

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

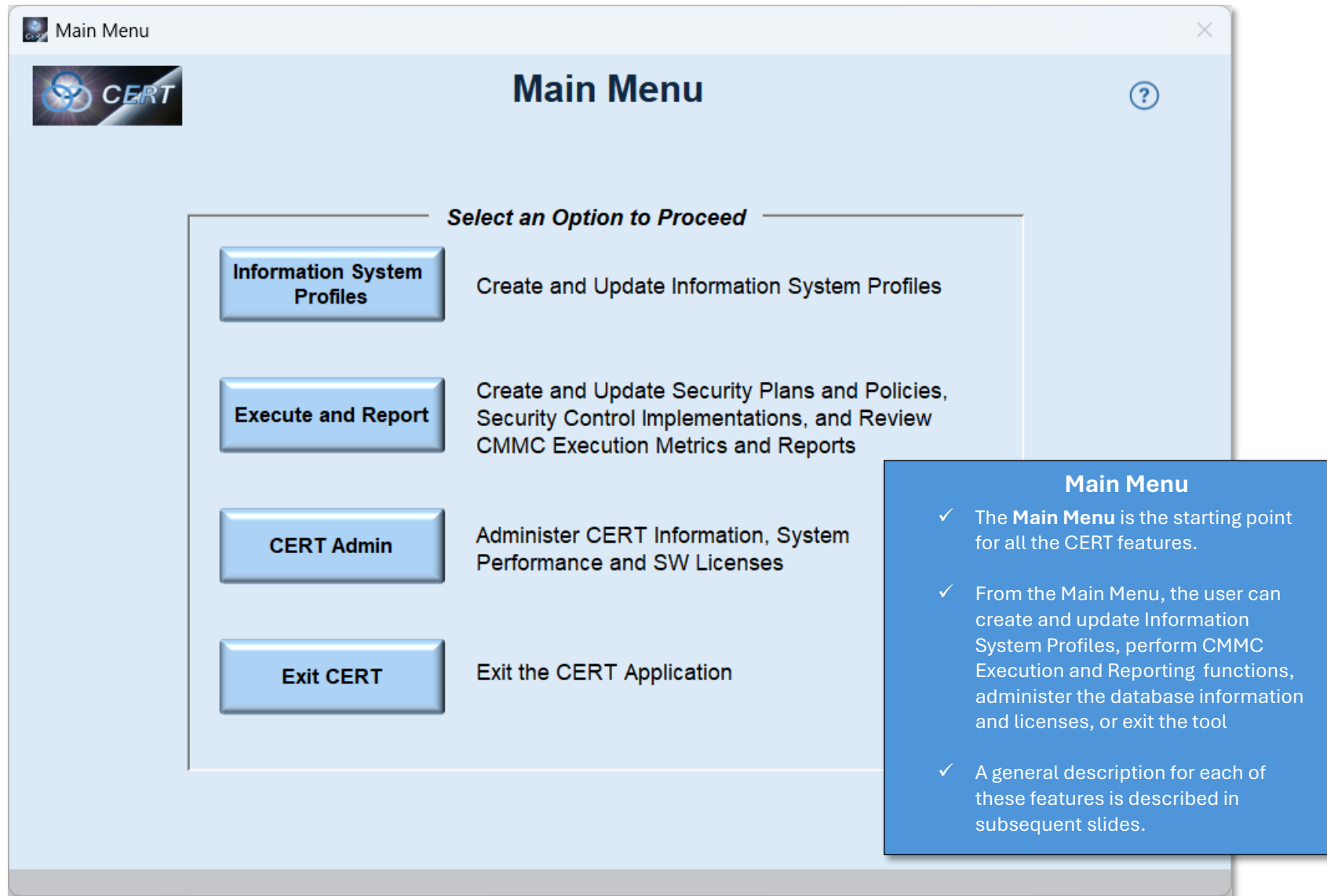
The Cybersecurity Maturity Model Certification (CMMC) Execution & Reporting Tool (CERT), V2.0, is an affordable, all-in-one, stand-alone software application to facilitate compliance with CMMC requirements.

- The CERT was specifically designed to assist cybersecurity and IT professionals who are tasked to implement and track CMMC regulatory compliance for small to mid-sized businesses.
- The CERT user license is *perpetual* and *portable*: meaning no annual renewal fees and the licensed user can host on multiple devices.
- The CERT manages system profiles and key stakeholders; documents security control implementations; creates and tracks plans of action and milestones; and provides real-time CMMC performance metrics.
- The CERT produces System Security Plans, Security Policies, POAM Reports, Supplier Performance Risk System (SPRS) report inputs, and captures and catalogs artifacts/evidence to support certification assessments.

The following slides illustrate and describe several CERT V2.0 forms, features and outputs.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

System Profiles



System Profiles

?

System Name: *

Mission System Planner

CMMC Level 1, *

2 or 3:

2

CAGE Code:

11234

Generate Requirements

* Minimum Items needed to Generate Requirements

System Profile Enabled:

☒

System Description:

The Mission System Planner (MSP) information system (MSPIS) is used by the DarkRock Corporation to develop, test and deliver MSP products to the US Army. The MSPIS stores, processes and transmits Controlled Unclassified Information (CUI) as design and performance requirements provided by the US Army program office. The MSPIS external interfaces are to/from the US Army program office and DarkRock suppliers utilizing the US Army secure web portal and encrypted email.

System and Assessment Scope

Enclave: ☒ Enterprise: ☐

Enclave

Approximate Numbers of Users

Non-Privileged:

50

Privileged:

CUI Categories:

CTI

System Security Plan:

☒

Version:

Unique Identification (UID):

CUI Description:

The Mission System Planner (MSP) information system (MSPIS) stores, processes and transmits CTI in the form of customer provided requirements; generated technical specifications, detailed software design documentation, test plans and reports, and; periodic engineering and contract management and status reports. The DarkRock Corp shares CTI with the US Army customer program office and suppliers via an encrypted portal for storage and transmission. At this time, the US Army program office requires CMMC Level-2

Key Stakeholders and Contact Info

	Responsible Organization	Information Owner	System Owner	Security Office
Name	DarkRock Corporation	Col Hugh Darnell	Frank Meyer	Ralph Jones
Title		Director, MSP Program	CEO, DarkRock Corp	Chief of Security
Address	12 Buklmyshuse Ct., Eugene	200 Platoon Lvl Dr., Camp I	12 Buklmyshuse Ct., Eugene	12 Buklmyshuse
Phone	(211) 765-4321	(211) 123-4567	(211) 765-4321	(211) 765-4322
Email		hugh.darnell@usarmy.mil	frank.meyer@darkRock.cor	ralph.jones@dar

Return to Main Menu

Previous Profile

Next Profile

Add a New Profile

Information System Profiles

- ✓ The **System Profiles** form is used to establish and manage multiple Information System Profiles and to generate CMMC requirements.
- ✓ The form has two main sections: (1) System Identification and (2) Key Stakeholders and Contact Info.
- ✓ The System Identification section is used to describe the system, scope, and information, and to generate CMMC Requirements, enable or disable a system profile
- ✓ The Key Stakeholders and Contact Info section is used to capture the necessary organization, information, system and security points of contact information.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

The screenshot shows the 'Execute and Report' window of the CERT V2.0 tool. The window has a title bar 'Execute and Report' with a close button. Below the title bar is the CERT logo and a help icon. The main content area features a dropdown menu labeled 'Select System from Dropdown List:' with 'Mission System Planner' selected. Below this is a 'Menu Selection' section containing seven buttons, each with a description: 'System Security Plan' (Create or Update the System Security Plan), 'Security Policies' (Create System Security Policies), 'Security Controls' (Execute and Assess Security Control Implementations), 'POAM' (Manage Plan of Action and Milestones), 'Attachments/Artifacts' (Export List of System Attachments/Artifacts), 'Execution Metrics' (View Current CMMC Execution Metrics), and 'SPRS' (Export a Supplier Performance Risk System Report). At the bottom left is a 'Return to Main Menu' button.

Execute and Report

Select System from Dropdown List: **Mission System Planner**

Menu Selection

System Security Plan	Create or Update the System Security Plan
Security Policies	Create System Security Policies
Security Controls	Execute and Assess Security Control Implementations
POAM	Manage Plan of Action and Milestones
Attachments/Artifacts	Export List of System Attachments/Artifacts
Execution Metrics	View Current CMMC Execution Metrics
SPRS	Export a Supplier Performance Risk System Report

Return to Main Menu

- Execute and Report**
- ✓ The **Execute and Report** form is the entry point for performing CERT security functions/tasks for individual Systems.
 - ✓ The user first selects a system from the dropdown list. The drop-down list will only include System Profiles which have been created, have requirements generated, and are enabled.
 - ✓ After a system profile is selected from the drop-down list, the user can then execute CERT security functions by selecting any of the *Menu Selection* options listed.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

Mission System Planner (System Security Plan)	Mission System Planner (System Security Plan)	Mission System Planner (System Security Plan)
System Security Plan for the: Mission System Planner Information System Commercial and Government Entity (CAGE) Code: 11234 <u>Organization</u> DarkRock Corporation 12 Buklmyshuse Ct., Eugene OR 45678 <u>System Contact Information</u> Name: Frank Meyer Phone: (211) 765-4321 Email: frank.meyer@darkRock.com	Table of Contents 1. System Identification.....4 1.1 System Name/Title: Mission System Planner4 1.1.1 System Categorization: Moderate Impact for Confidentiality4 1.1.2 System Unique Identifier: TBD4 1.2 Responsible Organization:4 1.2.1 Information Owner:4 1.2.2 System Owner:4 1.2.3 System Security Officer:4 1.3 System Purpose and Description:5 1.3.1 System Users:5 1.4 General Description of Information:5 2. System Environment6 2.1 System Hardware:6 2.2 System Software:6 2.3 Network Topology:6 2.4 Hardware and Software Ownership and Maintenance:6 3. Requirements7 3.1 Access Control.....7 3.2 Awareness and Training12 3.3 Audit and Accountability.....13 3.4 Configuration Management15 3.5 Identification and Authentication17 3.6 Incident Response19 3.7 Maintenance.....20 3.8 Media Protection21 3.9 Personnel Security23	3.12 Security Assessment26 3.13 System and Communications Protection.....27 3.14 System and Information Integrity31 4. Record of Changes34

Execute and Report

- ✓ Selecting the *System Security Plan* (SSP) option from the Execute and Report form creates or updates an SSP based upon the system profile selected from the Execute and Report form.
- ✓ The contents of the SSP include the latest profile description and stakeholder information stored, the complete list of security requirements based on CMMC level, the current state of control implementations and supporting rationale, and any reference made to supporting attachments.
- ✓ The SSP title page and table of contents above illustrate the format and level of detail of the CERT generated SSP. Section 3 - Requirements includes the stated requirement text, Implementation Status (i.e., Implemented, Plan to be Implemented, or Not Applicable), and implementation details and supporting rationale.
- ✓ SSPs is created using MS Word and are stored on the local device within the applicable system profile's attachment folder.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

Information System Security Access Control Policy for the Mission System Planner 1. Purpose The purpose of this policy is to establish access control requirements for the Mission System Planner, hereinafter referred to as the "System", to protect Controlled Unclassified Information (CUI) and other sensitive data from unauthorized access, disclosure, alteration, or destruction. This policy ensures that access to system resources, data, and functions is granted only to authorized users, devices, and processes based on their role and the principle of least privilege. It aims to promote accountability, integrity, and confidentiality in all operations that interact with the System. The following paragraphs define the scope, roles and responsibilities, enforcement, and review and maintenance of this policy. 2. Scope This policy applies to all personnel and systems associated with the System, including Management, Engineering, Security, Information Technology (IT), and Users who manage, operate, or utilize communication systems and services. The policy also extends to contractors or third-party entities (e.g., managed service providers) with access to this System. This policy encompasses all components of the System, including networked servers, workstations, mobile devices, cloud services, storage devices, and remote access infrastructure that store, process or transmit CUI. 3. Roles and Responsibilities a. Management:	(1) Approves access control procedures and allocates resources for their implementation. (2) Ensures separation of duties among personnel to prevent collusion. (3) Approve and disseminate policy updates and ensure training for all affected personnel. b. Engineering and IT Personnel: (1) Implement technical controls including encryption, session locks, automatic logoff, and monitoring systems. (2) Restricts privileged functions to authorized administrators and ensure that all privileged activities are logged and auditable. (3) Manages remote and wireless access through approved, encrypted, and authenticated channels. c. Security: (1) Maintains overall accountability for this policy. (2) Ensures this policy aligns with organizational and regulatory requirements. (3) Leads periodic review and updates to this policy. (4) Monitors access logs, investigate suspicious or unauthorized activity, and enforce corrective actions. (5) Conduct periodic access reviews and ensure compliance with least privilege principles. (6) Oversee protection of CUI in mobile, remote, and external environments. d. System Users: (1) Use only assigned credentials and non-privileged accounts for standard operations. (2) Protect access tokens, passwords, and mobile devices against unauthorized use. (3) Immediately report lost credentials, suspicious access attempts, or violations of this policy. 4. Enforcement Violations of this policy may result in disciplinary action up to and including termination of employment, revocation of system privileges, and/or legal action	privilege misuse, or failure to protect CUI may be held accountable in accordance with organizational and regulatory standards. 5. Review and Maintenance This policy shall be reviewed annually or whenever significant changes occur to System, regulatory requirements, or organizational structure. The Information Security Officer, in collaboration with the IT, Engineering, and Management teams, is responsible for ensuring that the policy remains current, effective, and aligned with industry best practices and compliance requirements. 6. Version Control <table><thead><tr><th>Version</th><th>Date</th><th>Description</th></tr></thead><tbody><tr><td>New</td><td>4/30/2026</td><td>Initial release of the Access Control Policy.</td></tr></tbody></table>	Version	Date	Description	New	4/30/2026	Initial release of the Access Control Policy.
Version	Date	Description						
New	4/30/2026	Initial release of the Access Control Policy.						

Execute and Report

- ✓ Selecting the *Security Policies* option from the Execute and Report form allows the user to create individual Security Policies for any of the 14 Control Families. The example above is an Access Control Policy.
- ✓ Each policy contains a Purpose, Scope, Roles and Responsibilities, Enforcement, and a Review and Maintenance section which are uniquely based on CMMC assessment requirements and objective outcomes. The responsibility roles (i.e. Management, Engineering/IT, Security and System Users) are typical based on experience in the field.
- ✓ Security policies are created in MS Word format and will be saved in the "Attachments" folder where they can be further tailored to unique Information System, CMMC Level, and Organizational Roles and Responsibilities. Furthermore, the policies can (and should be) referenced by the applicable security control

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

Security Controls: Mission System Planner

Family: Access Control Assessment Identifier: 3.1.2 Control: Transaction & Functional Control [FCI/CUI Data] Weight: 5

Assessment Requirement: Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Security Requirement: [View Source Requirement](#)

Assessment Objectives:

Determine if...	Add a POAM?
3.1.2[a] the types of transactions and functions that authorized users are permitted to execute are defined	☐
3.1.2[b] system access is limited to the defined types of transactions and functions for authorized users.	☐

Security Control Implementation:

Select Implementation Result

Met: ☒ Not Met: ☐ Not Applicable: ☐

Enter Implementation Details and Supporting Rationale
(Respond to each of the referenced Assessment Objectives)

[a] The types of transaction and functions authorized users are permitted to execute (privileged and non-privileged), are documented in the Mission System Planner (MSP) user access request forms and are approved by management prior to granting access to the MSP information system. These forms are used by and maintained by IT department as source evidence.

[b] System access is limited to the defined types of transactions and functions for authorized users by users in their account profiles which grant read, write, and/or execute permissions based upon the user's group roles. User groups are also part of the MSP user access request forms, implemented in user/group profiles and accounts by IT personnel.

Supporting Evidence/Artifacts (Add/Modify/Delete): [Attachments](#)

Controls Met (99 of 110)

Filter Requirements

☐ Met ☐ Not Met ☐ Not Assessed

☐ Not Applicable ☒ All (No Filter)

Arrow Down to View/Select

- 3.1.1 Authorized Access Control [FCI/CUI Data]
- 3.1.2 Transaction & Functional Control [FCI/CUI Data]
- 3.1.3 Control CUI Flow
- 3.1.4 Separation of Duties
- 3.1.5 Least Privilege
- 3.1.6 Non-Privileged Account Use
- 3.1.7 Privileged Functions
- 3.1.8 Unsuccessful Logon Attempts
- 3.1.9 Privacy & Security Notices
- 3.1.10 Session Lock
- 3.1.11 Session Termination
- 3.1.12 Control Remote Access
- 3.1.13 Remote Access Confidentiality
- 3.1.14 Remote Access Routing
- 3.1.15 Privileged Remote Access
- 3.1.16 Wireless Access Authorization
- 3.1.17 Wireless Access Protection
- 3.1.18 Mobile Device Connection
- 3.1.19 Encrypt CUI on Mobile
- 3.1.20 External Connections [FCI/CUI Data]
- 3.1.21 Portable Storage Use
- 3.1.22 Control Public Information [FCI/CUI Data]
- 3.2.1 Role-Based Risk Awareness
- 3.2.2 Role-Based Training
- 3.2.3 Insider Threat Awareness
- 3.3.1 System Auditing
- 3.3.2 User Accountability
- 3.3.3 Event Review
- 3.3.4 Audit Failure Alerting
- 3.3.5 Audit Correlation

[Return to Execute and Report](#) [Assessment Methods](#) (Examine Interview Test) [Previous](#) [Next](#)

The Security Controls form includes all the assessment objectives associated with that security control. If the user determines an objective is not met, a POAM item can be initiated by clicking on the Add a POAM radio button.

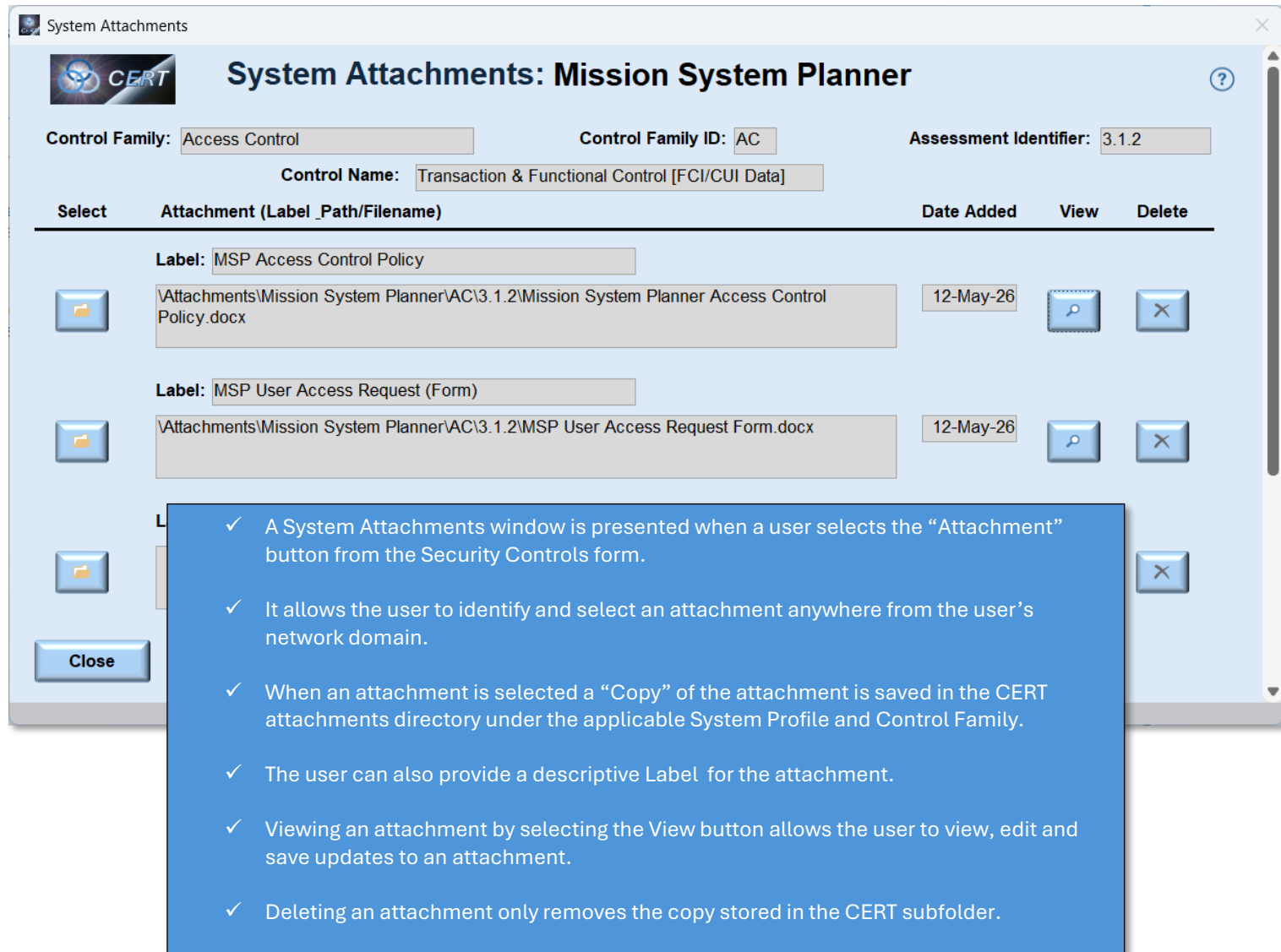
POAM Requirement follow rules outlined in 32 CFR 170.21

Execute and Report

- ✓ Selecting the *Security Controls* option from the Execute and Report form allows the user to enter implementation details, and to assess and record whether a control is met, not met or not applicable.
- ✓ Quick links to CMMC Assessment Methods and Source Requirements are provided for user reference.
- ✓ User can navigate between controls using either the Previous and Next buttons or by selecting controls from filtered list.
- ✓ Supporting Evidence/Artifacts associated with a control can be added as Attachments which can also be modified or deleted which is illustrated below.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



System Attachments: Mission System Planner

Control Family: Access Control Control Family ID: AC Assessment Identifier: 3.1.2

Control Name: Transaction & Functional Control [FCI/CUI Data]

Select	Attachment (Label_Path/Filename)	Date Added	View	Delete
	Label: MSP Access Control Policy Attachments\Mission System Planner\AC\3.1.2\Mission System Planner Access Control Policy.docx	12-May-26		
	Label: MSP User Access Request (Form) Attachments\Mission System Planner\AC\3.1.2\MSP User Access Request Form.docx	12-May-26		
				

Close

- ✓ A System Attachments window is presented when a user selects the “Attachment” button from the Security Controls form.
- ✓ It allows the user to identify and select an attachment anywhere from the user’s network domain.
- ✓ When an attachment is selected a “Copy” of the attachment is saved in the CERT attachments directory under the applicable System Profile and Control Family.
- ✓ The user can also provide a descriptive Label for the attachment.
- ✓ Viewing an attachment by selecting the View button allows the user to view, edit and save updates to an attachment.
- ✓ Deleting an attachment only removes the copy stored in the CERT subfolder.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



Plan of Action and Milestones: Mission System Planner

Assessment Objective: 3.1.1[c]

Current Status: Complete

Objective Reference:

Determine if devices (including other systems) authorized to connect to the system are identified.

Weakness Description:

An external hard-drive on one workstation is not specifically authorized to connect to the system

Remediation Plan:

Determine if the device should be authorized to connect to the system. If the device should be authorized, then update authorized HW list; otherwise, disconnect the device.

Milestone(s):

1 - 10/02/25: Determine if the external hard drive should be authorized. (completed)
2 - 10/10/25 Either disconnect the device, or follow change management procedures to add the device to the authorized inventory. (should be)

Assigned/POC:

Information Technology Team/Jeff Contreras

Resources Required:

Engineering change and CM approval - 8 hrs

Target Completion Date:

10/13/2025

Actual Completion Date:

10/10/2025

Select POAM Status:

Initiated: ☒ Open: ☒ In Work: ☒ Complete: ☒

Set POAM Filter

☐ Open ☐ In Work ☐ Complete
☐ Initiated ☒ All (No Filter)

Arrow Down to View/Select

Control | Date Initiated | Status

3.1.1[c]	9/22/2025	Complete
3.1.1[f]	5/5/2026	Initiated
3.1.5[b]	3/26/2026	Open
3.1.5[c]	3/26/2026	In Work
3.13.11[a]	9/30/2025	Complete
3.3.2[b]	2/19/2026	Initiated
3.8.7[a]	4/9/2026	Open

Execute and Report

- ✓ Selecting the *POAM* option from the Execute and Report form allows the user to manage all the POAM items associated with any System Profile.
- ✓ The form allows POAM item details to be entered, and status updated as POAM items are worked.
- ✓ POAM items are tracked from initiation to closure.
- ✓ A POAM Report can be generated and exported from this form, which includes ALL POAMs in their current state of completion (as illustrated next).

Previous

Next

Return to Execute and Report

Export POAM Report

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

Plan of Action and Milestones (POAM)										
Mission System Planner										
System Owner: Frank Meyer								POAM Date: 5/12/2026		
Control Reference	Reference Objective	Weakness Description	Date Discovered	Remediation Plan	Milestones	Required Resources	Assigned POC	Target Completion	POAM Status	Actual Completion
3.1.1[c]	Determine if devices (including other systems) authorized to connect to the system are identified.	An external hard-drive on one workstation is not specifically authorized to connect to the system	9/22/2025	Determine if the device should be authorized to connect to the system. If the device should be authorized, then update authorized HW list; otherwise, disconnect the device.	1 - 10/02/25: Determine if the external hard drive should be authorized. (completed) 2 - 10/10/25 Either disconnect the device, or follow change management procedures to add the device to the authorized inventory. (should be added to auth HW list) 3 - 10/13/25: Verify all actions were taken. All actions were completed on 10/10/25 - The device was removed.	Engineering change and CM approval - 8 hrs	Information Technology Team/Jeff Contreras	10/13/2025	Complete	10/10/2025
3.13.11[a]	Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI. NOTE: Subtract 5 points if no cryptography is employed; 3 points if mostly not FIPS validated	A non FIPS validated encryption solution is currently being used to protect the confidentiality of CUI.	9/30/2025	Replace the Mission System Planner encryption solution with a FIPS validated cryptography	1. (2 Nov 25): Identify viable FIPS-140 encryption solutions and perform trade study to determine optimal product. Consider effectivity, integration, maintenance, compatibility and cost. 2 - (10 Dec 25): Present recommendation to change management to obtain necessary technical, cost and schedule approvals. 3 - (9 Jan 26): Complete installation and checkout of the FIPS-140 encryption solution.	Trade Study - 32 hrs Engineering change and CM approval - 8 hrs Estimate Implementation cost - 40 hrs Estimate Hardware/Software costs - \$25K/Year	Information Technology Team/Jeff Contreras	1/9/2026	Complete	12/25/2025
3.3.2[b]	Determine if audit records, once created, contain the defined content.	Audit records created do not contain content user actions.	2/19/2026	✓ Example export of a POAM Report. ✓ POAMs exports are saved and stored in the CERT Attachments folder with the most recent/up-to-date status of all POAM records. ✓ The format used is consistent with industry standards and includes all the necessary data items to support Level-2 and Level-3 CMMC					Initiated	
3.1.5[c]	Determine if security functions are identified.	Security functions are not identified in writing	3/26/2026						In Work	

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

System Attachment List Mission System Planner

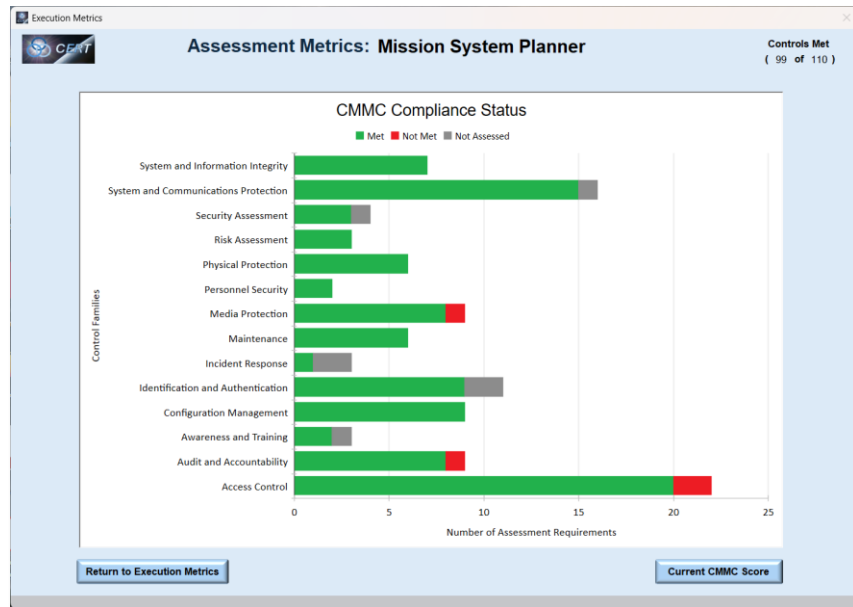
Family:	Access Control	Control:	Transaction & Functional Control [FCI/CUI Dat	Requirement:	3.1.2
CERT Path:	Attachments\Mission System Planner\AC\3.1.2\Mission System Planner Access Control Policy.docx			Title:	MSP Access Control Policy
Family:	Access Control	Control:	Authorized Access Control [FCI/CUI Data]	Requirement:	3.1.1
CERT Path:	Attachments\Mission System Planner\AC\3.1.1\RE POAM Closure Verification - Mission System Planner - 3.1.1c.msg			Title:	POAM Closure Verification 3.1.1.c
Family:	Access Control	Control:	Transaction & Functional Control [FCI/CUI Dat	Requirement:	3.1.2
CERT Path:	Attachments\Mission System Planner\AC\3.1.2\MSP User Access Request Form.docx			Title:	MSP User Access Request (Form)
Family:	Access Control	Control:	Authorized Access Control [FCI/CUI Data]	Requirement:	3.1.1
CERT Path:	Attachments\Mission System Planner\AC\3.1.1\Mission System Planner Access Control Policy.docx			Title:	Access Control Policy
Family:	Audit and Accountability	Control:	System Auditing		
CERT Path:	Attachments\Mission System Planner\AU\3.3.1\Mission System Planner Audit and Accountability Policy.docx				
Family:	Awareness and Training	Control:	Role-Based Risk A		
CERT Path:	Attachments\Mission System Planner\AT\3.2.1\Mission System Planner Awareness Training Policy.docx				

Execute and Report

- ✓ Selecting the *Attachment/Artifacts* menu option exports a list of all attachments added during security control assessments.
- ✓ This list includes the Family, Control Name, Requirement, CERT Path (local) and Title
- ✓ The attachment list sorted by security control Family, which is particularly useful to the CCA and C3PAO during audit activities.
- ✓ The export list is stored as a PDF file and will always include the latest information.

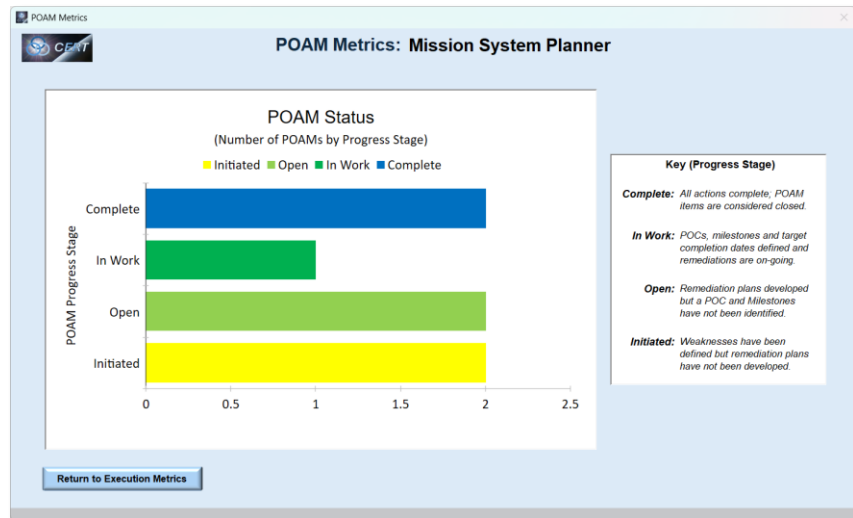
CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



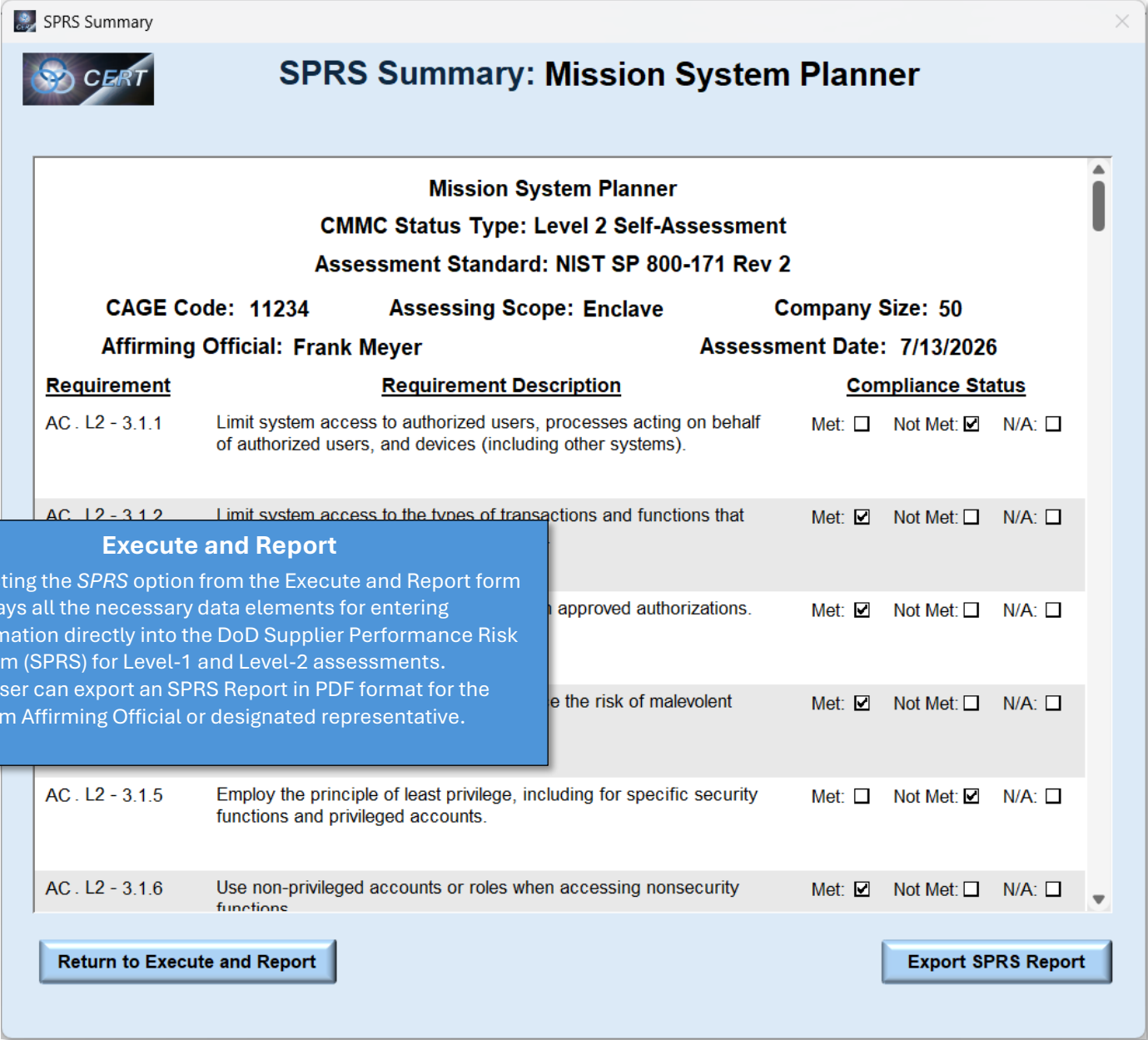
Execute and Report

- ✓ Selecting the *Execution Metrics* menu option from the Execute and Report form allows the user to choose Assessment Metrics or POAM Metrics.
- ✓ The **Assessment Metric** displays a bar chart showing the compliance status (met, not met, not assessed) by control family and allows the user to calculate a point-in-time CMMC assessment score.
- ✓ The **POAM Metric** shows numbers of POAM items in the current state (Progression), which is particularly helpful to help prioritize remediations
- ✓ Both metrics are based upon the latest security control assessment and POAM information stored in the CERT.



CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



The screenshot shows the 'SPRS Summary' window of the CMMC Execution & Reporting Tool (CERT) V2.0. The window title is 'SPRS Summary'. Inside, there's a header with the CERT logo and the title 'SPRS Summary: Mission System Planner'. Below this, the 'Mission System Planner' section displays the following information: CMMC Status Type: Level 2 Self-Assessment, Assessment Standard: NIST SP 800-171 Rev 2, CAGE Code: 11234, Assessing Scope: Enclave, Company Size: 50, Affirming Official: Frank Meyer, and Assessment Date: 7/13/2026. A table follows with three columns: Requirement, Requirement Description, and Compliance Status. The table lists several requirements, including AC.L2-3.1.1, AC.L2-3.1.2, AC.L2-3.1.5, and AC.L2-3.1.6. The compliance status for each requirement is shown as 'Met: [checkbox]', 'Not Met: [checkbox]', and 'N/A: [checkbox]'. A blue callout box on the left side of the table provides instructions on how to use the 'Execute and Report' button. At the bottom of the window, there are two buttons: 'Return to Execute and Report' and 'Export SPRS Report'.

SPRS Summary: Mission System Planner

Mission System Planner
CMMC Status Type: Level 2 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

CAGE Code: 11234 Assessing Scope: Enclave Company Size: 50
Affirming Official: Frank Meyer Assessment Date: 7/13/2026

<u>Requirement</u>	<u>Requirement Description</u>	<u>Compliance Status</u>
AC.L2-3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Met: ☐ Not Met: ☒ N/A: ☐
AC.L2-3.1.2	Limit system access to the types of transactions and functions that	Met: ☒ Not Met: ☐ N/A: ☐
	approved authorizations.	Met: ☒ Not Met: ☐ N/A: ☐
	the risk of malevolent	Met: ☒ Not Met: ☐ N/A: ☐
AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Met: ☐ Not Met: ☒ N/A: ☐
AC.L2-3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	Met: ☒ Not Met: ☐ N/A: ☐

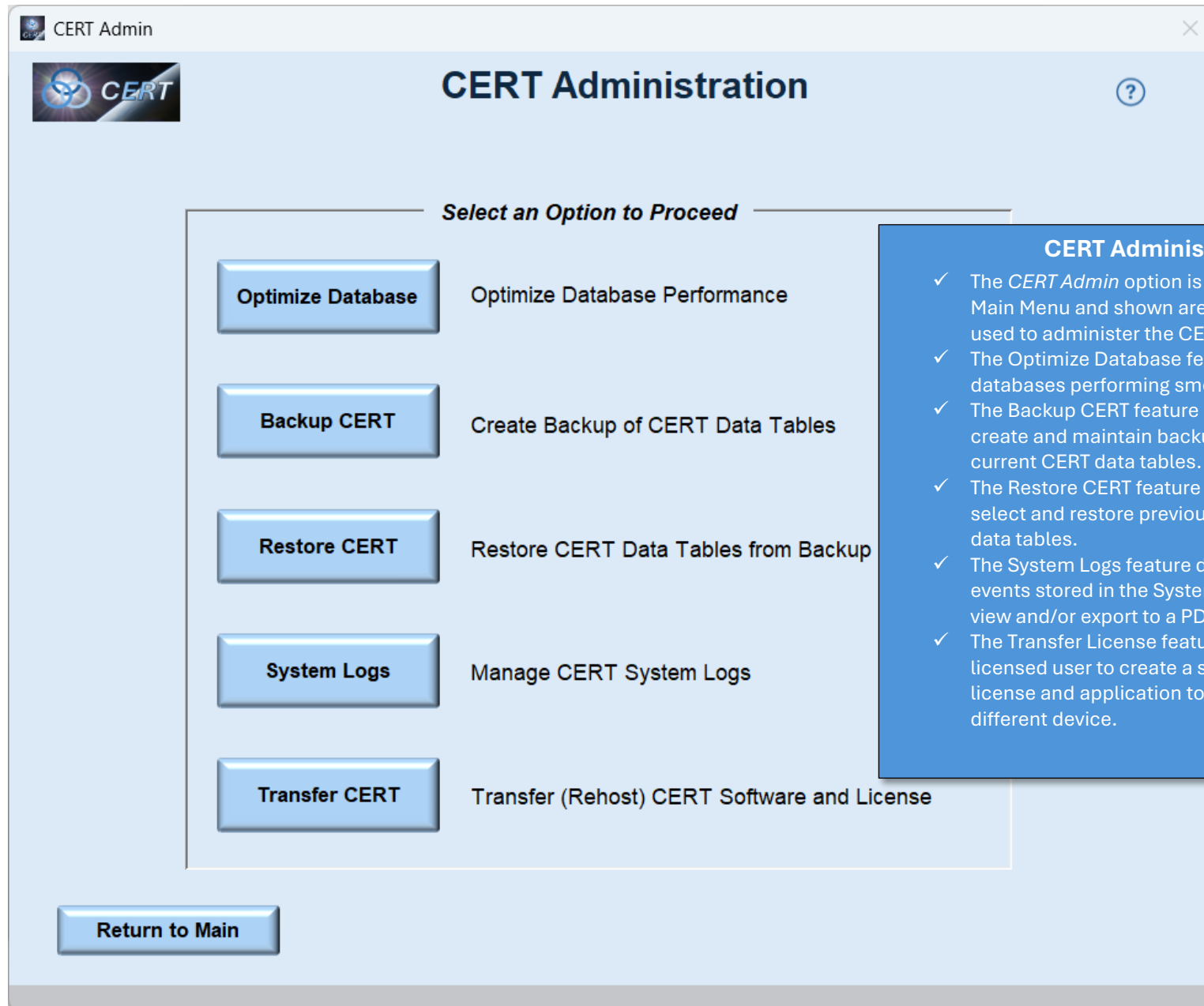
Execute and Report

- ✓ Selecting the *SPRS* option from the Execute and Report form displays all the necessary data elements for entering information directly into the DoD Supplier Performance Risk System (SPRS) for Level-1 and Level-2 assessments.
- ✓ The user can export an SPRS Report in PDF format for the system Affirming Official or designated representative.

Return to Execute and Report **Export SPRS Report**

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview



CERT Administration

- ✓ The *CERT Admin* option is accessed from the Main Menu and shown are several features used to administer the CERT.
- ✓ The Optimize Database feature helps to keep databases performing smoothly.
- ✓ The Backup CERT feature allows the user to create and maintain backup copies of all current CERT data tables.
- ✓ The Restore CERT feature allows the user to select and restore previously backed up CERT data tables.
- ✓ The System Logs feature displays all the CERT events stored in the System Log. The user can view and/or export to a PDF file.
- ✓ The Transfer License feature allows the licensed user to create a separate CERT license and application to be hosted on a different device.

CMMC Execution & Reporting Tool (CERT) V2.0

Product Overview

To purchase CERT V2.0 license, go to:

<https://cyber3po.com/shop/ols/products/cmmc-execution-and-reporting-tool-cert-version-20>

For additional information or to schedule a **FREE CERT V2.0 Demo**, contact us at:

<https://cyber3po.com/contact>