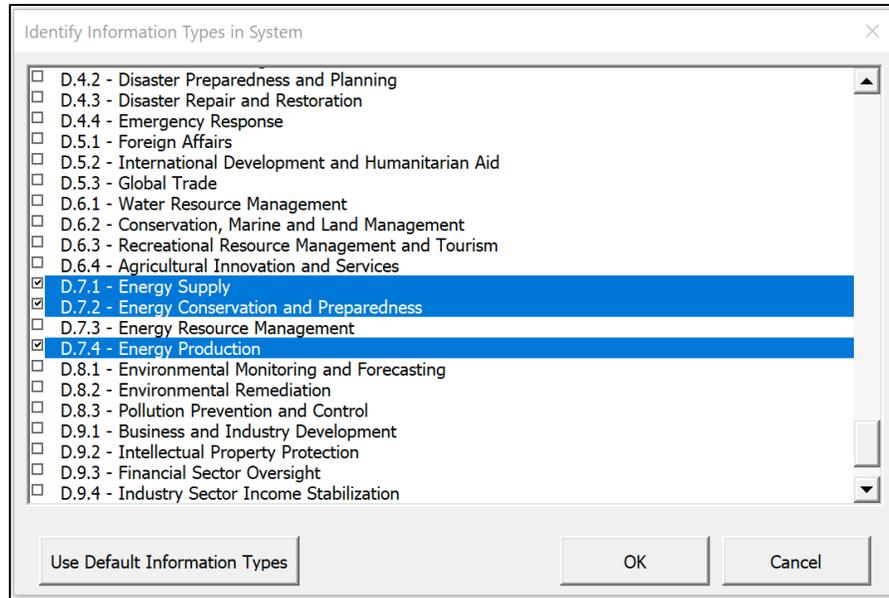
RMF Step 1: Categorize System		SYSTEM NAME:	FRCS TYPE:	RATIONAL AND FACTORS FOR ADJUSTMENTS			
		System Name	Microgrid Control System (MCS)				
SECURITY CATEGORIZATION				<p><i>*Special Factors are specific descriptions that may require User to adjust Provisional Impact Levels that have been auto populated by Tool. Users should reference NIST 800-60 VII to familiarize themselves with the guidelines for using Special Factors to adjust security categorization. The Tool ONLY populates Special Factors for Information Types that are identified on the FRCS Master List. Auto-population of Special Factors DOES NOT APPLY to the Information Types that are not included on the FRCS Master List. Users should reference NIST 800-60 VII if Special Factors column is blank to determine if Special Factors apply.</i></p>			
Information Type [Identifier]	Information Type [Name] <input type="button" value="Modify"/>	Description					
<i>Optional User entered text to document any determinations and decisions relative to the specific system</i>							
C.2.B.12	General Information						
C.3.1.1	Facilities, Fleet, and Equipment Management						
D.7.1	Energy Supply						
D.7.2	Energy Conservation and Preparedness						
D.7.4	Energy Production						
Information Type (per above)	Impact Level <i>The C-I-A Provisional Impact Levels are auto populated. User may Adjust Impact Levels to address system specific considerations.</i>	Confidentiality Impact Level	Integrity Impact Level	Availability Impact Level	Special Factors - Confidentiality (see description above)	Special Factors - Integrity (see description above)	Special Factors - Availability (see description above)
General Information	Provisional Impact: Low	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Unauthorized premature disclosure of much economic (e.g., agricultural commodity, economic indicators) data and statistics information can result in major financial	Recommended Integrity Impact Level: The provisional integrity impact level recommended for general-purpose data and statistics information is low.	Recommended Availability Impact Level: The provisional availability impact level recommended for general-purpose data and statistics information is low.
	Adjusted Impact: <i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>			
	Justification (only if modified)						
Facilities, Fleet, and Equipment Management	Provisional Impact: Low	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Information associated with maintenance, administration, and operation of many Federal government office buildings, transportation fleets, and operational facilities can be of	Special Factors Affecting Integrity Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, the integrity impact level associated with unauthorized	Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, the availability impact level associated with unauthorized
	Adjusted Impact: <i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>			
	Justification (only if modified)						
Energy Supply	Provisional Impact: Low	Moderate	Moderate	Moderate	Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of energy supply information can have a serious economic impact with respect to competitive advantages and financial and	Special Factors Affecting Integrity Impact Determination: Unauthorized modification of mission-critical information or information systems (e.g., electrical power distribution, petroleum or gas pipelines) can result in severe impacts to the environment, service, major assets and/or	Special Factors Affecting Availability Impact Determination: Mission-critical systems, functions supported by mission-critical information or information systems (e.g., electrical power generation, transmission, and/or distribution, petroleum or gas pipelines) are often adversely impacted by lack of availability.
	Adjusted Impact: <i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>			
	Justification (only if modified)						
Energy Conservation and Preparedness	Provisional Impact: Low	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed conservation measures or the distribution of energy in the event	Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency may result in extended outages. There is some	Special Factors Affecting Availability Impact Determination: Unavailability of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency may result in extended outages. There is some
	Adjusted Impact: <i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>			
	Justification (only if modified)						
Energy Production	Provisional Impact: Low	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some energy production information can result in major financial consequences. In some cases, premature disclosure of this information can	Special Factors Affecting Integrity Impact Determination: If the energy production information is time-critical or very sensitive, the integrity impact level may be moderate or high.	Recommended Availability Impact Level: The provisional availability impact level recommended for energy production information is low.
	Adjusted Impact: <i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>	<i>trust adjusted</i>			
	Justification (only if modified)						
C-I-A Security Impact Levels (high water mark based on aggregate)		Low	Moderate	Moderate			
Overall System Impact Level		Moderate					

Buttons

- Modify:** Select this button to add or remove Information Types by selecting or deselecting them from the popup menu.⁵ Information Types prescribed by the FRCS Master List are pre-selected.
 - Use Default Information Types:** clears all Information Types and auto-fills them based on the selected FRCS System Type (System Info Form drop-down)
 - OK:** populates the User selections
 - Cancel:** exits the list without saving changes

⁴ FRCS Master List Information Types (Reference (e)) based on FIPS 199 (Reference (f)), and NIST 800-60 Vol I and II (Reference ((j & k).

⁵ Modifiable Information Types include NIST SP 800-60 Vol 1 Table 4 (Mission Based and Delivery Mechanisms - excluding National Security Systems), Table 5 (Services Delivery Supported Functions), and Table 6 (Government Resource Management), and four USACE Information Types that are specific to DoD FRCS.



Optional Entries (green cells)

- **Information Type Description:** Users are encouraged to enter a description of how the Information Type is present on the FRCS. Modifying the Information Types is described below.
- **Adjusted Impact:** Users must review the auto-filled information Types, the FRCS Master List Special Factors⁶ provided (if it exists) for each Information Type and other known considerations to adjust Provisional Impact levels as appropriate. When adjustments are made, the User Adjusted Impact level will override the Provisional Impact level in the Overall System Impact Level determination.

Required Entries (orange cells)

- **Justification:** When Provisional Impacts are adjusted, the color of the associated cell for Justification turns orange indicating a required field. While this entry is not used further in R-SAT, justification will be required in eMASS for AO approval of the proposed Security Categorization.

Note: Special Factors text is only populated for Information Types that are listed on the FRCS Master List. The User should reference National Institute of Standards and Technology (NIST) 800-60 Vol II (Reference ((k) for Special Factors associated with all other Information Types.

Note: National Security Information and National Security Systems, such as Defense and National Security Information Types (D.1) and Intelligence Operations Information Types (D.3), are outside of the scope of NIST 800-60 Vol II and are not fully supported by R-SAT.

Note: Each time the FRCS System Type (System Info Form drop-down) is changed, the Information Types, Provisional Impacts, and Justifications (if completed) on the Security Categorization Form are cleared and repopulated to corresponding values based on the FRCS Master List.

⁶ Special Factors may also be reviewed in the FRCS Master List (Reference (e)) and NIST 800-60 Vol II (Reference ((k)).

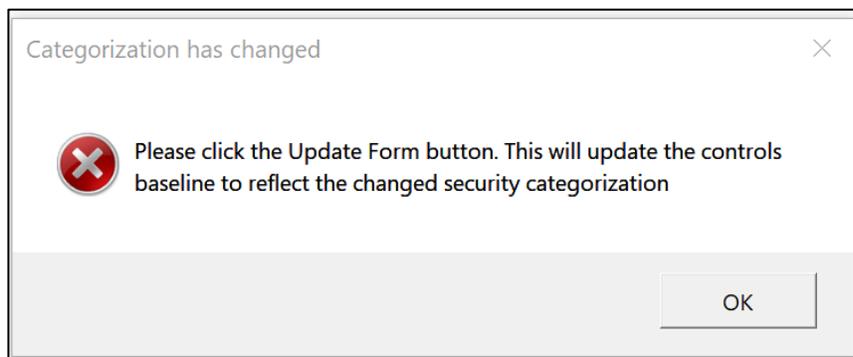
Control Information Form

Select Security Controls is RMF Step 2. The Control Information Form is where the baseline control set is generated based on the current Security Categorization and Committee on National Security Systems Instruction (CNSSI) No 1253, Appendix D-1 (Reference (a)). The CNSSI baseline includes the NIST 800-53 (Reference (h)) baseline. The System Name and the Security Categorization Impact Levels of the FRCS being assessed are indicated at the top. The Control Information Form fields that require data entry are color coded and use the same general format as the eMASS template of the same name. Read only fields are displayed without color and are provided for informational purposes only. A 2020 update to the Control Information eMASS template included the addition of a read only column (title: Compliance Status); this column does not require data entry and is not displayed on the R-SAT Control Information form.

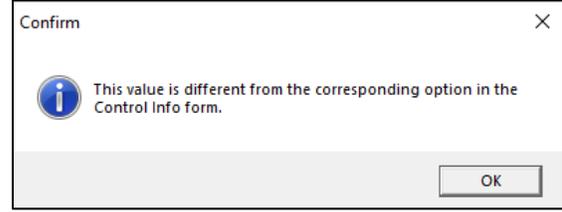
RMF Step 2: Select Security Controls															
Control Import Template:															
Update Form				Export Data				SYSTEM NAME		SECURITY CATEGORIZATION - IMPACT LEVELS					
								System Name		Confidentiality: Moderate		Integrity: Moderate		Availability: Moderate	
Control Information			Implementation Plan						IM		SLCM				
Control Number	Control Title	Control Information	Implementation Status	Common Control Provider	Security Control Designation	N/A Justification	Estimated Completion Date	Comments	Responsible Entities	Criticality	Frequency	Method	Reporting	Tracking	SLCM Comments
7	AC-1	Access Control Policy	Description: Planned	Common	System-Specific		01 Oct 2019		ISSM	CRWG White	Annually	Manual		Signature	Refer to
8	AC-10	Concurrent Session	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
9	AC-11	Session Lock	Description: Planned	Common	Hybrid		01 Oct 2019		Configuration	CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
10	AC-11(1)	Pattern-hiding	Description: Planned	Common	Hybrid		01 Oct 2019		Configuration	CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
11	AC-12	Session Termination	Description: Planned	Common	System-Specific		01 Oct 2019		Configuration	CRWG Yellow	Constantly	Automated		STIG/SRG	STIG/SRG
12	AC-12(1)	User-initiated	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG Yellow	Underdetermine	Underdetermine			
13	AC-14	Permitted Actions	Description: Planned	Common	System-Specific		01 Oct 2019		SO	CRWG White	Annually	Underdetermine			
14	AC-16	Security Attributes	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
15	AC-16(6)	Maintenance Of	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
16	AC-17	Remote Access	Description: Planned	Common	Common		01 Oct 2019		SO/Enclave	CRWG White	Annually	Manual		Acceptable	Applies to
17	AC-17(1)	Automated	Description: Planned	Common	Common		01 Oct 2019		Enclave	CRWG Yellow	Constantly	Automated			Applies to
18	AC-17(2)	Protection Of	Description: Planned	Common	Common		01 Oct 2019		Enclave	CRWG Yellow	Constantly	Automated			Applies to
19	AC-17(3)	Managed Access	Description: Planned	Common	Common		01 Oct 2019		Enclave	CRWG Yellow	Constantly	Automated			Applies to
20	AC-17(4)	Privileged	Description: Planned	Common	System-Specific		01 Oct 2019		Enclave	CRWG Yellow	Annually	Underdetermine			Applies to
21	AC-17(6)	Protection Of	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG Yellow	Underdetermine	Underdetermine		Acceptable	Applies to
22	AC-17(9)	Disconnect / Disable	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			Applies to
23	AC-18	Wireless Access	Description: Planned	Common	Common		01 Oct 2019		SO/Design	CRWG White	Annually	Manual		Acceptable	Applies to
24	AC-18(1)	Authentication And	Description: Planned	Common	Common		01 Oct 2019		NSS Best Practice	CRWG Yellow	Constantly	Automated			Applies to
25	AC-18(3)	Disable Wireless	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG Yellow	Underdetermine	Underdetermine			Applies to
26	AC-18(4)	Restrict	Description: Planned	Common	System-Specific		01 Oct 2019		Insider Threat	CRWG Yellow	Underdetermine	Underdetermine			Applies to
27	AC-19	Access Control For	Description: Planned	Common	Hybrid		01 Oct 2019		SO/Enclave	CRWG Yellow	Annually	Manual	Annual	Acceptable	Applies to
28	AC-19(3)	Full Device /	Description: Planned	Common	System-Specific		01 Oct 2019		Enclave	CRWG Yellow	Constantly	Automated			Applies to
29	AC-2	Account	Description: Planned	Common	Hybrid		01 Oct 2019		Account Manager	CRWG White	Annually	Underdetermine		STIG/SRG	Refer to
30	AC-2(1)	Automated System	Description: Planned	Common	Common		01 Oct 2019		Enclave	CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
31	AC-2(10)	Shared / Group	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG Yellow	Underdetermine	Underdetermine			
32	AC-2(12)	Account Monitoring	Description: Planned	Common	Common		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
33	AC-2(13)	Disable Accounts For	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG Yellow	Underdetermine	Underdetermine			
34	AC-2(2)	Removal Of	Description: Planned	Common	Common		01 Oct 2019		Design	CRWG White	Constantly	Automated		STIG/SRG	DoD has
35	AC-2(3)	Disable Inactive	Description: Planned	Common	Common		01 Oct 2019		Configuration	CRWG White	Constantly	Underdetermine		STIG/SRG	STIG/SRG
36	AC-2(4)	Automated Audit	Description: Planned	Common	Common		01 Oct 2019		Configuration	CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
37	AC-2(5)	Inactivity Logout	Description: Planned	Common	Common		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
38	AC-2(7)	Role-based Schemes	Description: Planned	Common	System-Specific		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
39	AC-2(9)	Restrictions On Use	Description: Planned	Common	Common		01 Oct 2019			CRWG White	Underdetermine	Underdetermine			
40	AC-2(20)	Use Of External	Description: Planned	Common	Common		01 Oct 2019		SO/Enclave	CRWG White	Annually	Manual		Service Level	Applies to
41	AC-20(1)	Limits On Authorized	Description: Planned	Common	Common		01 Oct 2019		SO/Enclave	CRWG White	Annually	Manual		Acceptable	Applies to

Popup Alerts

A popup alert will appear when selecting the Excel tab to open the form if the Security Impact Levels in the Security Categorization Form do not match the current Control Info Form levels. The Control Information Form must be regenerated each time the Security Impact Levels are changed by selecting the Update Form button and OK to confirm update options.



A popup alert will also appear to confirm selection of the Update Form button options:



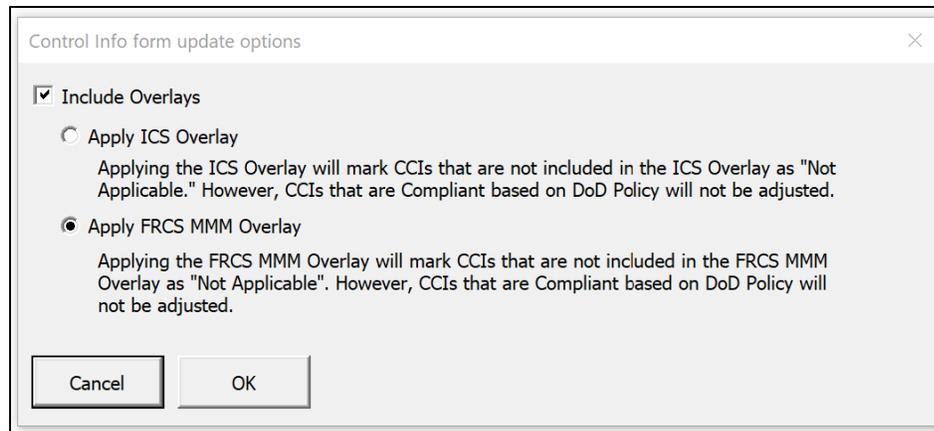
A popup will alert the User if 1) The Security Categorization is M-M-M, but the ICS Overlay was chosen, or 2) The selected overlay on one form does not match the selected overlay on the other form. For best results, the same overlay should be selected on the Control Information and Test Results forms.

Buttons

Update Form

Select this button to auto-fill the form with the security control baseline based on the current Security Categorization. Choose from the following options:

- **Include Overlays:** select the checkbox to apply either of the FRCS overlays (Reference (g)).
- **Apply Industrial Control System (ICS) Overlay:** this will apply the NIST 800-82 (Reference ((l) ICS Overlay for Low or Moderate (not MMM) FRCS.
- **Apply FRCS MMM Overlay:** this will apply the DoD CIO Overlay for FRCS with a Moderate-Moderate-Moderate security baseline. Determine if this is the required overlay with your RMF authorities (designated Authorizing Official (AO) representative).



Export Data

Select this button after the form is auto-filled (using the Update Form button) and all manual tailoring is complete to the point that it is ready to be uploaded to eMASS. This allows the User to export the data from the R-SAT form into a previously exported Control Information template for import and auto-fill of the FRCS record in eMASS.

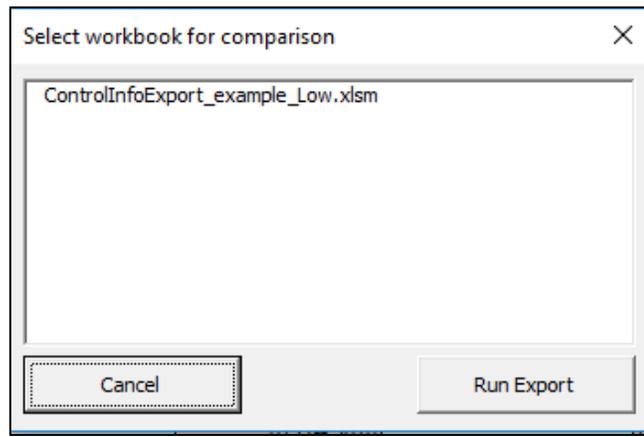
Note: Generic templates or templates from eMASS records other than the FRCS undergoing the Self-Assessment may not successfully import to eMASS. See eMASS Import Errors Section.

Note: It is recommended to import the R-SAT populated templates into eMASS and reexport prior to manual tailoring. Multiple import/exports will provide the User with fewer data fields to review if an error is generated during eMASS import.

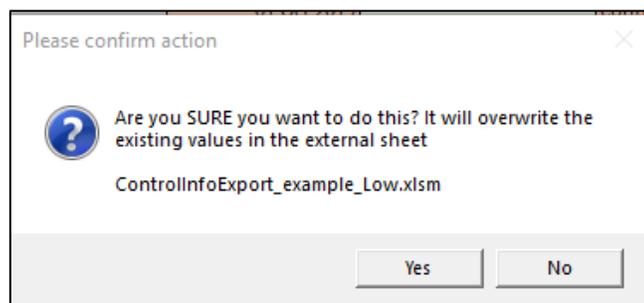
Export steps are:

The steps to export data from R-SAT forms into eMASS templates are:

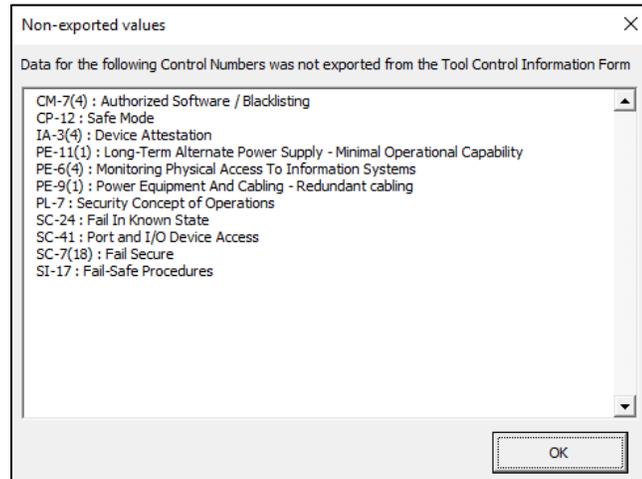
1. Export the Control Information Form from eMASS.
2. Open the eMASS template file and Enable Content.
3. Select <Export Data> from the top menu on the R-SAT Form. This will open a list of open Excel files in the “Select workbook for comparison” window (see below).



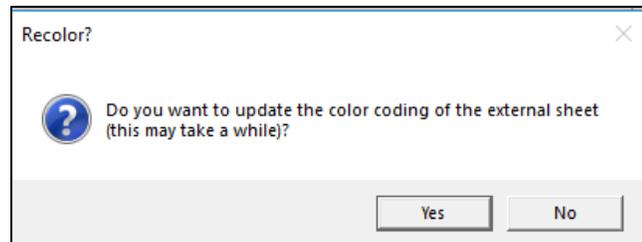
4. Select the appropriate Excel Worksheet (eMASS template file). If you do not see the desired worksheet, Cancel the export and ensure the exported eMASS template is open.
5. Select <Run Export> to populate the eMASS template with the R-SAT form data. A popup will appear to verify the execution of the data export. The eMASS record template is populated based on a match of the Control Number between the R-SAT form and the eMASS template.



6. A list of “Non-Exported values” may appear in a pop-up window (example below). These controls should be noted (click and drag to highlight them and select Ctrl-C to copy) and may require follow-up. These controls have been identified by R-SAT as belonging to the control baseline but were not found in the external eMASS template. These controls may need to be added to eMASS manually. You may add these controls to the eMASS record and export a new Controls Information Form template and start again at step 1 for the export. <OK> closes the popup list.



7. Select <Yes> in the popup to activate the macros in the external Control Information Template to adjust the color coding; Selecting <No> will close this pop-up without action.



8. Review the populated eMASS template for fields with an orange color. This indicates required control information not addressed in R-SAT and needs manual review and completion. See eMASS Import Errors for important notes and eMASS import troubleshooting guidance.

Auto-filled Fields

The auto-fill function in the Control Information Form uses the current Security Categorization, the user-selected Overlay options (Update Form button), and R-SAT database information to, at least partially, populate required fields. A summary of the auto-populated data is summarized in Table 1 Implementation Status - Auto-fill Data.

Note: These are suggested entries that must be reviewed for additional tailoring.

Table 1 Implementation Status - Auto-fill Data

Security Control Type	Implementation Plan Entry				
	Implementation Status	Common Control Provider	N/A Justification	Estimated Completion date	Comment
CNSSI control	Planned			User input date from System Info Form	
DoD policy control	Inherited	DoD or User entered DoD Component		Date in eMASS system for Inherited controls	Description of DoD Policy
4-010-06 UFC (Reference ((o) not applicable to FRCS systems control	Not Applicable		Description of applicability from 4-010-06 UFC Table H-2		Description of applicability from 4-010-06 UFC Table H-2
ICS Overlay excluded Control	Not Applicable [If ICS Overlay <button> is selected]		Excluded per ICS overlay is noted [If ICS Overlay <button> is selected]		
FRCS MMM excluded Control	Not Applicable [If FRCS MMM Overlay <button> is selected]		Excluded per FRCS MMM overlay is noted [If FRCS MMM Overlay <button> is selected]		

Blank fields indicate no data population – Grey fields indicate data is not required

Auto-filled field descriptions:

- **Control Information:** These three fields are from the NIST 800-53 security control descriptions in the eMASS Control Information Import/Export Template for the given Security Categorization.
- **Implementation Status:** auto-filled in accordance with the overlay options. "Planned" is the default value for any control that is applicable based on the selected User Security Categorization. "Inherited" is the value chosen for controls that are covered/provided (e.g., by DoD or Tier 2 policy). Any controls removed by the selected overlay are marked as "Not Applicable."
- **Common Control Provider:** auto-fills with the Common Control Provider if the Implementation Status is "Inherited."
- **Security Control Designation:** drop-down data field auto-filled with the designation for each security control as "Common," "System-specific" or "Hybrid."
- **N/A Justification:** auto-filled with default text for the justification of the auto-filled "Not Applicable" Implementation Status.
- **Estimated Completion Date:** auto-filled with the entry in "Estimated date of Self-Assessment Submission" in the System Information Form.
- **Comments:** auto-fills with information that may be useful for tailoring. Examples: justification of FRCS Non-applicability with guidance from 4-010-06 UFC Table H-2 or designation of an inherited DoD control.
- **Responsible Entities:** auto-fills the responsible entities for inherited/auto-filled controls. "DOD CIO" is entered for DoD inheritance. The DOD Component (e.g., Army, Navy, Air Force) entered by the User on the System Information Form for Tier 2 inheritance.
- **Criticality:** like the Control Information fields, this field is auto-filled with values from the eMASS Control Information Import/Export template for the given Security Categorization.
- **Frequency:** auto-fills a suggested frequency from the drop-down menu based on the control descriptions in NIST 800-53 and assessment objectives in NIST 800-53A (Reference ((i). "Undetermined" is entered when the frequency is not determined by the control.
- **Method:** auto-fills a suggested method from the drop-down menu based on the control descriptions in NIST 800-53 and assessment objectives in NIST 800-53A. "Undetermined" is entered when the method is not determined by the control.
- **Reporting:** auto-fills for Planned controls with "Non-compliant controls reported to Information Security System Manager (ISSM)".
- **Tracking:** auto-fills with "POA&M will be updated."
- **SLCM Comments:** auto-fills with a starting point of who reports what to whom by when. Note that the ISSM checklist (R-SAT Template) is referenced in the default text in this field for some controls. *This field always requires additional User tailoring to the organizational policies and procedures.*

Optional Entries (green cells)

These non-required cells may be populated as appropriate.

- **Comments:** use, for example, to provide additional rationale for identifying a security control as N/A or any deviations from control implementation guidance. Some controls are auto-filled with suggested information (e.g., justification of FRCS Non-applicability with guidance from 4-010-06 UFC Table H-2).
- **Risk Assessment fields:** these are optional in RMF Step 2 and not auto-filled by R-SAT.

Required Entries (orange cells)

Required cells must be populated. Auto-filled entries are described above and are intended as a time savings for the User. These should be reviewed and tailored to ensure the entry is applicable to the actual Implementation Status of the control. All required field are fully or partially auto-filled.

Note: The eMASS form will not import properly if any Required fields are blank.

- **Implementation Status:** a drop-down that identifies the implementation status of the security control as Planned, Implemented, Inherited, Manually Inherited, or Not Applicable.
- **Common Control Provider:** a drop-down data field that identifies the source of the Inherited security control as DoD, Component or Enclave. Data is required when the implementation status is "Inherited" or "Manually Inherited".
- **Security Control Designation:** drop-down auto-filled with the designation for each security control as:
 - "Common" for controls with features that are typically inherited by DoD policy or organizational policy.
 - "System-specific" for controls with features unique to the system based on NIST 800-53 descriptions and assumed methods of control implementation.
 - "Hybrid" for controls that have features with both Common and System-specific features based on NIST 800-53 descriptions and assumed methods of control implementation.
- **N/A Justification:** required only when the implementation status is "Not Applicable". Users may manually update the default text or enter justifications for controls they have manually marked as "Not Applicable."
- **Estimated Completion Date:** an estimated completion date for all tasks associated with the implementation of security controls.
- **Responsible Entities:** identifies personnel responsible for implementing each security control.
- **Frequency:** drop-down of the frequency with which the control is monitored. An entry of "Undetermined" is entered when the method is not determined by the control.
- **Method:** a drop-down data field that represents the method of monitoring the control. This should be aligned with the control requirements and tailored to the actual reporting structure.
- **Reporting:** the method of reporting for continuous monitoring - who reports what to whom by when. The reporting mechanism may vary depending on the criticality of the control.
- **Tracking:** the method of tracking information for non-compliant controls - how non-compliant or ineffective security controls will be tracked.
- **System Level Continuous Monitoring (SLCM) Comments:** who reports what to whom by when. The default text here is intended as a starting point for the required reporting explanation. *This field always requires additional User tailoring.* The *ISSM Checklist* referenced in this SLCM Comments field is a Template provided with R-SAT to assist with staffing security policies (discussed in Supporting Templates Section).

Once the Control Information Form is populated by R-SAT and manually tailored, the form data may be exported to an eMASS template for import into the related eMASS RMF record. See the **Export Data** section.

eMASS Import Errors

The Import of actual templates, exported from eMASS and populated by R-SAT, have been tested. If there are errors in the import process of your R-SAT populated (and manually tailored) template, consider the following:

- Incorrect formatting in fields with dates or drop-down entries. A space or capitalization mismatch will cause errors.
- eMASS templates will not import properly if any Required fields (orange shaded) are blank. Some Required fields may not be populated by R-SAT if the response requires User input.
- R-SAT will only export data into the controls listed in the eMASS templates. R-SAT will not add fields into the external eMASS Control Information Export form.
- The Security Categorization must be entered in the eMASS record before a template can be exported and this must match the Security Categorization in R-SAT to ensure correct matching and population of all controls.

Note: It is recommended to import the R-SAT populated templates into eMASS and reexport prior to changes with R-SAT or manual tailoring. Multiple import/exports will provide the User with fewer data fields to review if an error is generated during eMASS import.

Test Results Form

Implement Security Controls is RMF Step 3. At this step, evidence and implementation descriptions for CCI (the decomposition of security control requirements into singular, actionable statements) are documented. The System Name and the Security Categorization of the FRCS being assessed is indicated on the top of the form. The Test Results Form fields that require data entry are colored light blue and use the same format as the eMASS template of the same name. Read only fields are displayed without color and are provided for informational purposes only. A 2020 update to the Test Results eMASS template included the addition of read only columns (titles: Control Implementation Status, Security Control Designation, Inherited); these columns does not require data entry and is not displayed on the R-SAT Test Results form.

Control / AP Information							Test Results			Latest Test Results				
Control	Contro	AP	CCI	CCI	Implem	Assessment Procedures	Compliance	Date Tested	Tested By	Test Results	Compliar	Date	Tested B	Test Result
AC-1	Description: AC-1.3	000001	The	The	The organization conducting the									
AC-1	Description: AC-1.4	000002	The	The	The organization conducting the									
AC-1	Description: AC-1.7	000003	The	The	The organization conducting the									
AC-1	Description: AC-1.5	000004	The	The	The organization conducting the									
AC-1	Description: AC-1.6	000005	The	The	The organization conducting the									
AC-1	Description: AC-1.9	000006	The	The	The organization conducting the									
AC-1	Description: AC-1.8	001545	The	DoD has	The organization being									
AC-1	Description: AC-1.10	001546	The	DoD has	The organization being									
AC-1	Description: AC-1.1	002107	The	DoD has	The organization being									
AC-1	Description: AC-1.2	002108	The	DoD has	The organization being									
AC-10	Description: AC-10.1	000054	The	The	The organization conducting the									
AC-10	Description: AC-10.2	000055	The	The	The organization conducting the									
AC-10	Description: AC-10.3	002252	The	DoD has	The organization being									
AC-11	Description: AC-11.9	000056	The	The	The organization conducting the									
AC-11	Description: AC-11.1	000058	The	The	The organization conducting the									
AC-11	Description: AC-11.2	000059	The	DoD has	The organization being									
AC-11(1)	Description: AC-11(1).1	000060	The	The	The organization conducting the									
AC-12	Description: AC-12.1	002360	The	The	The organization conducting the									
AC-12	Description: AC-12.2	002361	The	The	The organization conducting the									
AC-12(1)	Description: AC-12(1).1	002362	The	DoD has	The organization being									
AC-12(1)	Description: AC-12(1).2	002363	The	The	The organization conducting the									
AC-12(1)	Description: AC-12(1).3	002364	The	The	The organization conducting the									
AC-14	Description: AC-14.1	000061	The	The	The organization conducting the									
AC-14	Description: AC-14.2	000232	The	The	The organization conducting the									
AC-16	Description: AC-16.1	002256	The	The	The organization conducting the									
AC-16	Description: AC-16.2	002257	The	The	The organization conducting the									
AC-16	Description: AC-16.3	002258	The	The	The organization conducting the									
AC-16	Description: AC-16.4	002259	The	The	The organization conducting the									

Popup Alerts

Just like with the Control Information Form, a popup alert will appear when selecting the Excel tab to open the form if the Security Impact levels in the Security Categorization Form do not match the current Test Results Form levels. The Test Results Form must be regenerated each time the Security Impact Levels are changed by selecting the Update Form button and OK to confirm update options.

A popup alert will also appear to confirm selection of the Update Form button options if 1) The Security Categorization is M-M-M, but the ICS Overlay was chosen, or 2) The selected overlay on one form does not match the selected overlay on the other form. For best results, the same overlay should be selected on the Control Information and Test Results forms.

See Popup Alerts in the Control Information Form section for graphical examples.

Buttons

Update Form

Select this button to generate the CCI baseline based on the current Security Categorization and auto-fill the Test Results fields (columns H-K) with tailorable, default values. Choose from the following options:

- **Include UFC 4-010-06:** Check this box to auto-fill CCIs as “Not Applicable” in accordance with Table H-2 of the UFC.
- **Include Policy and Procedure Template Data:** select the checkbox if you intend to use the security policy and procedure templates provided with R-SAT. See *Security Policies & Procedure Templates* section for more information.
- **Include Tier 1 and Tier 2 DoD Inherited Controls:** select the checkbox to auto-fill test results data for CCIs that may already be covered by Federal, DoD or Component-level (Tier 2) policy.
- **Include Overlays:** select the checkbox to apply either of the FRCS overlays.
 - **Apply ICS Overlay:** this will apply the NIST 800-82 ICS Overlay for the control baseline.
 - **Apply FRCS MMM Overlay:** this will apply the DoD CIO Overlay for FRCS with a Moderate-Moderate-Moderate security baseline. Determine if this is the required overlay with your RMF authorities (designated AO representative).

Test Results form update options

Include UFC 4-010-06 "Not Applicable" Controls

Include Policy and Procedure Template Data (High Impact Level Controls are not included in Templates)

Include Tier 1 and Tier 2 DoD Inherited Controls

Include Overlays

Apply ICS Overlay
Applying the ICS Overlay will mark CCIs that are not included in the ICS Overlay as "Not Applicable." However, CCIs that are Compliant based on DoD Policy will not be adjusted.

Apply FRCS MMM Overlay
Applying the FRCS MMM Overlay will mark CCIs that are not included in the FRCS MMM Overlay as "Not Applicable". However, CCIs that are Compliant based on DoD Policy will not be adjusted.

Cancel OK

Export Data

Select this button after the form is auto-filled (using the Update Form button) and all manual tailoring is complete to the point that it is ready to be uploaded to eMASS. This allows the User to export the data from the R-SAT form into a previously exported TReExport template for import and auto-fill of the FRCS record in eMASS.

See **Export Data** section in the **Control Information Form** section for sample screen shots and Steps 1-6 of the export process. After Step 6, you will see the “Test Results comparison” window:

TR Export comparison

Showing values for CCI 000001, control # AC-1 (1 out of 5 potential conflicts)
eMASS Record - Latest Test Results

creat conflict

Proposed Test Results

The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document

Use Proposed Test Results Use Proposed For All Use Latest For All

<< < Prev Next > >> Cancel OK

This window steps you through each potential conflict between the R-SAT populated Test Results entries (column K) in the form and existing eMASS template entries (column O). The example figure shows CCI 000001 as having the Test Results text, “create conflict” in the eMASS template, which means this CCI is already addressed in eMASS. R-SAT is proposing the auto-filled Test Results text shown to populate column K in the template for this CCI. Anything populated by R-SAT will go into columns H-K in the template and will append existing CCI test result information upon import to eMASS. For each conflict, you may choose from the following options:

- Select “ Use Proposed Test Results” to auto-fill the template with R-SAT form data – leave this box blank if you do not wish to update what already exists in eMASS (Latest Test Results).
 - Select “Next” to advance to the next conflict
 - Select “Prev” button to return to a previous selection
- Select “Use proposed for all” to populate R-SAT form Test Results data into template columns H-K for all CCIs “conflicts”
- Select “Use latest for all” to keep eMASS template data as-is for all CCIs “conflicts” (No auto-fill is performed).
- When finished with conflict selections, select “OK” to complete the data export. “Cancel” will forego any export from R-SAT to the template.

Note: R-SAT will not export data when there is an exact text match between the Proposed Test Results on the R-SAT form and the Latest Test Results on the eMASS template. This avoids duplication in eMASS by importing the same text again.

Note: Import of the eMASS Test Result template will create an additional entry in the Test Results for a CCI in eMASS if data is exported to columns H-K in the template and existing data is present in the “Latest Test Results Fields” (Columns L-O). Please carefully review the Comparison pop-up window prior to exporting data, and review columns H-K in the template after the export and prior to importing the template into eMASS.

Auto-filled Fields

The auto-fill function in the Test Results Form uses the current Security Categorization, the user-selected options (Update Form button), and R-SAT database information to, at least partially, populate required fields. The auto-populated data is summarized in Table 2 Test Results - Auto-fill Data.

Note: These are suggested entries that must be reviewed for additional tailoring.

Table 2 Test Results - Auto-fill Data

Security Control Selection Option	Test Result Entry - Columns H - K			
	Compliance	Date Tested entry	Tested By	Test Results
Include UFC 4-010-06 not applicable control	Not Applicable	Current date	User entered ISO/PM Name	UFC 4-010-06 Table H-1 text
Include Policy and Procedures Template responses	Compliant	Current date	User entered ISO/PM Name	Text to match Supporting R-SAT templates documentation
Include Tier 1 and 2 DoD Inherited controls	Compliant	Date in eMASS system for DoD Tier1/2 control	"DoD CIO" or User entered Component	DoD described applicability
Include ICS Overlay (Documentation for excluded controls)	Not Applicable	Current date	User entered ISO/PM Name	Text to justify the use of the ICS Overlay
Include FRCS MMM Overlay (Documentation for excluded controls)	Not Applicable	Current date	User entered ISO/PM Name	Text to justify the use of the FRCS MMM Overlay

Once the Test Results Form is populated by R-SAT and manually tailored, the form data may be exported to an eMASS template for import into the related eMASS RMF record. See the Export Data section.

Baseline Control Summary

Baseline Control Summary			SYSTEM NAME	SECURITY CATEGORIZATION - IMPACT LEVELS			Overlay Applied
			System Name	Confidentiality: Moderate	Integrity: Moderate	Availability: Moderate	ICS overlay
Baseline Controls	Controls Removed from Baseline by Overlay	Controls Added to Supplement the Baseline					
6 AC-1 - Access Control Policy And Procedures	AC-2(5) - Inactivity Logout	CM-7(5) - Authorized Software / Whitelisting					
7 AC-2 - Account Management	AC-2(7) - Role-based Schemes	CP-12 - Safe Mode					
8 AC-2(1) - Automated System Account Management	AC-2(9) - Restrictions On Use Of Shared Groups / Accounts	IA-3(1) - Cryptographic Bidirectional Authentication					
9 AC-2(2) - Removal Of Temporary / Emergency Accounts	AC-2(10) - Shared / Group Account Credential Termination	IA-3(4) - Device Attestation					
10 AC-2(3) - Disable Inactive Accounts	AC-2(12) - Account Monitoring / Atypical Usage	PE-6(4) - Monitoring Physical Access To Information Systems					
11 AC-2(4) - Automated Audit Actions	AC-2(13) - Disable Accounts For High-risk Individuals	PE-9(1) - Power Equipment And Cabling - Redundant cabling					
12 AC-3 - Access Enforcement	AC-3(4) - Discretionary Access Control	PE-11(1) - Long-Term Alternate Power Supply - Minimal Operational Capability					
13 AC-4 - Information Flow Enforcement	AC-6(7) - Review Of User Privileges	PL-7 - Security Concept of Operations					
14 AC-5 - Separation Of Duties	AC-6(8) - Privilege Levels For Code Execution	SC-7(18) - Fail Secure					
15 AC-6 - Least Privilege	AC-10 - Concurrent Session Control	SC-24 - Fail In Known State					
16 AC-6(1) - Authorize Access To Security Functions	AC-12(1) - User-initiated Logouts / Message Displays	SC-41 - Port and I/O Device Access					
17 AC-6(2) - Non-privileged Access For Nonsecurity Functions	AC-16 - Security Attributes	SI-17 - Fail-Safe Procedures					
18 AC-6(5) - Privileged Accounts	AC-16(6) - Maintenance Of Attribute Association By Organization						
19 AC-6(9) - Auditing Use Of Privileged Functions	AC-17(6) - Protection Of Information						
20 AC-6(10) - Prohibit Non-privileged Users From Executing Privileged Functions	AC-17(9) - Disconnect / Disable Access						
21 AC-7 - Unsuccessful Logon Attempts	AC-18(3) - Disable Wireless Networking						
22 AC-8 - System Use Notification	AC-18(4) - Restrict Configurations By Users						
23 AC-11 - Session Lock	AC-20(3) - Non-organizationally Owned Systems / Components/Devices						
24 AC-11(1) - Pattern-hiding Displays	AC-23 - Data Mining Protection						
25 AC-12 - Session Termination	AT-3(2) - Physical Security Controls						

The security baseline control sets in eMASS are based on the CNSSI 1253 controls, which includes NIST SP 800-53 (revision 4). The Baseline Control Summary lists the CNSSI controls applicable to the C-I-A Security Categorization from the Security Categorization Form. This list provides a snapshot of the controls listed in the Control Information Form, and summary updates each time the User updates the Control Information Form. The Baseline Controls (Column A) are the full list of applicable controls required by the Security Categorization and as tailored by Control Information Form Update Form options. Controls that have been removed from the CNSSI 1253 baseline based on an Overlay applied by the User are summarized (Column B). Controls that have been added to the CNSSI 1253 baseline to supplement an Overlay applied by the User are summarized (Column C). The User may use this list to determine if any controls must be manually added to the eMASS registry.

Note: The Baseline Control Summary represents the same set of controls listed in the Control Information Form. Each time the FRCS System Type on the System Information Form is changed, or the Security Impact Levels on the Security Categorization Form are changed, the selected controls must be re-populated on the Control Information Form using the <Update Form> button.

Security Policies & Procedure Templates

Many of the singular, actionable item that comprise the security control best practices are accomplished at the organizational level. There are nineteen Policy and Procedures (P&P) Supporting Templates with related appendices and log sheets/lists that accompany R-SAT. This set of documents includes:

- **Overview Document:** general procedural requirements for NIST family controls.
- **Control Family Documents:** unique policies and procedures for each NIST control family.
 - **System Specific Requirements List** (“Overview Document” Appendix A): system-specific security controls to be addressed during the design and configuration of the system.
- **ISSM Checklist** (“Overview Document” as Appendix B): ongoing actions and ISSM responsibilities for system security and RMF package maintenance.
- **Log Sheet Templates:** Templates to record ongoing actions and documentation to comply with security requirements. Log Sheets are referenced throughout the P&P Supporting Templates.

The P&P Templates serve as a starting point to implement and document organization-level implementation of security controls (i.e., acceptable use restrictions or assurance requirements). Sections of the text, [delineated within brackets], require specific tailoring by the User. The Supporting Templates are cross-referenced with the related CCIs, and each policy-related CCI in the Test Results Form points to the associated P&P document.

Note: The Supporting Templates are tailored to a Low and/or Moderate Impact Level FRCS with the ICS Overlay implemented; High Impact Level Controls are not addressed.

Implementation Instructions: System Specific Requirements List

Some security controls address system-specific aspects and require the User to develop procedures or apply configurations to address implementation. Controls with system-specific aspects are not addressed in the P&P Supporting Templates; therefore, these rows have blank entries in Columns H-K of the Test Result Export Form (when the User selects UPDATE FORM>> Include Policy and Procedure Templates). Controls that may require system-specific tailoring are identified on the System Specific Requirements List to assist the User with identification of these controls. The System Specific Requirements List is intended to provide Users a starting point for identifying controls with system-specific procedural aspects.

Implementation Instructions: ISSM Checklist

The security controls, periodically and when necessary, must be maintained and updated in the System Security Plan in eMASS. An action list for implementation of P&Ps is provided as the ISSM Checklist. The ISSM Checklist is divided into “Low “and “Moderate” Impact Level Controls; All Low Impact Level Controls are also applicable to Moderate Impact level systems.

Controls that have actions items described on this list are also referenced in the R-SAT Control Information Form <SLCM Comment> field (Column Q). The SLCM portion of the Control Information Form is intended to address System Level Continuous Monitoring strategies.

Templates to record on-going actions and documentation to comply with security requirements are provided as Log Sheet Templates. The ISSM Checklist and Log Sheet Templates are intended to provide the User a starting point for developing continuous monitoring strategies for systems.

Appendix 1: References

The references used throughout this document are listed below. This User Guide is intended to supplement, not replace, the content in these references to support the use of R-SAT. Information in these references will take precedence over any conflicts in this User Guide.

- a. Committee on National Security Systems Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014, as amended.
- b. Defense Information System Agency (DISA) dashboard on DoD Cyber Exchange (<https://public.cyber.mil/stigs/cci/>)
- c. DoD Instruction 8510.01: "Risk Management Framework (RMF) for DoD Information Technology (IT)," Change 2, July 28, 2017.
- d. DoD Instruction 8500.01 "Cybersecurity," Change 1, Oct 07, 2019.
- e. RMF FRCS Master List, Final: June 23, 2018 posted on SERDP-ESTCP Portal, <https://www.serdp-estcp.org>
- f. Federal Information Processing Standard Publication (FIPS Pub) 199, "Standards for Security Categorization of Federal Information Systems," eb 2004.
- g. Facility Related Control System (FRCS) Overlay, RMF Implementation Division DoD-CIO, DCIO-CS, CSRM, Last Updated: May 31, 2019.
- h. NIST Special Publication (SP) 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 30, 2013.
- i. NIST Special Publication (SP) 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," Dec 18, 2014
- j. NIST Special Publication (SP) 800-60 Volume 1 Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," Aug 2008.
- k. NIST (SP) 800-60 Volume 2 Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," Aug 2008.
- l. NIST (SP) 800-82 Revision 2, "Guide to Industrial Control Systems (ICS) Security," May 2015, as amended.
- m. DoD RMF Knowledge Service portal, <https://rmf.ks.osd.mil>
- n. SERDP-ESTCP Portal, <https://www.serdp-estcp.org>
- o. UFC 4-010-06, Unified Facilities Criteria, "Cybersecurity of Facility-Related Control Systems," January 18, 2017 as amended.

Appendix 2: Acronyms

The acronyms and abbreviations used in the User Guide are included below. Additional information and definitions can be found in the reference listed in parenthesis.

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
C-I-A	Confidentiality – Integrity -Availability (NIST 800-60 Vol 1 and Vol II)
CCI	Control Correlation Identifier (https://public.cyber.mil/stigs/cci/)
CIO	Chief Information Officer (DoDI 8510.01)
CNSSI	Committee on National Security Systems Instruction (CNSSI 1253)
DISA	Defense Information System Agency (www.disa.mil)
DoD	Department of Defense
DoDI	DoD Instruction
eMASS	Enterprise Mission Assurance Support Service
ESTCP	Environmental Security Technology Certification Program (www.serdp-estcp.org)
FIPS	Federal Information Processing Standards (FIPS 199)
FRCS	Facility Related Control Systems (RMF KS web portal)
ICS	Industrial Control System
ISO	Information System Owner (DoDI 8510.01)
ISSM	Information Security System Manager
PM	Project Manager
P&P	Policy and Procedures
NIST	National Institute of Standards and Technology
NSS	National Security System (CNSSI 1253)
RMF	Risk Management Framework (DoDI 8510.01)
R-SAT	RMF Self-Assessment Tool
SCA	Security Control Assessor
SCAR	Security Control Assessor Representative
SERDP	Strategic Environmental Research and Development (www.serdp-estcp.org)
SLCM	System Level Continuous Monitoring
SP	Special Publication
UFC	Unified Facilities Criteria (UFC 4-010-06)