ESTCP

FINAL REPORT

Risk Management Framework Self-Assessment Tool (RSAT) Technology Transfer

Aura Lee Keating
S&C Electric Company

Joseph Bush
US Army Engineer Research & Development Center Construction Engineering Research Laboratory (ERDC-CERL)

October 2023

ESTCP Project EW21-5184

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
31/10/2023	ESTCP Final Report	1/6/2022 - 1/31/2024

4. TITLE AND SUBTITLE

Risk Management Framework Self-Assessment Tool (RSAT) Technology Transfer

5a. CONTRACT NUMBER
22-C-0009

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Aura Lee Keating
S&C Electric Company

Joseph Bush
US Army Engineer Research & Development Center Construction Engineering Research Laboratory (ERDC-CERL)

5d. PROJECT NUMBER
EW21-5184

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
S&C Electric Company
CMR 480 Box 552
APO, NY 09128

CEERD-CERL
P.O. Box 9005
2902 Newmark Dr.
Champaign, IL 61826-9005

8. PERFORMING ORGANIZATION REPORT NUMBER
18194

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Deputy Assistant Secretary of Defense (Energy Resilience & Optimization)
3500 Defense Pentagon, RM 5C646
Washington, DC 20301-3500

10. SPONSOR/MONITOR'S ACRONYM(S)
ESTCP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
EW21-5184

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Cybersecurity Submittal Automation Tool (CySAT) Tool supports Government and Industry stakeholders involved in the Facility Related Control System (FRCS) cybersecurity design requirements and Risk Management Framework (RMF) processes through automation of FRCS Cybersecurity Unified Facility Criteria (UFC) 4-010-06 and RMF Enterprise Mission Assurance Support Service (eMASS) submittals. CySAT has the following features:

- Design Phase Control Set Automation: generates tailored (with overlays and tailoring options) control and control correlation indicator (CCI) lists as draft UFC Basis of Design and Concept Design Submittals.
- RMF/eMASS Artifact Automation: facilitates security categorization and auto-populates the Control Information and Test Results forms in eMASS-importable formats to provide initial tailoring of control and CCI sets with overlays, inheritance, and other options.

Targeted user groups

15. SUBJECT TERMS
Facility Related Control System; Cybersecurity Unified Facility Criteria; Risk Management Framework

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Aura Lee Keating
UNCLASS	UNCLASS	UNCLASS	UNCLASS	41	19b. TELEPHONE NUMBER *(Include area code)* 405-294-3566

FINAL REPORT
Project: EW21-B1-5184

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (Continued)

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

ACRONYMS AND ABBREVIATIONS

APR	Army Policy Record
ATO	Authority to Operate
CAC	Common Access Card
CCI	Control Correlation Identifier
CERL	Construction Engineering Research Laboratory
CIA	Confidentiality – Integrity -Availability
CySAT	Cybersecurity Submittal Automation Tool
DoD	Department of Defense
DoN	Department of Navy
DoR	Designer of Record
eMASS	Enterprise Mission Assurance Support Service
ERDC	Engineer Research and Development Center
ESTCP	Environmental Security Technology Certification Program
FRCS	Facility Related Control System
ICS	Industrial Control System
ISO	Information Security Officer
ISSM	Information Systems Security Manager
IT	Information Technology
NAVFAC	Naval Facilities Engineering Systems Command
RMF	Risk Management Framework
R-SAT	RMF Self-Assessment Tool
UFC	Unified Facilities Criteria (UFC 4-010-06)
USACE	United States Army Corps of Engineers

ACKNOWLEDGEMENTS

This work was supported by the U.S. Department of Defense Environmental Security Technology Certification Program under S&C Electric Project EW21-B1-5184. S&C Electric Company and ERDC-CERL are very thankful for the technical support provided by Naval Facilities Engineering Command (NAVFAC) and USACE Control System Cybersecurity Mandatory Center of Expertise (CSC-MCX) staff who consulted on this project.

ABSTRACT

INTRODUCTION AND OBJECTIVES

The Cybersecurity Submittal Automation Tool (CySAT) supports Government and Industry stakeholders involved in the Facility Related Control System (FRCS) cybersecurity design requirements and Risk Management Framework (RMF) processes. CySAT provides automation of FRCS Cybersecurity Unified Facility Criteria (UFC) 4-010-06 and RMF Enterprise Mission Assurance Support Service (eMASS) submittals, specifically:

- RMF Self-Assessment steps: CySAT builds on the previously developed R-SAT toolset to streamline the process for obtaining an Authority to Operate by aiding with RMF submittals in Steps 1-3.
- UFC Designer of Record (DoR) processes: CySAT facilitates the generation of UFC 4-010-06 cybersecurity submittals to describe the requirements for incorporating cybersecurity into the design of all FRCS which include a network.

The primary objective of CySAT is to incorporate the features of previously developed toolsets – the ESTCP-funded R-SAT and a USACE-funded DoR tool - into a single toolset and obtain Government sponsorship.

TECHNOLOGY DESCRIPTION

The functions of CySAT reside in macro-based Microsoft Excel worksheets with tabs that represent steps in the UFC and RMF processes. CySAT offers the following advantages:

- CySAT is free, requires no license fee, and utilizes common software (Microsoft Excel).
- CySAT does not require a government-issued computer or Common Access Card (CAC) to use. Users can prepare correctly formatted eMASS templates prior to system registration.
- CySAT provides a standard format for UFC submittals thereby reducing inconsistency and streamlining review.
- UFC and RMF documentation is populated with standard responses related to FRCS and DoD inheritance policy, providing cybersecurity professionals with a starting point for tailoring the selection and assessment of controls to system features.

PERFORMANCE AND COST ASSESSMENT

There are no costs to users for implementing CySAT. The performance assessment and demonstration provide evidence that CySAT is a useful toolset. ERDC-CERL intends to take ownership of CySAT and has accepted responsibility for continued maintenance. CySAT will be uploaded to the Whole Building Design Guide website for users to download. To further track usefulness, CySAT users will be required to provide demographic data and intended use at the time of download. This information will be used to further evaluate the cost/benefit of any required updates to CySAT (estimated at $70,000 per event) and prolonged support (estimated at $32,000 annually).

IMPLEMENTATION ISSUES

The software was designed to be intuitive and user friendly; however, users must invest upfront time in learning the software. Additionally, CySAT is an Excel worksheet with Visual Basic programing and some users may have concerns using a macro-enabled file. Finally, CySAT functionality may be impacted by updates to eMASS, or FRCS policy and maintenance will be required.

EXECUTIVE SUMMARY

INTRODUCTION

The Cybersecurity Submittal Automation Tool (CySAT) supports Government and Industry stakeholders involved in the Facility Related Control Systems (FRCS) cybersecurity design requirements and Risk Management Framework (RMF) processes. CySAT provides automation of Unified Facility Criteria (UFC) and RMF Enterprise Mission Assurance Support Service (eMASS) submittals, specifically:

- RMF Self-Assessment steps: RMF is the DoD process for applying cybersecurity to information technology (IT), including FRCS. CySAT builds on the previously developed R-SAT toolset to streamline the process for obtaining an Authority to Operate (ATO) by aiding with RMF submittals in Steps 1-3.
- UFC Designer of Record (DoR) processes: The UFC 4-010-06 describes requirements for incorporating cybersecurity into the design of all FRCS which include a network. CySAT facilitates the generation of cybersecurity submittals in the planning, design, construction, renovation, and repair of new and existing FRCS.

Within the DoD, there are an estimated 2.5 million unique control systems that are used in over 300,000 buildings. FRCS are a subset of control systems that are used to monitor and control equipment and systems (for example, building control systems, utility control systems, electronic security systems, and fire and life safety systems) and must be cybersecure. DoD system owners are frequently supported by industry contractors to meet cybersecurity requirements. Often, there are different contractors and Government reviewers for the FRCS design phase and RMF validation which culminate in the construction phase. Cyber security requirements may not flow from the design process to the RMF validation. In addition, several RMF resources are Common Access Card (CAC)-enabled. Non-DoD designers and cybersecurity contractors must obtain sponsorship to access to these resources from DoD components. CySAT is intended to address these limitations.

OBJECTIVES

CySAT will support Government and Industry stakeholders involved in the FRCS cybersecurity design and RMF processes with automation of the submission requirements. Targeted user groups include Industry stakeholders performing a supporting role in FRCS Cybersecurity; government Design and Construction stakeholders; and FRCS Information System Owners. The primary objective of CySAT is to incorporate the features of previously developed toolsets – the ESTCP funded R-SAT and the USACE funded DoR tool - into a single toolset and obtain Government sponsorship. Supporting objectives include:

- Evaluate and coordinate FRCS Cybersecurity guidance for posting to DoD portals
- Develop Service-specific versions to accommodate unique RMF processes and inheritance
- Identify and design value-added enhancements from the existing toolsets (R-SAT and DoR)
- Align CySAT with related DoD efforts (e.g., FRCS Design Specifications)

TECHNOLOGY DESCRIPTION

The functions of CySAT reside in a macro-based Microsoft Excel worksheets with tabs that represent steps in the UFC and RMF processes. Data from worksheets can be exported to satisfy UFC cybersecurity submittals and RMF artifacts. CySAT starts at a degree of technical readiness as a Microsoft Excel based toolset, utilizing conventional data transfer processes (export/import of CSV files), and integrating with existing DoD tools (eMASS). The CySAT worksheets and steps are graphically represented in the figure below.

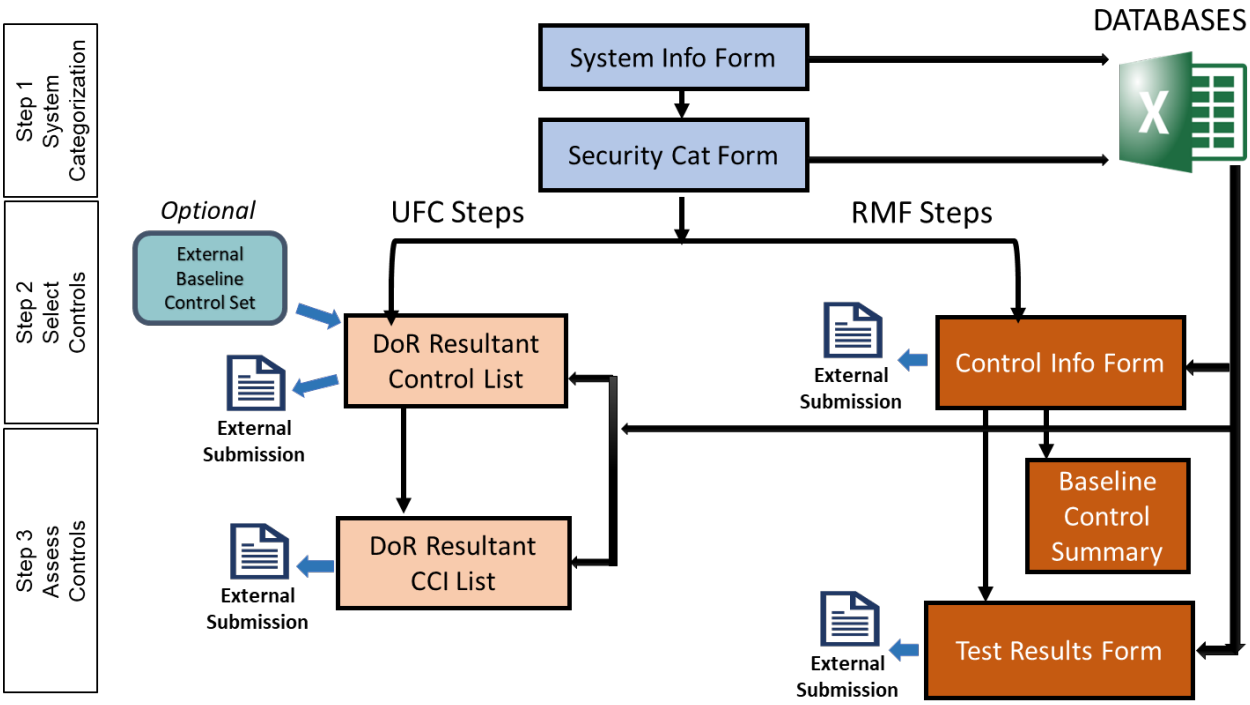

Figure ES-1. CySAT Overview of Features

Although there are alternative toolsets that allow the completion of the RMF self-assessment effort, none of the existing tools align with the UFC cyber security design process. CySAT offers the following advantages:

- CySAT is free, requires no license fee, and utilizes common software (Microsoft Excel).
- CySAT does not require a government issued computer or CAC to use. Users can prepare eMASS templates prior to system registration and without a government-issued computer or CAC.
- CySAT is a complement to the existing government-owned eMASS system and exported forms are compatible with the format that needs to be imported into eMASS.
- CySAT provides a standard format for UFC submittals thereby reducing inconsistency and streamlining review.
- UFC and RMF documentation is populated with standard responses related to FRCS and DoD inheritance policy, providing cybersecurity professionals with a starting point for tailoring the selection and assessment of controls to specific system features:

- CySAT generates a preliminary security categorization based on user selected FRCS System Type and populates information from service specific guidance and NIST special publications to streamline user tailoring.
- CySAT generates a control baseline specific to the security categorization. Users are able apply an overlay [Industrial Control System overlay or FRCS RMF Tag overlay] and/or tailoring features to modify this control baseline.
- CySAT provides users with service-specific inheritance and designer responsibility details, to assist in documenting how each control feature will be implemented in the design or addressed in the self-assessment process.

PERFORMANCE ASSESSMENT

The performance assessment focused on measuring CySAT's acceptance and value to FRCS stakeholders. A beta version of CySAT was tested between January and September of 2023 and improvements to the user interface and functional macros were made throughout the testing period. Testing consisted of operational testing and demonstrations. The objectives of the project were assessed using quantitative and qualitative performance metrics during the testing period:

- CySAT's capabilities were demonstrated to Industry Stakeholder to gauge the interest level of prospective users and to demonstrate the value of continued sustainment by the Government. This quantitative method used a simple measurement of number of requests for CySAT following demonstration to evaluate interest; CySAT was requested following 75% of the demonstrations. It is recognized that a request does not completely correlate to continued use; therefore, recorded comments during the demonstration are important data. Overall, users were impressed with CySAT's ability to streamline UFC and RMF steps and were eager to use CySAT. Based on the feedback, it is clear that there is interest in using CySAT's demonstrated features.
- User input without access to Government Systems was qualitatively assessed with operational testing. CySAT capability to generate correctly formatted RMF forms, suitable for import to eMASS, was evaluated. The generated RMF Forms were exported into external Control Information and Test Result Templates. These exports were then uploaded to the eMASS pilot site without error. This demonstrated that users without a CAC or laptop can generate and inform submittals and artifacts in usable formats for upload by Government representatives.
- CySAT capabilities were demonstrated to multiple Government Stakeholder to facilitate an agreement for technology transfer and ownership of CySAT. ERDC-CERL intends to take ownership of CySAT and accepted responsibility for continued maintenance. CySAT will be uploaded to wbdg.org for users to download. This is a web-based portal that provides government and industry practitioners with one-stop access to information on building-related guidance, criteria, and technology.

COST ASSESSMENT

CySAT will be free for public use and there are no costs for implementing the technology for users. The cost assessment focused on the cost to ERDC-CERL - and additional future Government sponsors - for ongoing maintenance or implementation of new features:

Maintenance of Current Features:

CySAT functionality relies on databases that incorporate control and Control Correlation Identifiers data from Federal Instructions. Some maintenance will be required to keep this data current when regulatory drivers are updated. It is estimated that 100 hours per year will be required to update data in existing databases, including validation, and testing of the updates. In addition, ERDC-CERL will provide an email contact to address user questions and comments related to the use of CySAT. A User Guide and Training Video were developed to minimize user questions and comments; however, an additional 60 hours per year will be allocated to account for user support. The cost to maintain CySAT's current functionality is estimated as $32,000 annually.

Additional Feature Implementation:

CySAT functionality relies on macros to apply user selections to populate worksheets with content from CySAT's integrated databases. It is assumed that some updates to CySAT may be required to keep in step with eMASS and RMF/UFC policy changes. The scope of labor hours for this effort is dependent on the scope of the changes required. By extrapolating the initial design phase labor hours, it is estimated that ~350 hours would be required update to identify, assess, and engineer any new CySAT logic at a cost of $70,000 per event.

IMPLEMENTATION ISSUES

The following implementation issues were identified during the development and demonstration of the toolset:

- CySAT utilizes Excel Visual Basic programming, and some users may have concerns with using a macro-enabled Excel document. Distributing MS Office documents with embedded macros can introduce some risk. Malicious code can reside within macros, so distributing CySAT via email should be avoided. This risk will be mitigated by allowing download of CySAT from the approved sites, such as the Whole Building Design Guide and ESTCP portals.
- CySAT is suitable for control systems of any impact rating, however HIGH Impact systems typically require customized requirements not addressed by CySAT. Auto-populated fields on CySAT forms are specific to control systems assigned a LOW or MODERATE impact level and significant tailoring for systems at HIGH impact levels will still be required.
- CySAT is a tool that requires a learning curve for users to understand the functionality and tailoring options. CySAT was designed to be intuitive and user friendly; however, users must be willing to invest upfront time in learning the applications. The User Guide and training video are intended to decrease the user's time to learn CySAT and minimize this risk. In addition, an ERDC-CERL monitored email contact will be provided to address user questions and comments related to the use of CySAT.
- CySAT functionality may be impacted by updates to the UFC, eMASS or FRCS policy and guidance. For example, security control categorization (CNSSI) and overlays (NIST 800-82 and FRCS RMF Tag) will need to be updated to reflect NIST 800-53r5 updates. Changes to CySAT databases and/or logic may also be necessary to keep pace with regulatory updates. ERDC-CERL intend to take ownership of CySAT and accept responsibility for the initial maintenance and user support. To download CySAT, users will be required to provide demographic data and intended application. This information will be used to evaluate the cost/benefit of any required updates to CySAT and prolonged support.

1.0 INTRODUCTION

This document describes the design and transition of the Cybersecurity Submittal Automation Tool (CySAT) for designers and owners of Department of Defense (DoD) Facility-Related Control System (FRCS). FRCS are a subset of control systems that are used to monitor and control equipment and systems related to DoD real property facilities (for example, building control systems, utility control systems, electronic security systems, and fire and life safety systems). CySAT facilitates the generation and completion of several cybersecurity submittals for:

- Risk Management Framework (RMF) Self-Assessment steps: RMF is the DoD process for applying cybersecurity to information technology (IT), including FRCS. CySAT builds on the previously developed R-SAT toolset to streamline the process for obtaining an Authority to Operate (ATO) by aiding with RMF submittals in Steps 1-3.
- Unified Facility Criteria (UFC) Designer of Record (DoR) processes: The UFC describes requirements for incorporating cybersecurity into the design of all FRCS which include a network. CySAT facilitates the generation of cybersecurity submittals in the planning and design of FRCS construction, renovation, and repair.

A representation of the complexity between the FRCS Design/Construction and RMF process, and feedback required from key stakeholders involved in the security assessment, is represented in Figure 1. CySAT provide these multiple stakeholders with a consistent process to document design and security related decisions.

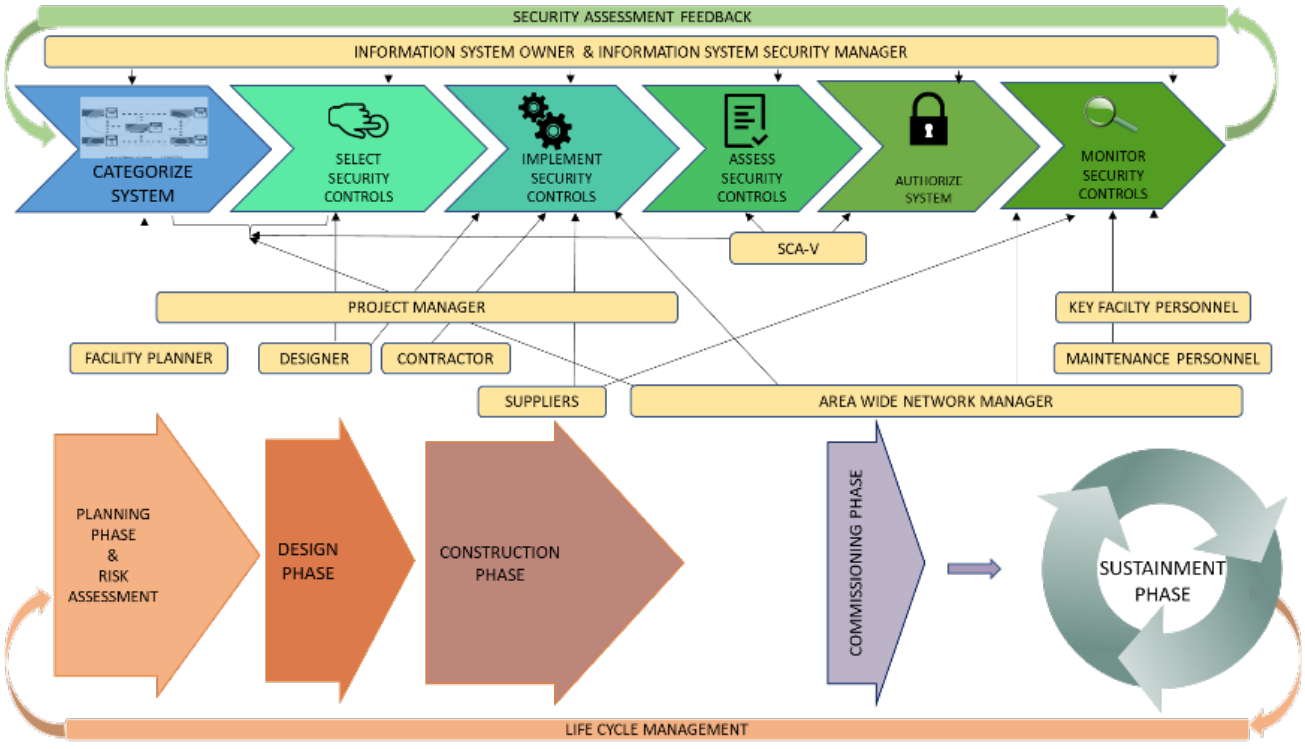

Figure 1. FRCS Cyber Security Design/Construction and RMF Process

1.1 BACKGROUND

Within the DoD, there are an estimated 2.5 million unique control systems that are used in over 300,000 buildings (each building may have 5-20 subsystems such as HVAC, lighting, fire, etc.) [Ref (p)]. One of the most common barriers faced by installations in adopting innovative technologies is the time and cost to meet the cybersecurity requirements and obtain an ATO. DoD system owners are frequently supported by industry contractors to meet cybersecurity requirements. Several RMF resources are Common Access Card (CAC)-enabled. Examples include the RMF Knowledge Service [Ref (q)] and the Enterprise Mission Assurance Support Service (eMASS). Non-DoD designers and cybersecurity contractors must obtain access to these resources from DoD components.

In 2019, the Environmental Security Technology Certification Program (ESTCP) invested in "Facility-related Control System Authorization Framework" (EW18-D2-5266) to develop a cost-effective solution to streamline and tailor the RMF processes for FRCS. This project resulted in the RMF Self-Assessment Tool (R-SAT) to help FRCS Information System Owners (ISOs) perform self-assessments to identify, mitigate, and monitor cyber-security risks and support RMF steps 1-3, specifically:

- Preliminary Security Categorization
- Initial tailoring of the Security Plan (control baseline)
- Initial tailoring of implementation plan for the Control Correlation Identifiers (CCIs)

A significant time-savings to develop RMF artifacts was demonstrated; the time savings was estimated to be 64%-87%, depending on the R-SAT options selected [Ref (f)]. Additionally, eMASS forms could be prepared without the need for a CAC. R-SAT has been well-received and widely requested by those who have been made aware of it, and it is already in use some DoD RMF efforts. However, this ESTCP project for development and demonstration of the R-SAT prototype ended without funding for further enhancement and/or ongoing maintenance.

During the same period, the U.S. Army Corps of Engineers (USACE) Engineer Research and Development Center, Construction Engineering Research Laboratory (ERDC-CERL) had developed a beta version of a tool to assist designers in identifying Designer of Record (DoR) requirements prescribed in the Unified Facility Criteria (UFC) 4-010-06 [Ref (r)]. This excel-based DoR Tool generated a list of security controls, based on a user-defined security categorization, and summarized considerations for incorporating cyber security into the design. The DoR Tool was intended for use by design and construction stakeholders but was not yet in a state for broad use.

1.2 OBJECTIVE OF THE DEMONSTRATION

CySAT provides a consistent process for documenting pre-RMF security planning (that occurs in the FRCS design phase) and risk management efforts (which culminate in the construction phase) by incorporating the above-mentioned R-SAT and DoR tools into a single toolset. This resultant toolset will support Government and Industry stakeholders involved in the FRCS cybersecurity design and RMF processes with automation of the UFC and RMF submission requirements. Targeted user groups include Industry stakeholders performing a supporting role in FRCS Cybersecurity; government Design and Construction stakeholders; and FRCS ISOs.

The enhanced capabilities of the new toolset will be transferred to one or more Department of Defense (DoD) sponsors.

Supporting objectives include:

- Evaluate and coordinate FRCS Cybersecurity guidance for posting to DoD portals
- Develop Service-specific versions to accommodate unique RMF processes and inheritance.
- Identify and design value-added enhancements from the existing toolsets
- Align with related DoD efforts (e.g., FRCS Design Specifications)

1.3 REGULATORY DRIVERS

Federal and DoD policies and publications are the foundational elements which drive CySAT processes. Federal Instruction requires agencies to categorize their information systems as low, moderate, or high impact for confidentiality, integrity, and availability (CIA). Specific DoD Instruction provides directives to establish a DoD cybersecurity program to protect and defend DoD information and IT infrastructure. Additional guidance and publications have been incorporated to address DoD Operational Technology and Facility Related Control Systems. These publications are summarized in the text that follows:

Federal and DoD Instruction:

- **DoD Instruction 8500.01**, Cybersecurity, March 14, 2014 [Ref (d)].
- **DoD Instruction 8510.01**, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017 [Ref (e)].
- **Federal Information Processing Standard Publication (FIPS Pub) 199**, "Standards for Security Categorization of Federal Information Systems," Feb 2004 [Ref (i)].
- **Committee on National Security Systems (CNSS) Instruction No. 1253**, **Security Categorization and Control Selection for National Security Systems,** March 27, 2014 [Ref (b)].

National Institute of Standards and Technology (NIST) special publications (SP):

- **NIST SP 800-82**, Guide to Industrial Control Systems (ICS) Security, Revision 2, May 2015: Provides a tailored baseline of security controls to secure Industrial Control Systems (ICS) [Ref (o)].
- **NIST SP 800-53, Revision 4, Security and Privacy controls for Information systems and Organizations:** Provides descriptions of security controls and assessment procedures. CNSSI is a companion document to NIST SP 800-53 [Ref (l)]. *At this time, CNNSI has not been updated to reflect the new control mappings published in Revision 5 (Dec 10, 2020)*.
- **NIST SP 800-60, Information Security, Revision 1, Volumes I & II, Information Security, August 2008:** provides a list of Information Types and the suggested security categorization to assist Federal government agencies in developing security categorization [Ref (m)(n)].

Whole Building Design Guide (http://www.wbdg.org/) publications [Ref (t)]:

- **Unified Facilities Criteria (UFC) 4-010-06:** describes requirements for incorporating cybersecurity in the design of all facility-related control systems for implementation at DoD installations [Ref (r)].
- **RMF FRCS Master List**: This list was published by the Office of the Assistant Secretary of Defense for Sustainment (Energy, Installations and Environment). The list assigns Confidentiality, Integrity, Availability (CIA) impact ratings, by FRCS category and mission criticality, as a starting point for the security categorization [Ref (g)].
- **FRCS Overlay:** This document is used to provide a tailored baseline of security controls applicable to FRCS at a Moderate-Moderate-Moderate CIA level [Ref (h)].
- **Unified Facilities Guide Specification (UFGS) 25 05 11 20**: Cybersecurity for Facility Related Control Systems [Ref (s)].

Service-specific guidance:

- **Army Policy Record (APR):** addresses security controls that have requirements met by existing DoD policies (eMASS record) [Ref (a)].
- **NAVFAC-ENT_FRCS_Policy**: addresses security controls that have requirements met by existing NAVFAC-ENT_FRCS_Policy (eMASS record) [Ref (k)].
- **Department of Navy Information Types USN RMF Information System Categorization Form v 1.6**: Identifies FRCS Information Types and their selected DoN Impact Levels [Ref (j)].

2.0 TECHNOLOGY DESCRIPTION

2.1 TECHNOLOGY DESCRIPTION

The functions of CySAT reside in a macro-based Excel worksheets with tabs for each step. Each worksheet represents a step in the UFC and RMF process, graphically represented in Figure 2. Data from worksheets can be exported to satisfy UFC cybersecurity submittals and RMF artifacts. CySAT starts at a degree of technical readiness with being based in Microsoft Excel, utilizing conventional data transfer processes (export/import of CSV files), and integrating with existing DoD tools (eMASS) which are mandated for the served audience. An overview of the technology is provided below. More detail on the design of each worksheet is provided in Section 5.3.

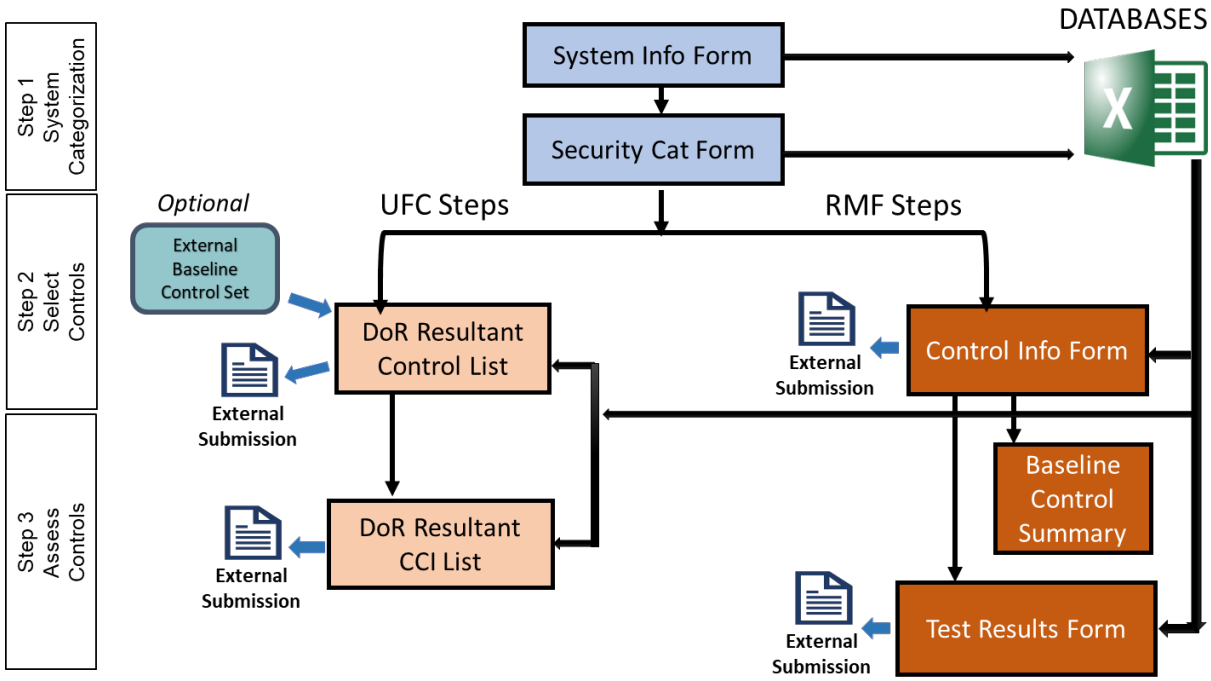

Figure 2. CySAT Overview of Features

The toolset begins with the **System Information Form** worksheet. On this form, basic information about the system is entered. Based on entries on this initial worksheet, subsequent worksheets are auto populated using macros and underlying databases. CySAT requires the selection of:

- DoD Service to employ CySAT's service-specific capabilities.
- FRCS System type (e.g., Microgrid Control System) to autofill suggested information types and preliminary impact levels.

The next worksheet represents the **Security Categorization Form** worksheet. This is the initial step in both the UFC and RMF processes. The preliminary Information Types, Security Impact Levels, and Overall Security Categorization are automatically generated by CySAT, based on the data populated on the **System Information Form** worksheet. The auto-generated CIA impact levels may be manually adjusted.

A list of security controls (control baseline) is automatically generated by CySAT. This list is based on the CIA impact levels selected by the user on the **Security Categorization Form** worksheet. During this step, users can apply an overlay and/or tailoring options to the control baseline. The remaining DoR and RMF tabs are completed independently of each other. For the UFC submittals, security controls are populated on the **DoR Resultant Control List** Worksheet and for the RMF process, the population is on the **Control Information Form** Worksheet. The **Baseline Control Summary** worksheet provides an informational overview of the security controls included in the resultant baseline, as well as those added and removed from the selected baseline.

The final worksheet(s) will document the planned implementation for the selected security controls. For the UFC submittals, this is completed on the **DoR Resultant CCI List** Worksheet and for the RMF process, this is completed on the **Test Results Form** Worksheet. CySAT provides users with service-specific inheritance and designer responsibility details, to assist in documenting the implementation of each CCI.

2.2 TECHNOLOGY DEVELOPMENT

To meet the technical objectives, the proposal team evaluated the existing RSAT and DoR toolsets to design the overall integration and implement new capabilities. The incorporation of these two tools into a single toolset allows the cybersecurity designers and RMF stakeholders to work from the same tool and the same control baseline. This will reduce potential conflicts and streamline the controls selection by preventing multiple parallel efforts.

To identify the most relevant enhancements to incorporate, Government stakeholders within the FRCS Community of Interest (COI) were consulted and input was collected. Based on this effort, the requirements and enhancements listed below were identified:

1. **Service-Specific Requirements and Inheritance (new feature):** CySAT contains an option to select a component (NAVFAC, or Army) which will incorporate the service's specific requirements for FRCS. *For example, if NAVFAC is selected, the DoN FRCS CIA Impact Levels\ for Information Types will be used*.
2. **Additional tailoring options for auto-populated CIA impact levels (updated):** The Overall Security Categorization for Confidentiality, Integrity and Availability is automatically generated. Several tailoring options are provided:
   - Auto-population based on Information Types and Preliminary CIA Impact levels generated for the user-selected FRCS system Type.
   - Auto-population based on Mission Criticality, generated for the user-selected FRCS system Type.
   - Manual user entry of overall Security Categorization.
3. **Application of FRCS Specific Overlay (updated):** Users can apply an overlay to the control baseline. The overlay options include ICS Overlay, FRCS RMF Tag Overlay or a combined ICS/RMF Tag Overlay.
4. **Application of FRCS Specific Tailoring Options (new feature):** Users can select from (11) different tailoring options to apply non-applicability when certain conditions exist in the system. *For example, CCIs that relate to use of wireless capabilities are marked as N/A if the tailoring option "System contains no wireless" is selected*.

5. **Application of User-Generated Control Baseline (new feature for design)**: In lieu of using the generated baseline controls, users can populate a custom baseline control list into CySAT's UFC DoR Resultant Control worksheet. This allows users the option to proceed with cybersecurity design for a system-specific set of controls.
6. **RMF Control Information Form (updated):** CySAT populates the Control Information Form worksheet with a preliminary Implementation Plan and System Level Continuous Monitoring (SLCM) Plan, based on the selected security categorization and overlay. DoD and Service specific inheritance is auto populated. The form can be exported into an external worksheet that is compatible with eMASS upload. Export processes were improved to minimize the need to accommodate updates to the format of eMASS templates.
7. **RMF Test Results Form Template (updated):** CySAT populates the Test Results Export Form worksheet with preliminary results, based on the selected security categorization and any overlay. DoD- and Service-specific inheritance is identified. For Army users, organizational security policies and procedures can be applied as an option (see Section 5.3.5 Supplemental Policy Templates). For NAVFAC users, the FRCS ENT policy and procedure can be applied as an option. The data can be exported into an external worksheet that is compatible with eMASS upload. The export process was improved to minimize the need to accommodate updates to the format of eMASS templates.
8. **Supplemental Policy Templates (updated):** The organizational security policies and procedures for Low and Moderate systems, developed as a deliverable for the original R-SAT toolset, were refreshed. These documents were developed for staffing by the FRCS-owning organization and are most applicable to Army components. Referenced templates for eMASS artifacts (e.g., access control rosters) and an Information System Security Manager (ISSM) checklist are also provided.
9. **UFC Basis of Design Submittal Template (new feature):** A list of security controls based on the CIA selected impact levels is generated, along with preliminary recommendations and justifications for further tailoring of the security control set. The list can be exported into an external worksheet for use as the UFC Basis of Design submittal, as prescribed by UFC 4-010-06 for the Designer of Record.
10. **UFC Concept Design and Interim Design Submittal Templates (new feature):** A list of the CCIs resulting from the tailored security control list is generated, with the responsibility designation for each CCI (i.e., designer, enclave). The list can be exported into an external worksheet for use as the UFC Concept Design and Interim Design submittals, as prescribed by UFC 4-010-06 for the Designer of Record.

2.3 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY

The primary objective of CySAT is to bridge the gap between security planning that occurs in the FRCS design phase and the RMF self-assessment efforts which culminate in the construction phase. Advantages to using CySAT include:

- CySAT is free, requires no license fee, and utilizes common software (Microsoft Excel).

- CySAT does not require a government issued computer or CAC to use. Users can prepare eMASS templates prior to system registration and without a government-issued computer or CAC. CySAT is a complement to the existing government-owned eMASS system and exported forms are compatible with the format that needs to be imported into eMASS.
- CySAT provides a standard format for UFC submittals thereby reducing inconsistency for reviewers.
- UFC and RMF documentation is populated with standard responses related to FRCS and DoD inherited policy, providing cybersecurity professionals with a starting point for tailoring the selection and assessment of controls to specific system features.

There are alternative tools that allow the completion of RMF self-assessment effort, as summarized in the Facility-Related Control System Authorization Framework Risk Management Framework (RMF) Self-Assessment Tool (R-SAT) Final Report [Ref (f)]. None of the existing tools align with the UFC cyber security design process. CySAT does contains macros and relative to alternative RMF tools CySAT has accessibility limitations:

- Not all DoD organizations can email .xlsm files and a few organizations may block files with macros for download. Users may need to use DoD Secure Access File Exchange to share CySAT files.
- Users will be required to allow macros to run CySAT. Some users may be required to work with IT departments to achieve approval for execution of CySAT macros.

3.0 PERFORMANCE OBJECTIVES

The performance objectives and findings focused on the measurement of CySAT's acceptance and value to FRCS stakeholders. These objectives, submitted to ESTCP in the Demonstration Plan dated April 18, 2023, are summarized in Table 1 and described in the section that follows. A detailed discussion of the findings is provided in Section 6.

Table 1. Performance Objectives

Performance Objective	Metric	Data Requirements	Success Criteria	Findings
Quantitative Performance Objectives				
Industry Adoption	Industry Utilization	Number of requests for the toolset; number of organizations attending demonstrations	≥ 60% of attending organizations request the new toolset	**Achieved** 75% of attending organizations request the new toolset
Qualitative Performance Objectives				
Industry Input without Government System Access	Facilitation of cybersecurity and RMF submittals	Required format of importable eMASS templates and DoR submittals	Generation of industry input that is importable or is in otherwise acceptable formats without the need for government system access	**Achieved** CySAT RMF Forms were exported into external templates and uploaded to the eMASS pilot site without error
Government Ownership & Maintenance	Government Accepts Ownership	Written consent that the government accepts ownership and maintenance	Government owner and continued maintenance of toolset	**Achieved** CySAT will be maintenance by ERDC-CERL

3.1 QUANTITATIVE

3.1.1 Quantitative–Industry Adoption

The level of interest for CySAT by prospective users was quantitatively evaluated by tracking the number of requests for the CySAT toolset following virtual capability demonstrations, conducted between Jan to Sep 2023. It is extrapolated that acceptance of CySAT by prospective users can be demonstrated by measuring interest immediately following a demonstration. More importantly, user interest in CySAT capabilities was assessed by addressing user questions during the presentation. A summary of the data collected for this performance objective is provided in Section 5.6 and Table 2. A discussion of the results is provided in Section 6.1.

3.2 QUALITATIVE

3.2.1 Qualitative–Industry Input without Government System Access

As stated in Section 2.3, some DoD and Federal cybersecurity process websites require a CAC and/or a government-furnished computer with VPN to access. The time and expense required to issue these resources is burdensome for both Industry and the DoD. The ability to generate correctly formatted RMF forms, without a CAC or government-issued computer, is useful to RMF Stakeholders. By demonstrating that CySAT RMF submittals can be uploaded without generating an error, it can be demonstrated that future users can generate submittals and artifacts in usable formats that can be passed to DoD user for future tailoring and upload. This equates to a time savings for both Industry and DoD. A summary of the qualitative testing to demonstrate this performance objective is provided in Section 5.5.1 and a discussion of the results is provided in Section 6.2.

3.2.2 Qualitative–Government Ownership & Maintenance

The overall objective of this demonstration project is Government ownership and accepted responsibility for continued maintenance of the CySAT toolset. S&C received a confirmation of intent to take ownership and continue maintenance from ERDC-CERL. Additional details are provided in Section 6.3.

4.0 FACILITY / SITE DESCRIPTION

This section is not applicable to the CySAT toolset. A beta version of CySAT was developed, demonstrated, and shared with government and industry users. Demonstrations were conducted virtually using WebEx or MS Teams.

4.1 FACILITY/SITE LOCATION AND OPERATIONS

This section is not applicable to the CySAT toolset.

4.2 FACILITY/SITE CONDITIONS

This section is not applicable to the CySAT toolset.

5.0 TEST DESIGN

5.1 CONCEPTUAL TEST DESIGN

A beta version of CySAT was developed in January 2023. This working version was virtually demonstrated and shared with government and industry users between January to September to gauge interest and collect suggestions for improvements. The Test Design focused on measuring CySAT acceptance and value to FRCS stakeholders and ultimate transition of CySAT to a Government owner.

5.2 BASELINE CHARACTERIZATION

The RMF Self-Assessment Tool (R-SAT) and Designer of Record Tool (DoR), both described in Section 1.1 were used as the baseline to develop CySAT.

The purpose of the USACE-developed DoR Tool was to reduce errors in generating a list of designer security controls. However, performance metrics for the DoR tool were not assessed by USACE. Operation testing will focus on ensuring proper functionality of the DoR features in CySAT. CySAT is also expected to standardize UFC submissions and therefore reduce the time to review and approve future submissions.

The purpose of R-SAT was to facilitate RMF Steps 1-3. The performance findings collected during the demonstration of R-SAT indicated a time savings and value to FRCS stakeholders. Specifically:

- A reduction in labor hours to tailor RMF controls of 87% (Low Impact Level), 71% (Moderate Impact Level) and 64% (High Impact Level) was demonstrated [Ref (f)].
- An endorsement of "significant" usefulness by FRCS Stakeholders (based on Likert scale survey results) and positive comments in written endorsements received during outreach efforts [Ref (f)].

A similar time savings is expected by incorporating R-SAT functionality into CySAT. Therefore, testing focused on ensuring proper functionality of those features.

5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS

CySAT is an end-to-end framework focused on FRCS Owner's in-practice duties for cybersecurity design and RMF self-assessment. The available tools and resources are clear and assist with the integration of automation and streamlining techniques where possible. Individual elements of CySAT are described below. The underlying technology of CySAT is an Excel macro-enabled workbook with several Worksheets. The Visual Basic programming apply user selections to populate worksheets with content from CySAT's integrated databases. The result is auto-populated templates with standard responses based on user-defined FRCS characteristics. A complete description of CySAT functionality is provided in the CySAT User Guide (Appendix C); however, an overview of the significant features is summarized in the sections that follow.

5.3.1 CySAT Automation of Security Categorization

System Categorization is the Step 1 of both the UFC and RMF process. Based on the organizational mission and details of the control system, the user must determine the CIA impact levels (LOW, MODERATE, or HIGH) for the FRCS control system. This is typically determined by assigning Information Types, reviewing the Security Impact Levels for these Information Types, and calculating an Overall Security Categorization based on the high watermark of the individual security impact levels. CySAT automatically generates a security categorization by comparing the selected DoD Component and FRCS System Type to data on the FRCS Master List [Ref (g)] and NIST 800-60 [Ref (m)(n)] or USN Information System Categorization Form [Ref (j)]. The generated impact levels may be further tailored, as described in the section that follows. The CySAT generation of the security categorization is graphically represented by the flow chart in Figure 3.

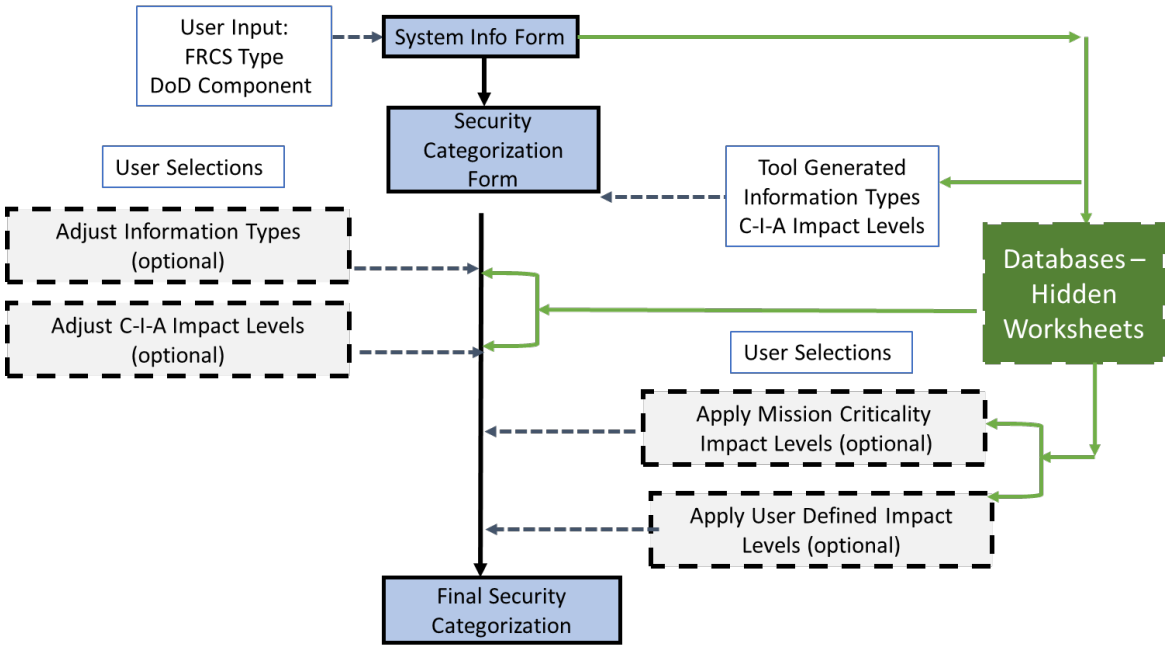

Figure 3. CySAT Overview of Security Categorization Options

5.3.1.1 System Information Form

Users enter basic information about their system and make selections to drive the auto population of subsequent forms. Based on entries on this initial worksheet, subsequent worksheets are populated using macros and underlying databases. The selections that drive the auto population include:

- DoD Component: The DoD Component is the entity that has authorization responsibility for the system. This selection determines the service-specific capabilities to be used for NAVFAC or Army users.
- FRCS System type: This selection populates information types and preliminary impact levels associated with each information type. Alternatively, users may select to use the FRCS Mission Criticality levels (Mission Support, Mission Essential and Mission Critical), as defined on the FRCS Master List [Ref (g)].

5.3.1.2 Security Categorization Form:

CySAT generates default Information Types and a preliminary security categorization, based on entries in the **System Information Form** worksheet. Users have the option to review and adjust the auto-populated data in several ways:

- Users may add or delete from the auto-populated Information Types. When adjustments are made, the Overall System Impact Level will be recalculated by CySAT based on NIST 800-60 [Ref (m)(n)] or USN Information System Categorization Form [Ref (j)].
- Users may increase or decrease the provisional impact level auto populated for each Information Types. When adjustments are made, the Overall System Impact Level will be recalculated by CySAT based on NIST 800-60 [Ref (m)(n)]] or USN Information System Categorization Form [Ref (j)].
- Users can set the Security Impact Level for CIA using Mission Criticality levels as defined on the FRCS Master List [Ref (g)]. This bypasses the calculated values.
- Users can set the Security Impact Level for CIA manually. This bypasses the calculated values. This is useful if the security categorization is known or prescribed by the government.

5.3.2 CySAT Automation of UFC Steps

CySAT's Designer of Record Forms (DoR) apply to the design of cybersecurity for FRCS. After the security categorization is determined, controls are selected. CySAT automatically generates a baseline control set and CCI list with details pertaining to cybersecurity design. CySAT also provides the opportunity to apply various overlays or tailoring options to the list of controls. The CySAT automation of these UFC Steps is represented in the flow chart in Figure 4.

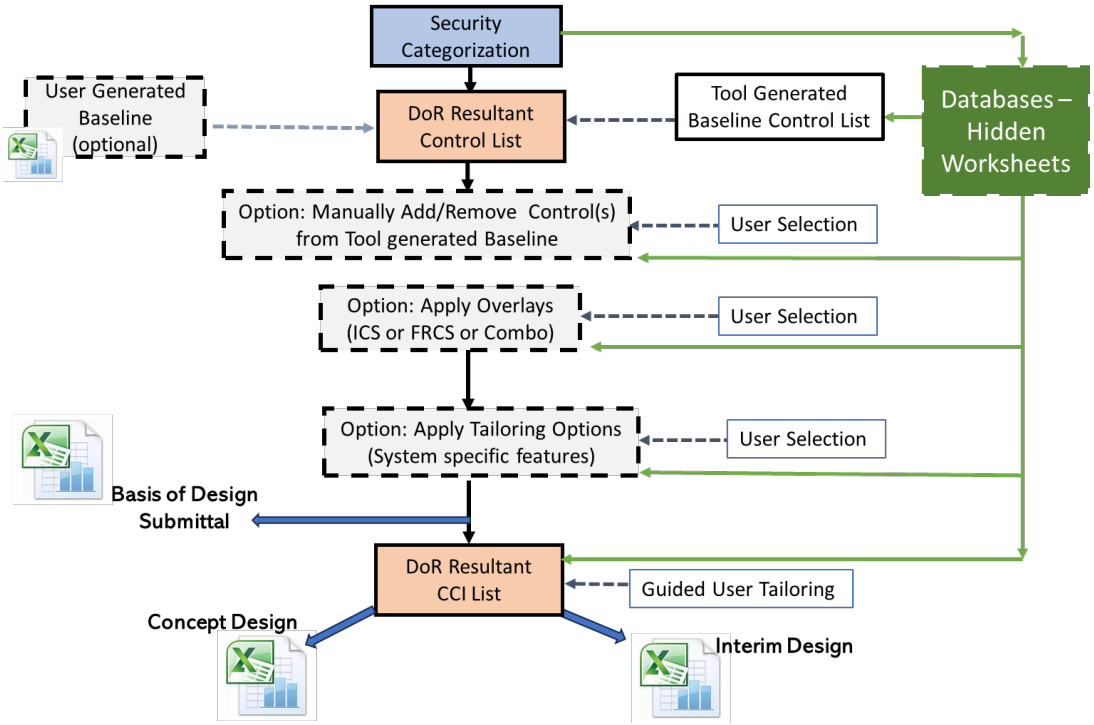

Figure 4. CySAT Overview of UFC Steps and Options

5.3.2.1 DoR Resultant Control List

The DoR Resultant Control List Form is where the control set is generated based on the current Security Categorization and the Committee on National Security Systems Instruction (CNSSI) No 1253 [Ref (b)]. Users can apply three different overlays (ICS overlays [Ref (o)], RMF Tag FRCS Overlay [Ref (h)], or a combined ICS/RMF Tag FRCS overlay) and/or nine different tailoring options (e.g., system does not use wireless, stand-alone system) to this list of controls. Users can review the starting controls baseline, and CySAT-populated details to determine if each control should be tailored out from (or added to) the security control baseline. In addition, users can manually add or remove controls from the baseline. The final list of controls can be exported to a UFC Basis of Design control list as a submittal.

5.3.2.2 DoR Resultant CCI List

The DoR Resultant CCI Form summarizes the resulting list of CCIs for the controls retained on the DoR Resultant Control List. Additionally, the UFC-defined responsibility for each CCI is populated. The DoR Resultant CCI List provides the starting point for identifying cybersecurity requirements to be included in the control system design and can be exported to a UFC Concept Design Submittal. In addition, CySAT identifies the UFGS design specification section for each CCI categorized as "Designer" [Ref (s)]. This information is a starting point for determining how CCI requirements will be incorporated into the design (UFC Interim Design Submittal).

5.3.3 CySAT automation of RMF Steps

CySAT's RMF Forms populate eMASS templates for RMF Self-Assessment Steps 1-3. After the security categorization is determined (RMF Step 1), security controls are selected (RMF Step 2) and assessed (RMF Step 3). CySAT automatically generates a baseline control set and CCI list with details pertaining to cybersecurity design. CySAT also provides the opportunity to apply various overlays or tailoring options to the list of controls. The automation of these RMF Steps is represented by the flow chart in Figure 5.

5.3.3.1 Control Information Form

The DoR Resultant Control List Form is where the control set is generated based on the current Security Categorization and the Committee on National Security Systems Instruction (CNSSI) No 1253 [Ref (b)]. Users can select one of three different overlays (ICS overlays [Ref (o)], RMF Tag FRCS Overlay [Ref (h)], or a combined ICS/RMF Tag FRCS overlay) and/or nine different tailoring options (e.g., system does not use wireless; stand-alone system) to this list of controls. CySAT populates an Implementation Plan for the baseline control set. Service-specific Inheritance, Non-Applicability and a preliminary Continuous Monitoring Strategy are also populated as a starting point. The data on the form can be tailored and exported into an eMASS form of the same name.

5.3.3.2 Test Results Form

The assessment of security controls is RMF Self-Assessment Step 3. At this step, evidence, and implementation descriptions for CCIs (the decomposition of security control requirements into singular, actionable statements) are documented. CySAT populates preliminary implementation procedures for each CCI, based on DoD inheritance and the application of service-specific policy data. The data on the form can be tailored by the user and exported into an eMASS form of the same name.

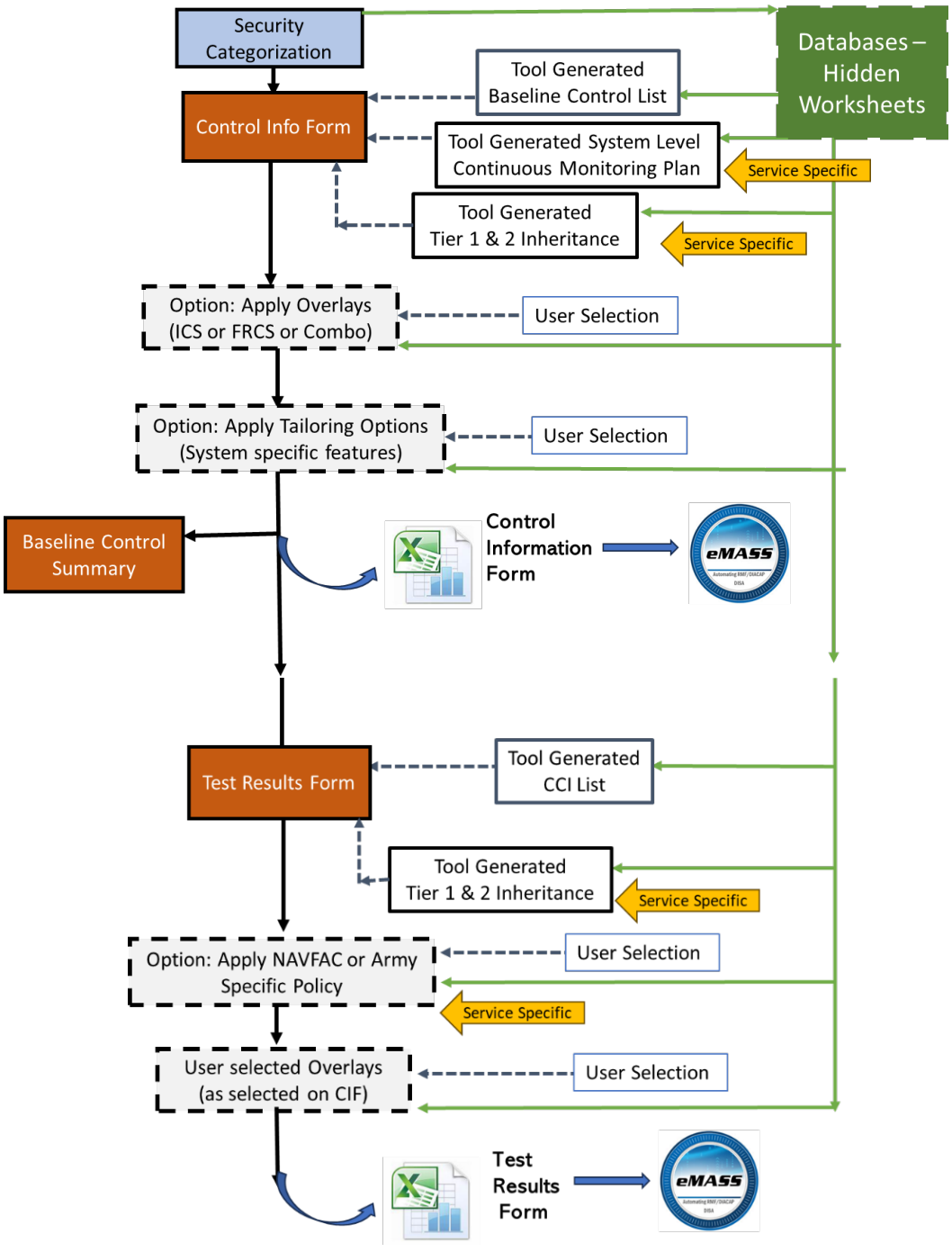

Figure 5. CySAT Overview of RMF Steps and Options

5.3.4 CySAT User Guide

A User Guide accompanies CySAT to provide an orientation to CySAT processes, including relevant definitions and references, and describe in detail the selections and options available to the user.

5.3.5 CySAT Supplemental Policy Templates

Supplemental Security Policy and Procedures Templates accompany the CySAT toolset and address administrative control elements. These supporting templates serve as a starting point to document organization-level implementation of security controls (i.e., acceptable use restrictions). This set of documents includes:

- **Control Family Documents:** unique policies and procedures for each NIST control family.
- **ISSM Checklist:** An ongoing summary of 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.

5.3.6 CySAT Training Video

A training video accompanies CySAT to provide a demonstration of **CYSAT USE**.

5.4 OPERATIONAL TESTING

Testing was conducted between January and September of 2023. A beta version of CySAT was tested, and improvements to the user interface and functional macros were made throughout the testing period. Testing consisted of operational testing and demonstrations.

5.4.1 Operational Testing

Operational testing consisted of simply performing CySAT processes and evaluating CySAT-populated exports to ensure no unexpected errors occurred. Testing was evaluated on a pass/fail basis; any identified errors were considered unacceptable and immediately corrected. Specific testing included:

- Performing all CySAT processes: This testing ensured macros function as expected and without error. Testing was conducted by CySAT developers (to identify logic issues) as well as novice users (to identify issues with ease of use).
- Generating CySAT security control sets: The CySAT-generated controls sets were compared to control sets generated by the USACE DoR Tool to check for accuracy.
- Generating CySAT RMF Forms: CySAT RMF Forms were generated and exported to check for errors. CySAT RMF templates were imported into an eMASS pilot site to ensure successful upload.
- Generating CySAT UFC Forms: CySAT UFC Forms were generated and exported to collect feedback from USACE reviewers on content to demonstrate acceptance by Government reviewers.

5.4.2 Demonstration

Testing also consisted of capability demonstrations of CySAT for external users. The purpose of the demonstrations was to quantify user acceptance and collect feedback on usefulness. Eight virtual presentations were conducted for approximately 327 prospective users and stakeholders to demonstrate CySAT's capabilities. Following each demonstration, participants were given the opportunity to officially request a copy of CySAT and feedback was recorded.

5.5 SAMPLING METHODS

5.5.1 Operational Sampling Results

The ability to generate a correctly formatted RMF and UFC forms that can be passed to DoD users for future tailoring and upload is useful to RMF Stakeholders. All operational testing was evaluated using a pass/fail criteria.

- The functionality of all macros was tested to ensure accuracy in the control set generated by CySAT.
- The CySAT populated eMASS templates were uploaded into the eMASS pilot site to demonstrate that RMF exports are compatible.
- The CySAT populated UFC templates were reviewed by the Tri-Service Standards and Criteria Program) Control Systems Discipline Working Group and were accepted for format and content.

5.5.2 Demonstration Sampling Results

Acceptance of CySAT by Industry demonstrates value and can be extrapolated to justify continued maintenance by a Government sponsor. CySAT acceptance was assessed by tracking the interest level of prospective users, following a virtual demonstration of capabilities. Participants were given the opportunity to provide feedback and officially request a copy. The number of requests for CySAT, following the demonstration, was recorded. In addition, user feedback was recorded at the time of the demonstration and in follow-up communications. This feedback was used to tailor CySAT functionality.

5.6 SAMPLING RESULTS

Eight virtual presentations were conducted to various organizations to demonstrate CySAT's capabilities between Jan 2023 and Sep 2023. A summary of the demonstration testing is provided in Table 2. Participant's specific comments and questions are summarized in Section 6.3

Table 2. CySAT Demonstration Testing

Date	Organization	Attendees	Demonstration Results
Feb 08	NAVFAC	Barley, Thomas Williams, Tia Gary, David	Demo only
Mar 03	Tri-Service Cybersecurity Commissioning Meeting	Gary, David McClellan, Mark Barley, Thomas Polacheck, Kevin Walters, James Robinson, Alton	Demo only
Apr 26	Burns and McDonnell	Williams, Lorenzo Russell, Calab B Richards, Jared B Gamonal, Yulio J	Working version of CySAT and User Guide requested C: Discussion of how this will be helpful for users that do not have a CAC
May 18	CyCx Bi-weekly Drumbeat	21 NAVFAC employees / contractors	Working version of CySAT and User Guide requested Discussion of how this will streamline processes
June 7 Morning session	Electrical and Mechanical Communities of Practice meetings	138 NAVFAC employees / contractors	Working version of CySAT and User Guide requested Discussion of how this will streamline processes
June 7 Afternoon session	Electrical and Mechanical Communities of Practice meetings	23 NAVFAC employees /contractors	Working version of CySAT and User Guide requested Discussion of how this will streamline processes
July 28	USACE Control System Communities of Practice meetings	25 Army employees /contractors	Working version of CySAT and User Guide requested
Sep 6	Joanna Stabile	NAVFAC FEC SW	Requested CySAT – no Demo
Sep 29	USARMY Control System Communities of Practice meetings	116 Army employees / contractors	Working version of CySAT and User Guide requested Discussion of how this will be helpful for control selection, particularly for developmental systems that are not registered in eMASS

6.0 PERFORMANCE ASSESSMENT

6.1 QUANTITATIVE–INDUSTRY ADOPTION

CySAT capabilities were presented to Industry Stakeholder to gauge the interest level of prospective users and to demonstrate the value of continued sustainment by the Government. S&C conducted eight presentations to 337 prospective users between Jan 2023 and Sep 2023. Following demonstrations, participants were given the opportunity to provide feedback and officially request a copy of CySAT. A summary of the requests following these demonstrations is provided in Table 2.

It is understood that some attendees may have requested a version to share with colleagues within the same organization. Therefore, the number of "overall" requests for CySAT was used in the evaluation. The toolset was requested and shared after six of the eight presentation (75% of the presentations). This **exceeds** the success criteria of 60% of attending organizations request the new toolset and demonstrates acceptance and continued use of CySAT by Industry.

This quantitative method used a simple measurement of number of requests for CySAT following demonstration to evaluate interest. It is recognized that a request does not completely correlate to continued use; therefore, recorded comments are important data. Many users were impressed with CySAT's ability to streamline UFC and RMF steps and were eager to use CySAT. Based on the feedback, it is clear that there is interest in using CySAT's demonstrated features.

6.2 QUALITATIVE–INDUSTRY INPUT WITHOUT GOVERNMENT SYSTEM ACCESS

CySAT capability to generate correctly formatted RMF forms, suitable for import to eMASS, was tested. The generated RMF Forms were exported into external Control Information and Test Result Templates. These exports were uploaded to the Army eMASS pilot site without error. The **meets** the qualitative success criteria "Generation of industry input that is importable or is in otherwise acceptable formats without the need for government system access" and demonstrates that users without a CAC or laptop can generate and inform submittals and artifacts in usable formats for upload by Government representatives.

6.3 QUALITATIVE–GOVERNMENT OWNERSHIP AND MAINTENANCE

CySAT capabilities were demonstrated to Government Stakeholder to facilitate an agreement for technology transfer and ownership of CySAT. A summary of the S&C conducted demonstrations is provided in Table 2. Following each demonstration, participants were also given the opportunity to provide feedback. Each demonstration generated positive feedback regarding the time savings expected from the CySAT demonstrated capabilities. A summary of participant's unique questions/comments and the S&C response is provided below

- NAVFAC Stakeholder: **Suggested a supplemental tool to allow government agency design review team to evaluate a DoR/eMASS submission more quickly**. In response, S&C developed a supplemental tool to compare two CySAT generated UFC Basis of Design submissions and summarize the differences for reviewers.

- Tri-Service Cybersecurity Commissioing Meeting: **Suggested an evaluation if Air Force controls would be useful to populate**. The project team evaluated this request and determined this would not be useful to perspective users.
- Tri-Service Cybersecurity Commissioing Meeting: **Suggested an evaluation if COINE inheritance would be useful to populate**. The project team evaluated this request and determined this would not be useful to perspective users.
- NAVFAC Stakeholders: **Suggested an evaluation if Cybersafe overlay would be useful to populate**. The project team evaluated this request and determined this would not be useful to perspective users at this time.
- Industry Stakeholder: **Please provide references for auto populated fields**. S&C has incorporated the references for all populated fields into the User Guide
- Industry Stakeholder: **Have the auto populated fields had been accepted by Services?** ERDC-CERL have vetted the UFC submission format with the approriate organizations. RMF forms are populated with data that is primarily from APR and NAVFAC-ENT policy record.
- USACE Stakeholders: **Suggested to share CySAT with USACE construction group to ensure correct format for design submittals for construction**. ERDC-CERL has vetted the UFC submission format with the approriate organizations.
- USARMY Stakeholders: **Suggested the Personally Identifiable Information Processing (PII) controls may be applicable to FRCS**. The current version of CySAT does not include PII controls.

ERDC-CERL intends to take ownership of CySAT and accepted responsibility for continued maintenance; This **meets** the qualitative success criteria for this performance objective. S&C has prepared a Maintenance Guide and training on CySAT processes to facilitate a smooth transition. CySAT will be uploaded to wbdg.org [Ref (t)] for users to download. This is a web-based portal that provides government and industry practitioners with one-stop access to information on building-related guidance, criteria, and technology. Users will be required to complete a questionnaire prior to download. This questionnaire is intended to capture user demographics and intended user application to allow continued evaluation of CySAT's benefit to FRCS stakeholders. Survey questions may include:

- What is your email address (this will be used to track DoD vs Industry)?
- What Agency or Service are you working for or contracted with?
- What type of FRCS System are you assessing?
- Which CySAT forms do you intend to complete "RMF" or "UFC" or "both"

7.0 COST ASSESSMENT

7.1 COST MODEL

CySAT will be free for public use and there are no cost elements for implementing the technology for users. This cost assessment focuses on the cost to the Government sponsor for ongoing maintenance or implementation of new features. Labor hours for cost elements were derived from project hours to develop the CySAT's initial functionality. The cost model assumes a fully burdened labor rate of $200/hr and a 5-year project life cycle. A summary is provided in Table 3.

Table 3. Cost Model for CySAT Maintenance

Cost Element	Data Analysis/Assumptions	Estimated Annual Costs
INITIAL COST		
Hardware capital costs	Assumes use of existing workstation.	$0
Initial Familiarization	Incorporated into EW21-B1-5184 budget.	$0
MAINTAIN CURRENT FEATURES		
Annual Maintenance	100 hours per year to maintain databases 60 hours per year for user support	160 hrs/year $32,000 annual costs at fully burdened labor rate
Present value of annual cost to maintain existing CySAT features over 5-year period		**$142,560 (rounded)**
IMPLEMENT ADDITIONAL FEATURES in 2-years		
Implement additional feature	~350 hours to implement additional features	350 hours $70,000
Present value of future cost to develop additional CySAT features After a 2-year period		**$64,720 (rounded)**
PRESENT WORTH ESTIMATE of COSTS ELEMENTS		**$207,280 (rounded)**

7.1.1 Hardware Capital Costs:

The cost model assumes a workstation with MS Excel is available to run CySAT; no capital hardware costs are anticipated.

7.1.2 Initial Familiarization:

The labor hours required to familiarize the Government sponsor with CySAT logic has been incorporated into the EW21-B1-5184 project budget. This will be accomplished with training and a CySAT Maintenance Guide.

7.1.3 Maintenance of Current Features:

CySAT functionality relies on databases that incorporate control and CCI data from Federal Instruction. Some maintenance will be required to keep this data current when regulatory drivers (described in Section 1.3) are updated. It is estimated that 100 hours per year will be needed to update data in existing databases, including validation, and testing of the updates.

The Government sponsor will provide an email contact to address user questions and comments related to the use of CySAT. It is anticipated the User Guide (Section 5.3.4) and Training Video (Section 5.3.6) will minimize user questions and comments; however, an additional 60 hrs per year will be allocated to account for user support.

7.1.4 Additional Feature Implementation:

CySAT functionality relies on macros to apply user selections to populate worksheets with content from CySAT's integrated databases, as described in Section 5.3. It is assumed that continual updates to CySAT may be required to keep in step with eMASS and RMF/UFC policy changes. The macro that "exports" RMF data from CySAT was improved to minimize the need to update the logic when eMASS templates are changed, however it is recognized that updates may be required over time. Labor hours during the initial design phase to implement additional features were ~350 hours. For this economic analysis, it is estimated that a similar update to identify, assess, and engineer CySAT logic will be required at Year 2 in the 5-year project life cycle.

7.2 COST DRIVERS

Implementations of CySAT's current features are expected to carry little to no costs (estimated: $32,000 annually). Continued support and implementation of any additional desired features can be assessed by the Government sponsor for value of implementation, as these needs occur.

7.3 COST ANALYSIS AND COMPARISON

Operationally, there are no additional costs for implementation by users. The cost elements described are for optional, Federal life-cycle costs for overall maintenance and updates to CySAT. Annual cost estimates are provided in the cost model. These costs, in comparison to manual UFC designer and RMF Self-Assessment processes are eclipsed by time savings for users of CySAT. CySAT is also expected to support the standardization of UFC submittals and therefore reduce the time for government review and approval of future submissions. The government sponsor will need to assess the value of this time savings versus the cost to maintain.

8.0 IMPLEMENTATION ISSUES

The following implementation issues have been identified:

- CySAT is an Excel worksheet with Visual Basic programing and some users may have concerns with using a macro-enabled Excel document. Distributing MS Office documents with embedded macros can introduce some risk. Malicious code can reside within macros, so distributing CySAT via email should be avoided. This risk will be mitigated by allowing download of CySAT from the Whole Building Design Guide and ESTCP portals.
- CySAT is suitable for control systems of any impact rating, however HIGH Impact systems typically require customized requirements not addressed by CySAT. Auto-populated fields on CySAT forms are specific to control systems assigned a LOW or MODERATE impact level.
- CySAT is a tool that requires a learning curve for users to understand the functionality and tailoring options. CySAT was designed to be intuitive and user friendly; however, users must be willing to invest upfront time in learning the applications. The User Guide and training video are intended to decrease the user's time to learn CySAT and minimize this risk. In addition, an email contact will be provided to address user questions and comments related to the use of CySAT.
- CySAT functionality may be impacted by updates to the UFC, eMASS or FRCS policy and guidance. For example, security control categorization (CNSSI) and overlays (NIST 800-82 and FRCS RMF Tag) will need to be updated to reflect NIST 800-53r5 updates. Updates to CySAT databases and/or logic may also be necessary to keep pace. ERDC-CERL intend to take ownership of CySAT and accept responsibility for continued maintenance and user support. User demographics and intended user application of CySAT, collected from a user survey at time of download, will be used to evaluate the cost/benefit of any required updates to CySAT.

9.0 REFERENCES

a. Army Policy eMASS record Export; 15APR2019; File: Army Policy Record_TRExport_15Apr2019.xlsx

b. Committee on National Security Systems Instruction (CNSSI) 1253; "Security Categorization and Control Selection for National Security Systems"; March 27, 2014, as amended.

c. Defense Information System Agency (DISA) dashboard on DoD Cyber Exchange (https://public.cyber.mil/stigs/cci/).

d. DoD Instruction 8500.01; "Cybersecurity" Change 1; Oct 07, 2019.

e. DoD Instruction 8510.01; "Risk Management Framework (RMF) for DoD Information Technology (IT)" Change 2; July 28, 2017.

f. ESTCP Facility-Related Control System Authorization Framework Risk Management Framework (RMF) Self-Assessment Tool (R-SAT) Final Report; EW18-D2-5266; Dec 2019.

g. Facility Related Control System (FRCS) Master List; Office of the Assistant Secretary of Defense for Sustainment FRCS Cybersecurity Website; (https://www.acq.osd.mil/eie/IE/FEP_CSC.html); Oct 19, 2020.

h. Facility Related Control System (FRCS) Overlay; RMF Implementation Division DoD-CIO, DCIO-CS, CSRM; Last Updated: May 31, 2019.

i. Federal Information Processing Standard Publication (FIPS Pub) 199; "Standards for Security Categorization of Federal Information Systems"; Feb 2004.

j. Department of Navy Information Types USN RMF Information System Categorization Form v 1.6; last update: Aug 6, 2021; File: NAVFAC-SEC_CAT.xlsx.

k. NAVFAC-ENT_FRCS_Policy, 13566, NAVFAC-FAO-Platform IT eMASS record Export 21MAR2023; File: NAVFAC-ENT_FRCS_Policy_TRExport_21Mar2023.xlsx.

l. NIST Special Publication (SP) 800-53 Revision 4; "Security and Privacy Controls for Federal Information Systems and Organizations"; April 30, 2013.

m. 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.

n. 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.

o. NIST (SP) 800-82 Revision 2; "Guide to Industrial Control Systems (ICS) Security"; May 2015, as amended.

p. Pacific Northwest National Laboratory; Impacts of Commercial Building Controls on Energy Savings and Peak Load Reduction (PNNL-25985); May 2017.

q. RMF Knowledge Service (RMFKS) Portal; https://rmfks.osd.mil [The Risk Management Framework Knowledge Service (RMFKS) is a central repository for RMF DoD for IT].

r. UFC 4-010-06, Unified Facilities Criteria; “Cybersecurity of Facility-Related Control Systems”; Oct 10, 2023.

s. UFGS 25 05 11 20 Cybersecurity for Framework For Facility-Related Control Systems; Whole Building Design Guide website (wbdg.org); May 01, 2021.

t. Whole Building Design Guide; https://wbdg.org [WBDG is a gateway to up-to-date information on integrated 'whole building' design techniques and technologies].

APPENDIX A POINTS OF CONTACT

Point of Contact Name	Organization Name Address	Phone Fax Email	Role in Project
Aura Lee Keating	S&C Electric Company 6601 N Ridge Blvd, Chicago, IL 60626	703-350-6747 auralee.keating@sandc.com	Principal Investigator
Joseph Bush	U.S. Army Corps of Engineers Engineer Research & Development Center Construction Engineering Research Laboratory ATTN: CEERD-CERL P.O. Box 9005 2902 Newmark Dr. Champaign, IL 61826-9005	217-373-4433 Jospeh.Bush@usace.army.mil	Technical Lead