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.

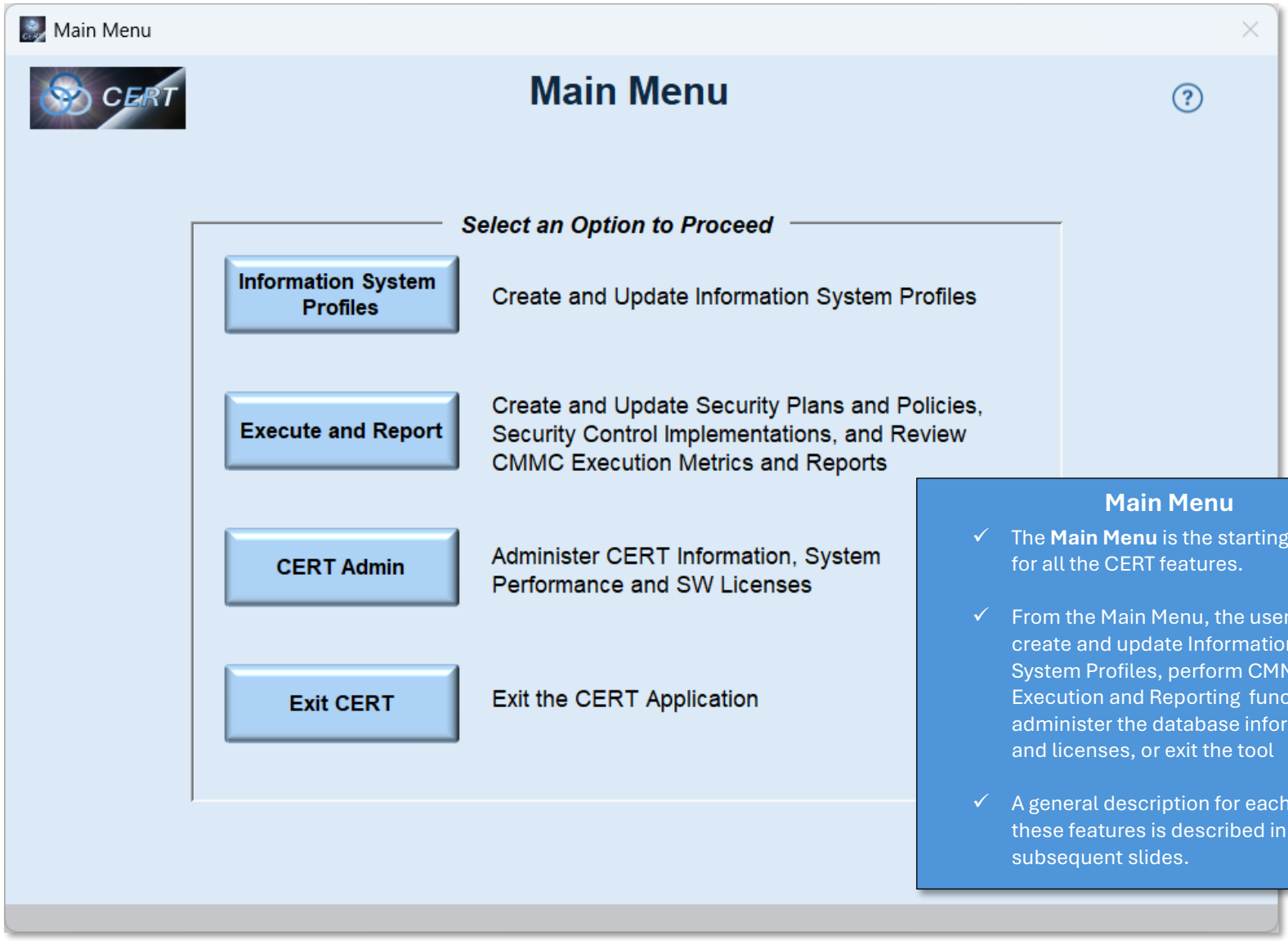
- The CERT user license is *perpetual* and *portable*: meaning no annual renewal fees and the licensed user can host on multiple devices.

- 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

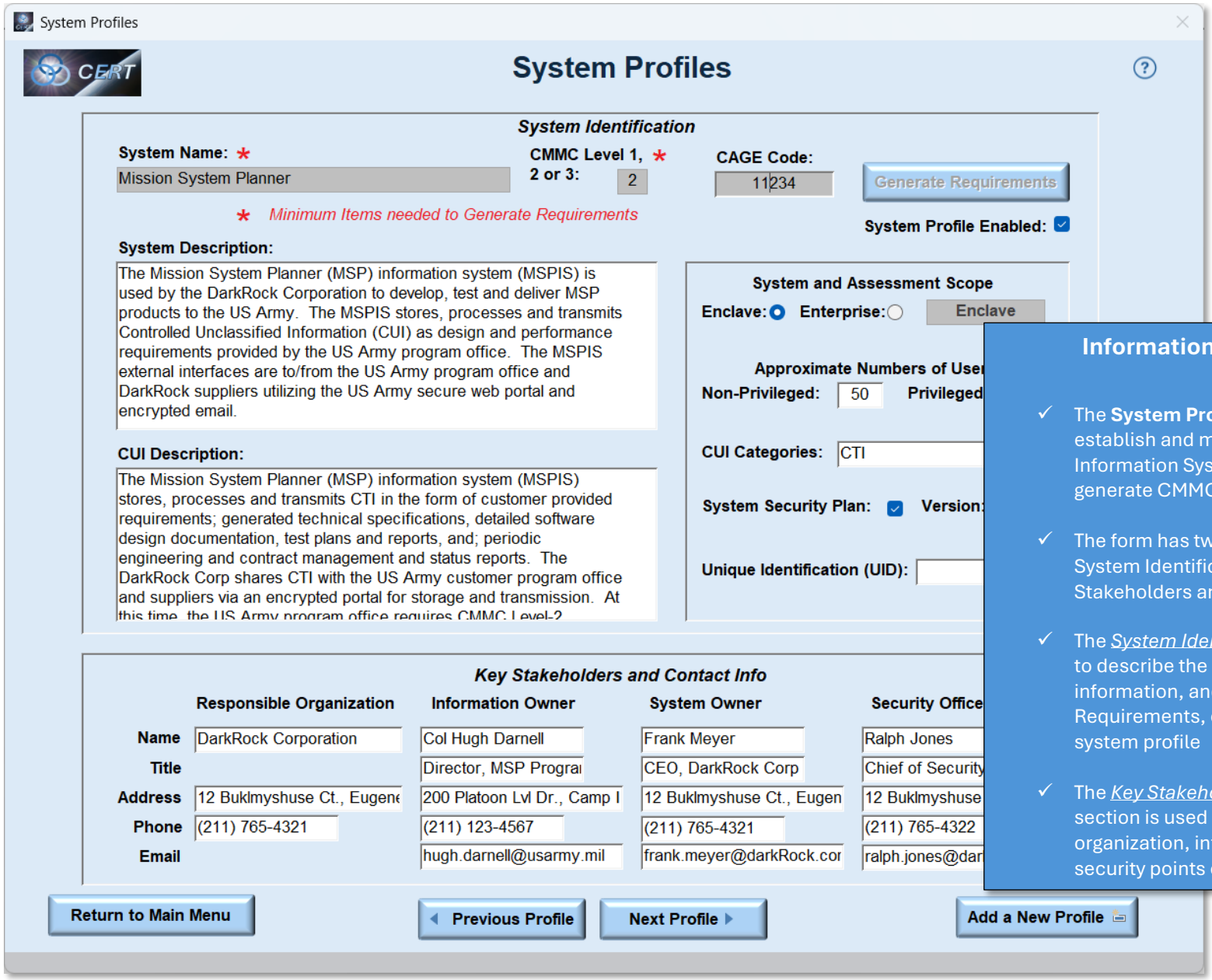


Main Menu

- ✓ The **Main Menu** is the starting point for all the CERT features.
- ✓ From the Main Menu, the user can create and update Information System Profiles, perform CMMC Execution and Reporting functions, administer the database information and licenses, or exit the tool
- ✓ A general description for each of these features is described in subsequent slides.

CMMC Execution & Reporting Tool (CERT) V2.0

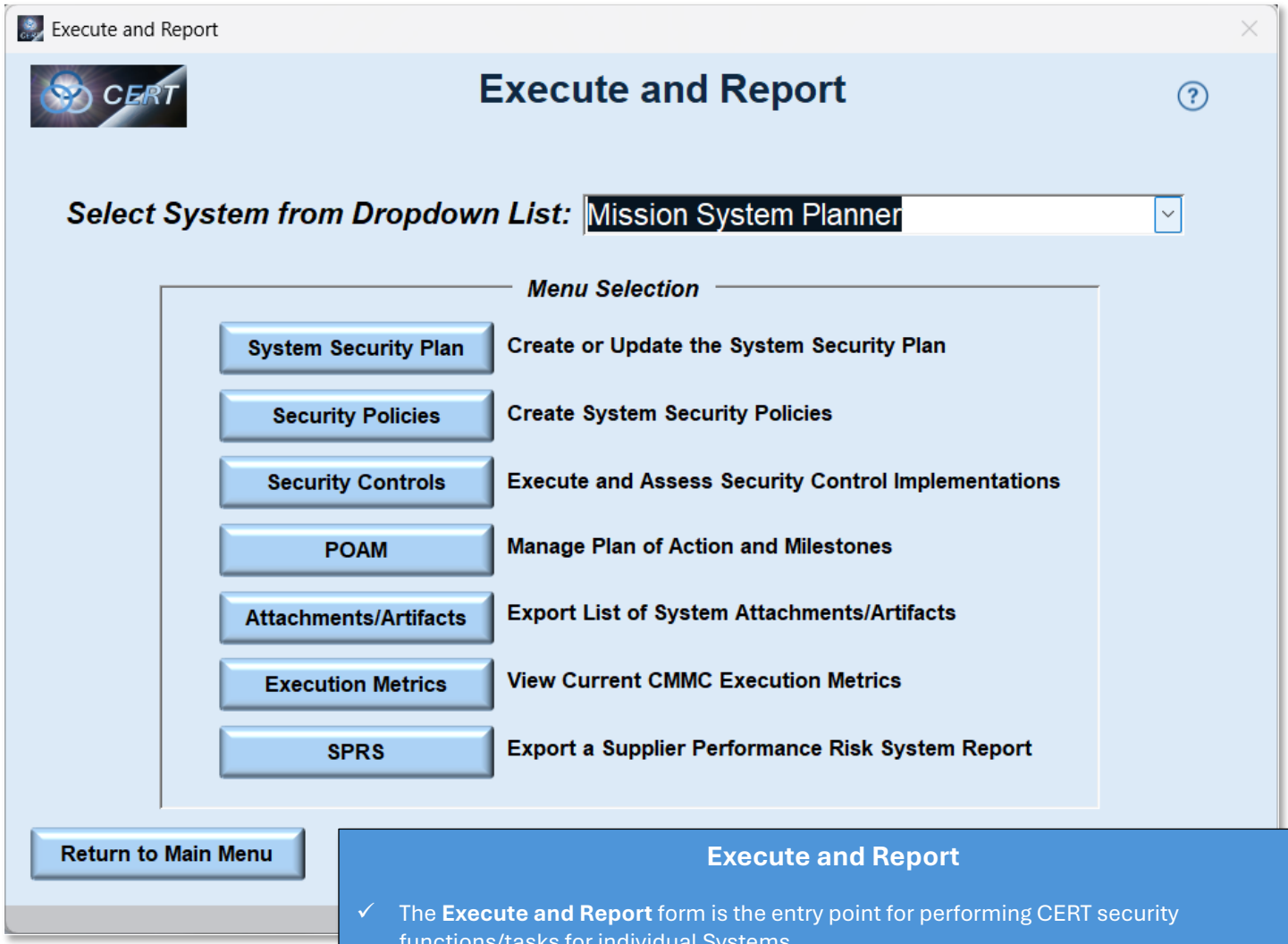
Product Overview



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

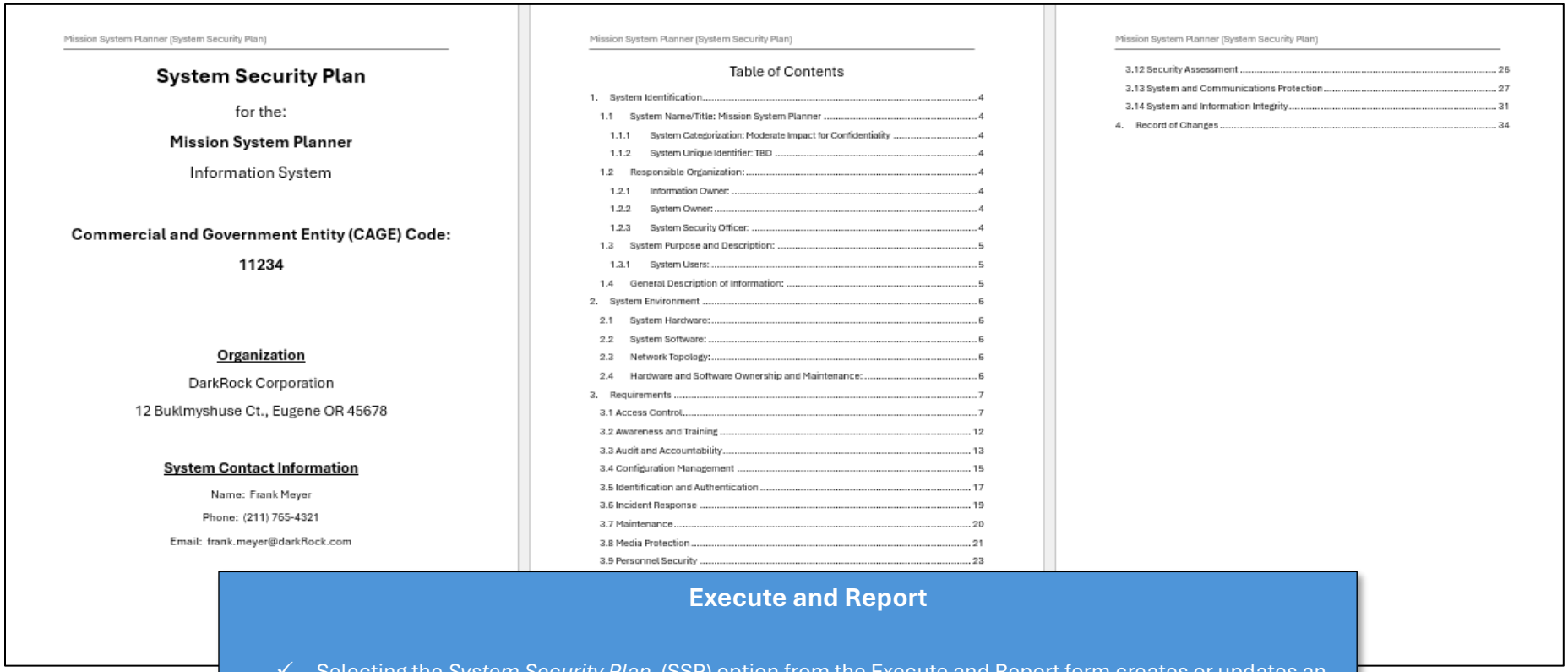


Execute and Report

- ✓ 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)

System Security Plan

for the:

Mission System Planner

Information System

Commercial and Government Entity (CAGE) Code:

11234

Organization

DarkRock Corporation

12 Buklmyshuse Ct., Eugene OR 45678

System Contact Information

Name: Frank Meyer

Phone: (211) 765-4321

Email: frank.meyer@darkRock.com

Mission System Planner (System Security Plan)

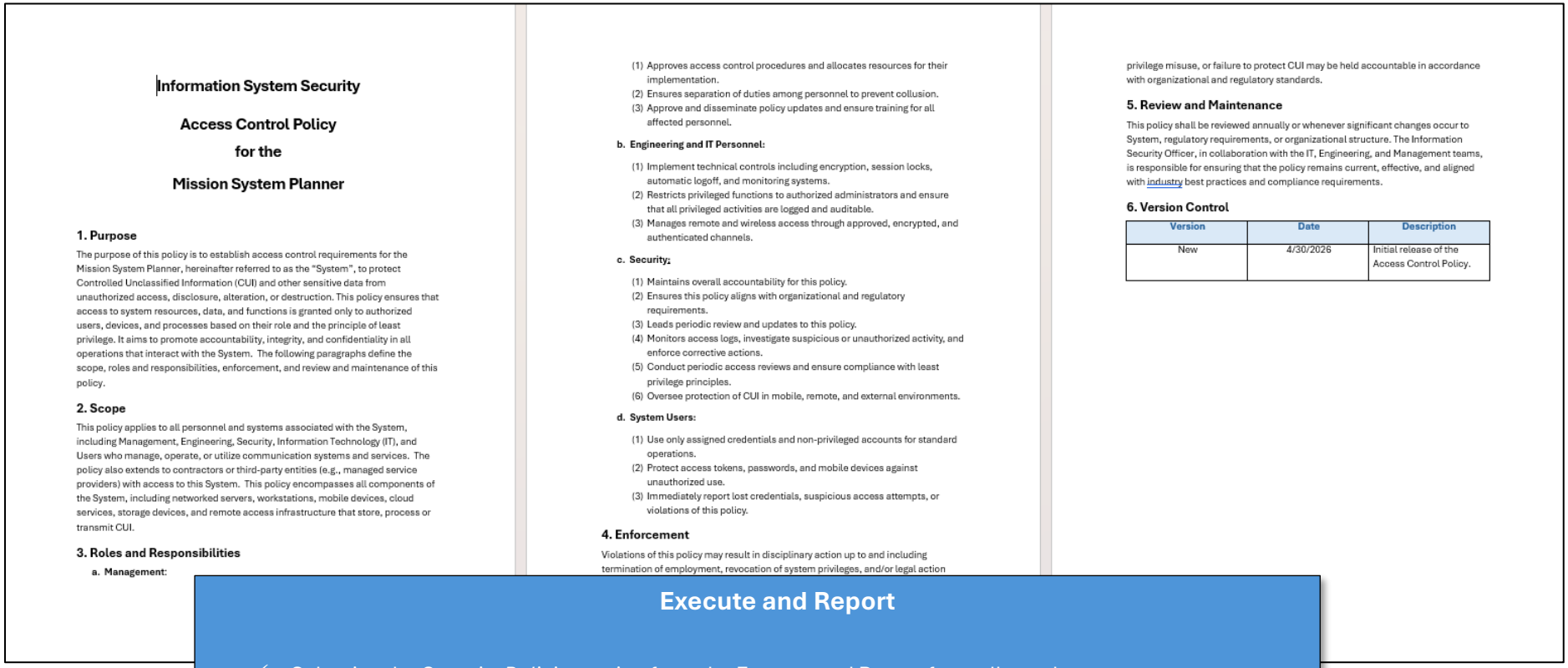
Table of Contents

Mission System Planner (System Security Plan)

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.

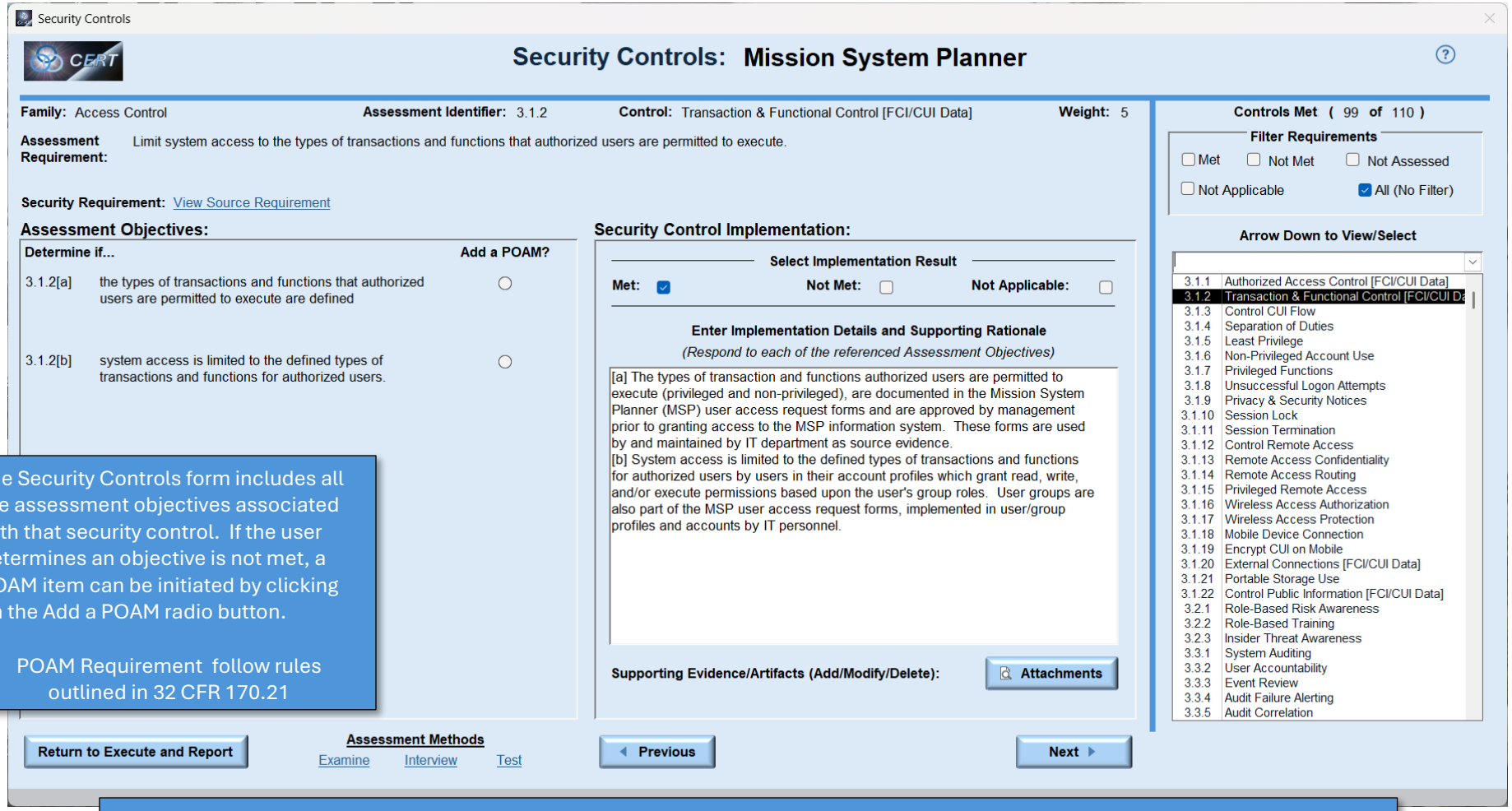
6. Version Control

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 polices can (and should be) referenced by the applicable security control

CMMC Execution & Reporting Tool (CERT) V2.0
Product Overview



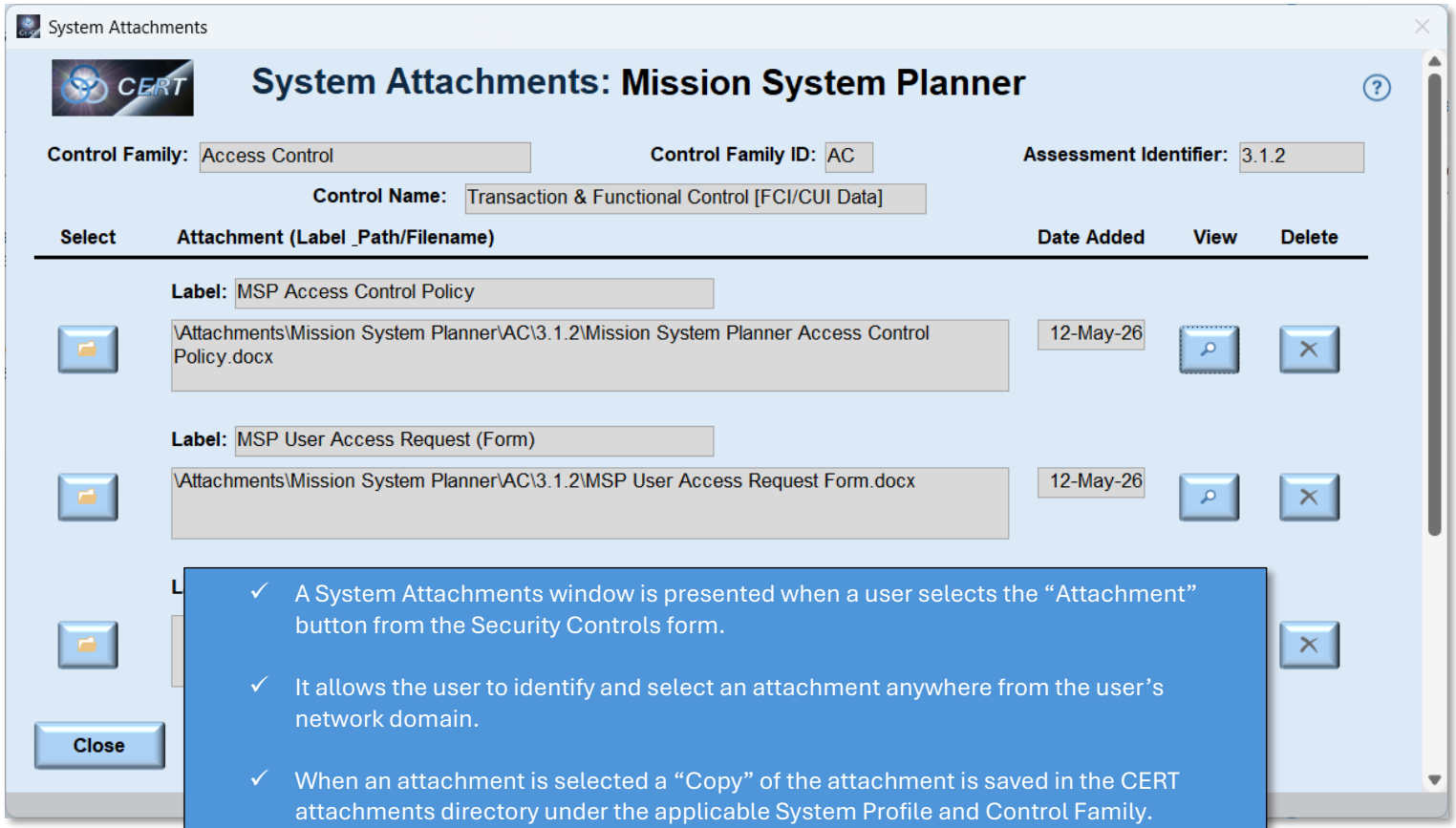
The Security Controls form includes all the assessment objectives associated with that security control. If the user determines an objective is not met, a POAM item can be initiated by clicking on the Add a POAM radio button.

POAM Requirement follow rules outlined in 32 CFR 170.21

Execute and Report

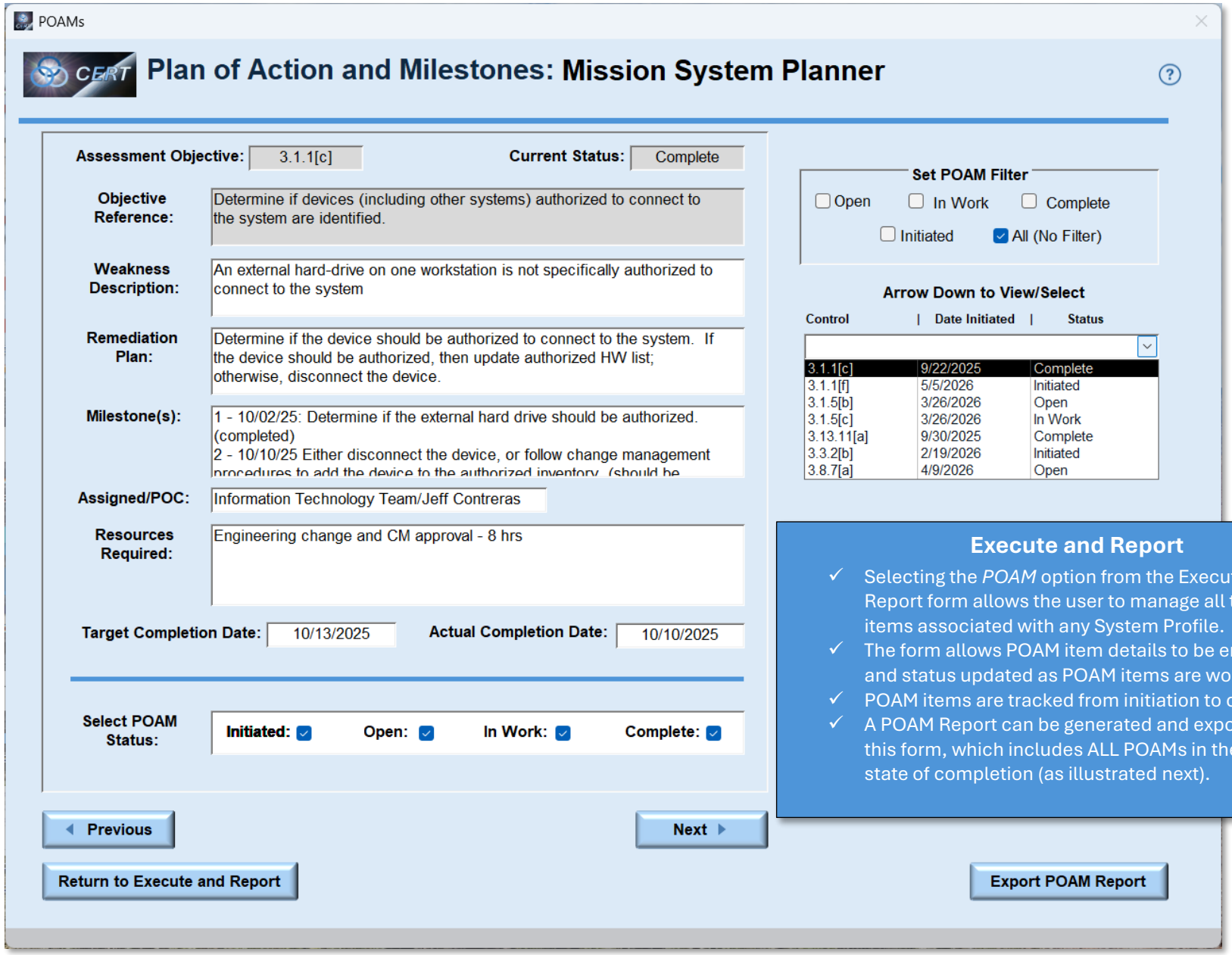
- ✓ Selecting the *Security Controls* option from the Execute and Report form allows the user to enter implementation details, and to assess and record whether a control is met, not met or not applicable.
- ✓ Quick links to CMMC Assessment Methods and Source Requirements are provided for user reference.
- ✓ 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



- ✓ 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



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).

CMMC Execution & Reporting Tool (CERT) V2.0
Product Overview

Plan of Action and Milestones (POAM)

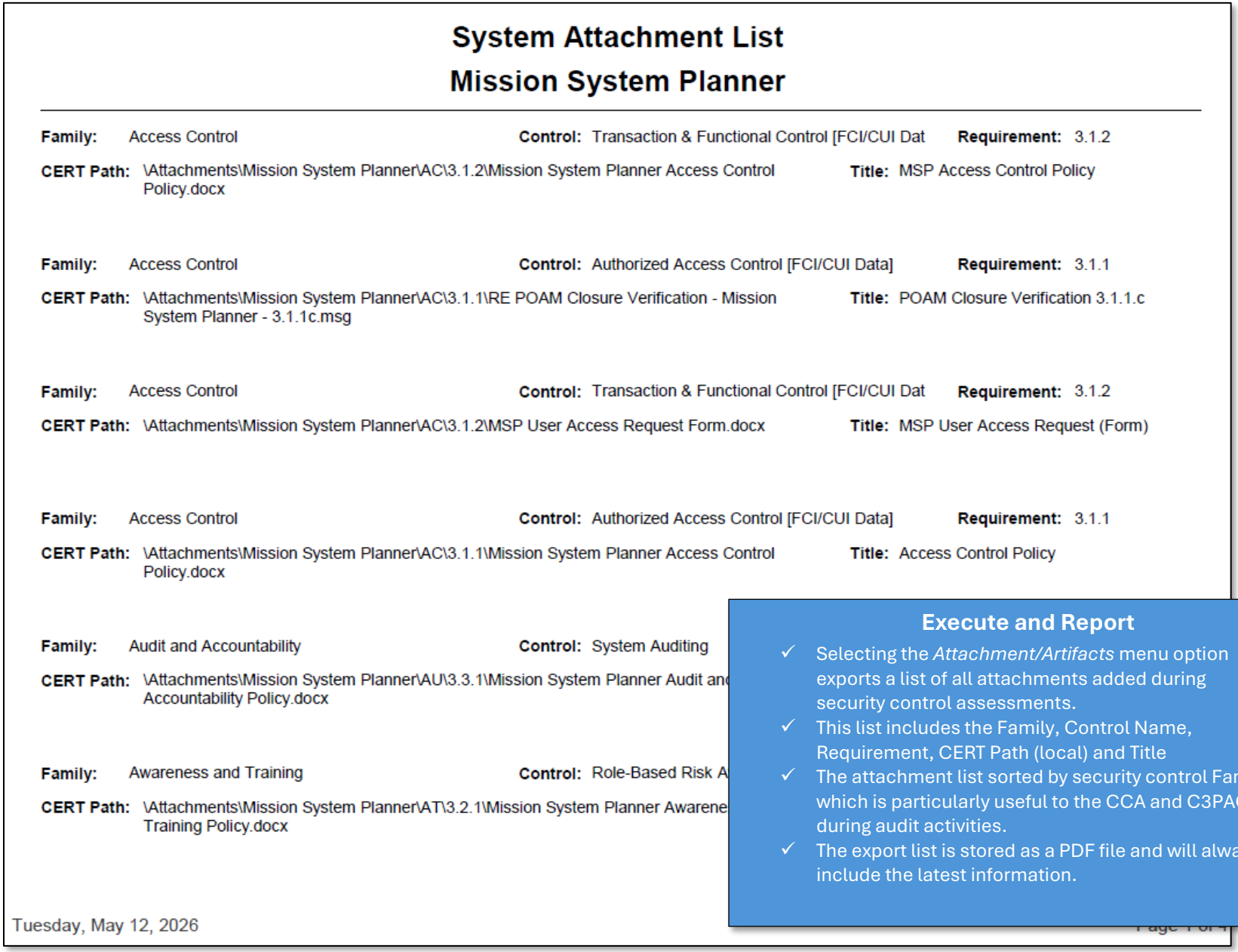
Mission System Planner

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]	Deterime if audit records, once created, contain the defined content.	Audit records created do not contain content user actions.	2/19/2026						Initiated	
3.1.5[c]	Deterime if security functions are identified.	Security functions are not identified in writing	3/26/2026						In Work	

- ✓ 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 assessments and certifications.
- ✓ Exports are created in PDF and provide supporting evidence to satisfy security control 3.12.2

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 an Accountability Policy.docx

Family: Awareness and Training **Control:** Role-Based Risk A

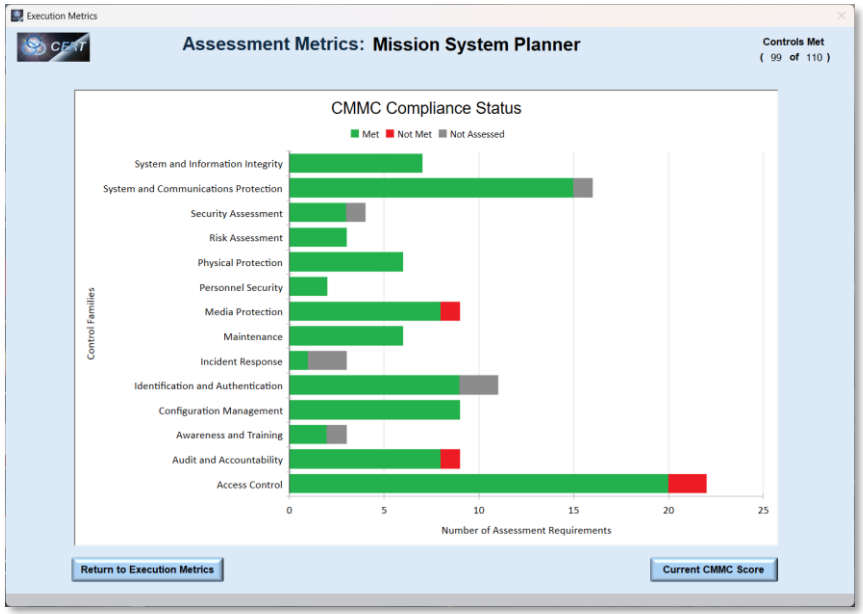
CERT Path: \Attachments\Mission System Planner\AT\3.2.1\Mission System Planner Awarene Training Policy.docx

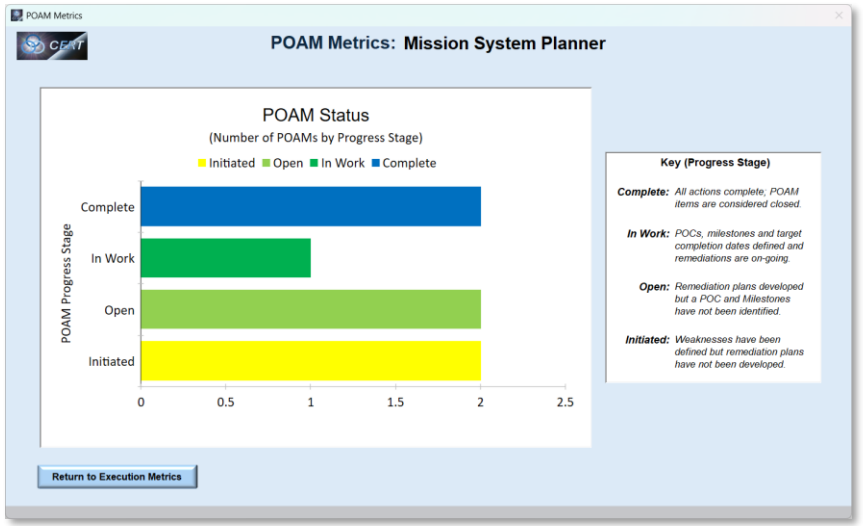
Tuesday, May 12, 2026

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

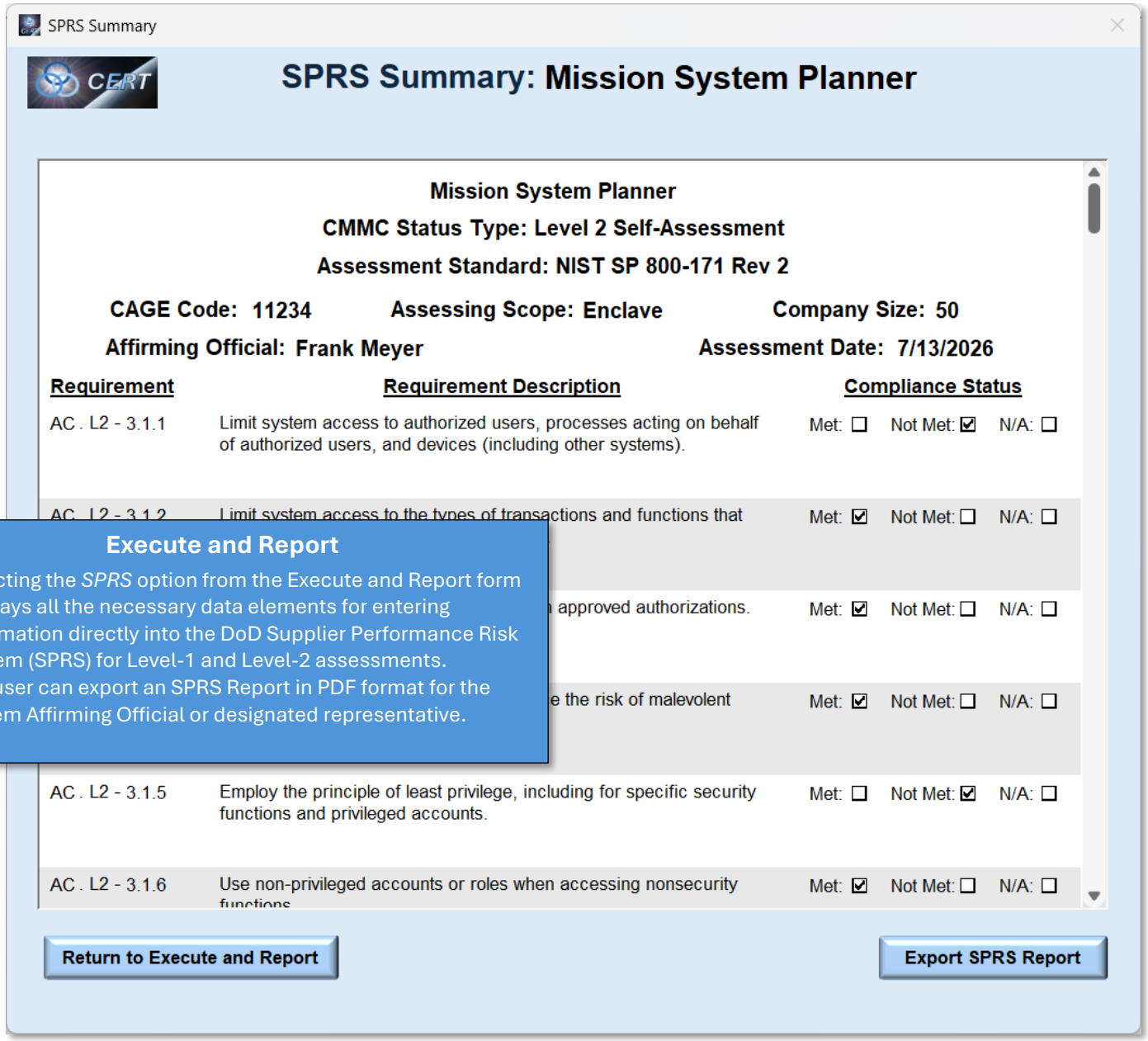




Execute and Report

- ✓ 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.

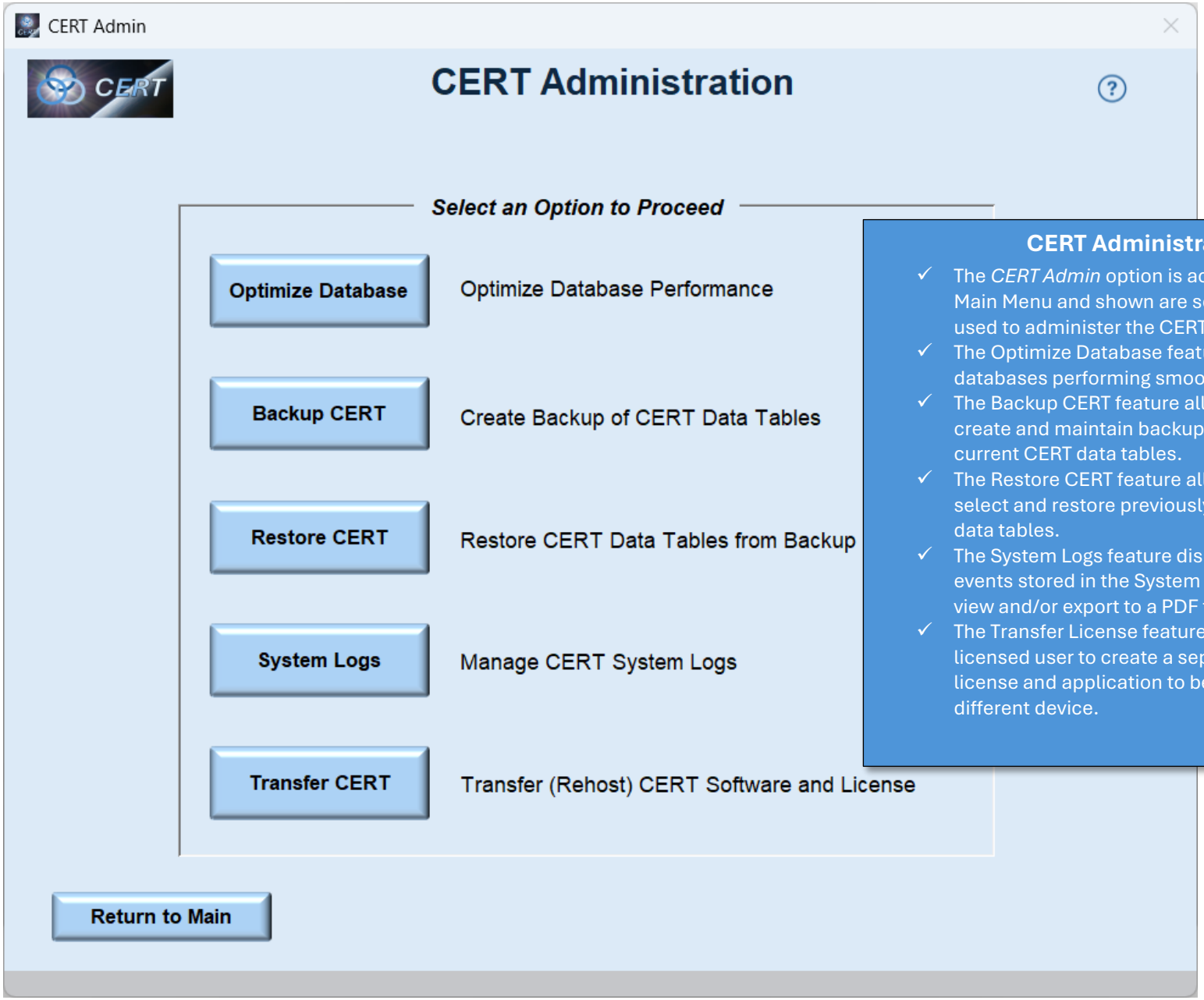
CMMC Execution & Reporting Tool (CERT) V2.0
Product Overview



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.

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