FINAL REPORT

Facility-Related Control System Authorization Framework Risk Management Framework (RMF) Self-Assessment Tool (R-SAT)

EW18-5266

Authors: Aura Lee Keating, IPERC
William Horner, Operations Division
C5ISR Center, NVESD

December 2019
Version 1.0

Distribution Statement A: Approved for Public Release

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
31/12/2019	ESTCP Final Report	

4. TITLE AND SUBTITLE

Facility-Related Control System Authorization Framework Risk Management Framework (RMF) Self-Assessment Tool (R-SAT)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Aura Lee Keating, IPERC
William Horner, RDECOM, CERDEC, NVESD

5d. PROJECT NUMBER
EW18-5266

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
RDECOM, CERDEC, NVESD
10221 Burbeck Road
Ft. Belvoir, VA 22060

8. PERFORMING ORGANIZATION REPORT NUMBER
EW18-5266

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Environmental Security Technology Certification Program
4800 Mark Center Drive, Suite 16F16
Alexandria, VA 22350-3605

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S) EW18-5266

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The objective of this project was to provide a prescriptive, step-by-step method to facilitate and accelerate Risk Management Framework (RMF) Self-Assessments through automation. The RMF Self-Assessment Tool (R-SAT) is an Excel based tool that was designed to streamline the process for obtaining an Authority to Operate for network-enabled Facility-Related Control Systems (FRCS) by providing focused, step-by-step guidance and outputs supporting RMF Steps 1-3. RSAT works in conjunction with the Enterprise Mission Assurance Support Service (eMASS) government-owned application. R-SAT's customized Visual Basic macros apply user inputs against a series of condition-specific integrated databases to produce output forms for additional tailoring and subsequent eMASS upload. R-SAT was demonstrated and circulated to FRCS stakeholders. The findings and performance assessment from the demonstration and outreach provide evidence that R-SAT is a useful tool that will yield a time savings to FRCS system owners that must perform RMF Self Assessments.

15. SUBJECT TERMS

Facility-Related Control System Authorization, Framework Risk Management Framework, RMF, Self-Assessment Tool, R-SAT

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			William Horner
UNCLASS	UNCLASS	UNCLASS	UNCLASS	305	19b. TELEPHONE NUMBER *(Include area code)* 703-704-2855

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

A&A	Assessment and Authorization
AO	Authorizing Official
APR	Army Policy Record
ASD-EI&E	Assistant Secretary of Defense for Energy, Installations, and Environment
ATO	Authority to Operate
CNSSI	Committee on National Security Systems Instruction
CRN	Closed Restricted Network
CCI	Control Correlation Identifier
DASD-E	Assistant Secretary of Defense for Energy, Installations, and Environment
DoD	Department of Defense
DoDI	Department of Defense Instruction
eMASS	Enterprise Mission Assurance Support Service
FRCS	Facility Related Control Systems
GOTS	Government off the shelf
GUI	Graphical User Interface
HMI	Human Machine Interface
ICS	Industrial Control Systems
ISO	Information System Owner
IPC	Intelligent Power Controllers
NIST	National Institute of Standards and Technology
NVESD	Night Vision and Electronic Sensors Directorate
OSD	Office of the Secretary of Defense
OT	Operational Technology
PACS	Physical Access Control System
PM	Project Manager
PNNL	Pacific Northwest National Laboratory
POC	Point of Contact
P&P	Policy & Procedures
RMF	Risk Management Framework
RMF-KS	RMF Knowledge Service
R-SAT	RMF Self-Assessment Tool
SCA-V	Security Control Assessor-Validator
SDLC	Software Development Lifecycle
SIPOC	Suppliers, Inputs, Process, Outputs, Customers
SLCM	System Level Continuous Monitoring
SO	System Owner
SP	Special Publication
SSP	System Security Plan
UFC	Unified Facilities Criteria

UMCS	Utility Monitoring & Control System
USAG-KA	US Army Garrison Kwajalein-Atoll
WHS	Washington Headquarter Service

Acknowledgements

This work is supported by the U.S. Department of Defense ESTCP program under IPERC Project EW18-D2-5266. IPERC is very thankful for the technical support provided by Dr. Michael Chipley, ESTCP Cyber Support SME, and by Sarah Medepalli of Noblis. The team gratefully acknowledges the support received from Bethany Hill, CISSP, of Spectrum Solutions, Inc., and William Horner, William Elliott and Kevin Brady at the Night Vision and Electronic Sensors Directorate (NVESD) who participated in this project.

ABSTRACT

The objective of this project was to provide a prescriptive, step-by-step method to facilitate and accelerate Risk Management Framework (RMF) Self-Assessments through automation. The RMF Self-Assessment Tool (R-SAT) is an Excel based tool that was designed to streamline the process for obtaining an Authority to Operate for network-enabled Facility-Related Control Systems (FRCS) by providing focused, step-by-step guidance and outputs supporting RMF Steps 1-3. R-SAT works in conjunction with the Enterprise Mission Assurance Support Service (eMASS) government-owned application. R-SAT's customized Visual Basic macros apply user inputs against a series of condition-specific integrated databases to produce output forms for additional tailoring and subsequent eMASS upload. R-SAT was demonstrated and circulated to FRCS stakeholders. The findings and performance assessment from the demonstration and outreach provide evidence that R-SAT is a useful tool that will yield a time savings to FRCS system owners that must perform RMF Self Assessments. However, there are some implementation issues. R-SAT is a tool that requires a learning curve for users in order to understand the functionality and tailoring options. The software was designed to be intuitive and user friendly; however, users must be willing to invest upfront time in learning the software. Additionally, R-SAT is an Excel worksheet with Visual Basic programing and some users may have concerns with using a macro-enabled Excel document. Finally, R-SAT's functionality may be impacted by updates to eMASS or FRCS policy and guidance; therefore, updates to R-SAT will be necessary to keep pace.

EXECUTIVE SUMMARY

OBJECTIVES OF THE DEMONSTRATION

The main objective of the design of R-SAT is to provide a prescriptive, step-by-step method to facilitate and accelerate RMF Self-Assessments through automation.

Supporting objectives include:

- Low cost implementation
- Effective resource for all aspects of FRCS owner security planning and implementation
- Intuitive, highly repeatable and applicable across system types
- Clear delineation of cybersecurity stakeholder actions
- Government support of integration with RMF processes, such as Reciprocity and Reuse

DESCRIPTION OF THE TECHNOLOGY

The RMF Self-Assessment Tool (R-SAT) is an Excel based tool that was designed to streamline the process for obtaining an Authority to Operate for network-enabled Facility-Related Control Systems (FRCS) by providing focused, step-by-step guidance and outputs supporting RMF Steps 1-3. R-SAT works in conjunction with the Enterprise Mission Assurance Support Service government-owned application. R-SAT was developed with full recognition and appreciation for what eMASS provides and serves to advance the overall ecosystem supporting the DoD, rather than complicating DoD FRCS Owner's decision paths with alternative tool sets. R-SAT includes an extensive set of customized Microsoft Excel Visual Basic macros in order to execute automated aspects and perform various R-SAT functions. Ease of use is accomplished as the software's structure displays a familiar tab-based Excel workbook layout and each tab guides the user through basic input questions and utilizes embedded databases to autofill eMASS importable templates. R-SAT's workflow applies user inputs against a series of condition-specific integrated databases to

produce data for additional tailoring and subsequent eMASS upload. Associated artifacts, including Policy & Procedure documentation with cross references to applicable Control Correlation Identifiers (CCIs), round out the resources available with R-SAT.

PERFORMANCE ASSESSMENT

The objectives of the project were assessed using quantitative (reduction of labor hours to complete RMF) and qualitative (user acceptance) performance metrics. FRCS Stakeholders were sampled between August 2018 and the Short Course demonstration at the ESTCP Symposium on December 5, 2019. The performance objectives and findings indicate that R-SAT will contribute a time savings and value to FRCS stakeholders. The performance assessment data is summarized below:

- 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. This is further supported by an estimated 80% reduction in labor hours to perform a pilot RMF Self Assessments (based on measured labor hours) and a 90% reduction in eMASS Data Entry (based on measured eMASS data entry time for individual CCIs).
- An endorsement of "significant" usefulness (based on Likert scale survey results) and positive comments in written endorsements received during outreach efforts indicate R-SAT is a value to FRCS Stakeholders.

In addition to measured performance metrics, the feedback received during outreach efforts identified that many FRCS Stakeholders are unfamiliar with the RMF Process. Many potential users that were asked to evaluate R-SAT were unable to provide quantitative feedback because of unfamiliarity with the process. The R-SAT User Guide and training video were modified during the design phase to partially address this issue and better guide users through the RMF-Self Assessment process while using the features of R-SAT. However, use of R-SAT assumes a basic understanding of the RMF process.

COST ASSESSMENT

R-SAT is free for public use and performance metrics demonstrate a cost savings in terms of labor hours. R-SAT functionality may be impacted by updates to eMASS or FRCS policy and guidance. Updates to R-SAT will be necessary to keep pace. Therefore, a cost estimate for ongoing maintenance of R-SAT by a designated Federal organization was estimated:

- **Initial Familiarization ($1,120) -** Average of labor hours required to learn to use R-SAT based on metrics gathered during demonstration
- **Maintenance ($16,000) -** Estimate based on labor hours required to incorporate pilot user feedback into R-SAT during demonstration and testing
- **Additional feature implementation ($27,200) -** Estimate based on 50% labor hours required to identify, assess, and engineer R-SAT features during design phase
- **User training and materials update ($20,560) -** Estimate based on development of user guide, webinar, and training course materials during demonstration
- **Publishing ($1,600) -** Estimate based on labor hours to coordinate initial publishing of R-SAT and associated documents to two different websites.

IMPLEMENTATION ISSUES

Implementation issues are somewhat attributed to the short timeline for the project. The software development phase was extended to address several comments received by users throughout the

outreach phase. This ensured that the R-SAT software and the corresponding User Guide addressed the needs of the FRCS stakeholders. In addition, a training video was developed to ensure that potential users have visual resources to facilitate the use of R-SAT. The following implementation issues were identified during the development and testing of the software:

- R-SAT is an Excel worksheet with Visual Basic programing and some users may have concerns with using a macro-enabled Excel sheet. Distributing MS Office documents with embedded macros can introduce some risk. Malicious code can reside within macros, so distributing R-SAT via email should be avoided. Download of R-SAT from the RMF-KS and ESTCP portals should be facilitated by the appropriate government personnel and process.

- R-SAT is a tool that requires a learning curve for users in order to understand the functionality and tailoring options. The software was designed to be intuitive and user friendly; however, users must be willing to invest upfront time in learning the software. This unwillingness to invest time in learning a new program was recognized by the team when attempting to obtain metrics for R-SAT's time savings and usefulness. The User Guide and training video are provided to decrease the user's investment in learning R-SAT.

- As previously mentioned, the use of R-SAT assumes a basic understanding of the RMF Self-Assessment process. Many FRCS Stakeholders are unfamiliar with this process. The R-SAT User Guide and training video are intended to partially address this issue and better guide users in using R-SAT to complete the RMF-Self Assessment process.

1.0 INTRODUCTION

This document describes the design and application of the RMF Self-Assessment Tool (R-SAT) for owners of Department of Defense (DoD) Facility-Related Control System (FRCS). This tool serves a purpose of facilitating the application of the Risk Management Framework (RMF) and streamlining the process for obtaining Authority to Operate (ATO) network-enabled FRCS. R-SAT's operation focuses on the FRCS owner Self-Assessment consisting of preparation for and assembly of the RMF package, during RMF Steps 1-3.

The Enterprise Mission Assurance Support Service (eMASS) performs a valuable role in this overarching RMF process, and R-SAT complements eMASS with a form of guidance to DoD FRCS System Owners (SOs) engaged in the process. The complementary function of R-SAT is important because RMF packages for FRCS and Operational Technology (OT) systems are unique efforts and SOs are challenged to apply RMF to FRCS/OT systems. Additionally, FRCS SOs, who are responsible for performing self-assessments, tend to have little to no cybersecurity background or RMF experience.

Higher project costs go hand-in-hand with elongated duration of FRCS RMF projects and the inefficiencies associated with FRCS owners who are dependent on others to fulfill this aspect of their functional duties. Preventing higher project costs due to these factors are central to R-SAT's value proposition, but R-SAT also provides benefit through contributions to accelerate ATO for FRCS so corresponding energy efficiencies can be achieved – and achieved in a manner which does not carry vulnerabilities of a system whose operation is not governed by RMF.

1.1 BACKGROUND

DoD facilities employ digital and networked technologies to achieve greater energy efficiency, lower facility utility and equipment costs, and promote occupant safety and productivity. A 2017 Pacific Northwest National Laboratory (PNNL) study conducted through the U.S. Department of Energy's Building Technology Office revealed that installing currently developed and properly tuned controls could cut commercial building energy consumption by approximately 29%[1]. So, the environmental impact of these technologies and the increasingly interconnected FRCS is significant.

The increased use of network-connected FRCS comes with some risk which cannot be left unchecked. Cybersecurity requirements, such as the Unified Facilities Criteria (UFC) 4-010-06[2], provide cybersecurity requirements in the design and operation of all FRCS mitigating risks within this threat vector.

FRCS owners are typically engineers and operators that have little to no cybersecurity background and are dependent on others to perform self-assessments and manage risk. Exacerbating the issue, RMF packages for FRCS are unique, one-off efforts, leaving system owners to analyze each security control (requirement) and multiple sub-controls in relation to each of their systems. R-SAT provides forms, instructions, templates and automated tailoring in self-assessment processes

[1] https://buildingretuning.pnnl.gov/publications/PNNL-25985.pdf

[2] UFC 4-010-06, Unified Facilities Criteria, "Cybersecurity of Facility-Related Control Systems," January 18, 2017 as amended

to allow FRCS Owners to focus on tailoring the RMF package and applying security controls in ways specific to their FRCS environment.

1.2 OBJECTIVE OF THE DEMONSTRATION

The main objective of the design of R-SAT is to provide a prescriptive, step-by-step method to facilitate and accelerate RMF Self-Assessments through automation.

Supporting objectives:

- Low cost implementation
- Effective resource for all aspects of FRCS owner security planning and implementation
- Intuitive, highly repeatable and applicable across system types
- Clear delineation of cybersecurity stakeholder actions
- Government support of integration with RMF processes, such as Reciprocity and Reuse

1.3 REGULATORY DRIVERS

DoD cybersecurity and risk management policies and procedures to the unique operation of FRCS are prescribed in DoD Instruction (DoDI) 8510.01[3]. This document includes specific, tailored implementation guidance from the Assistant Secretary of Defense for Sustainment (DASD-E) [formerly the Assistant Secretary of Defense for Energy, Installations, and Environment (ASD-EI&E)] for new and legacy FRCS to secure, maintain, and provide mission assurance of the critical infrastructure and missions these systems support for DoD.

[3] DoD Instruction 8510.01: "Risk Management Framework (RMF) for DoD Information Technology (IT)," Change 2, July 28, 2017

2.0 TECHNOLOGY DESCRIPTION

2.1 TECHNOLOGY OVERVIEW

R-SAT is intended to bridge a gap for DoD FRCS system owners by providing focused, step-by-step guidance and outputs supporting an RMF Self-Assessment. Design requirements were identified based on a review of lessons learned during prior FRCS RMF Assessment and Authorization (A&A) efforts, and an analysis of existing RMF tools and resources. Additionally, coordination with RMF-related working groups helped inform design needs. A summary of project points of contact (POCs) is provided in Appendix A.

R-SAT works in conjunction with eMASS government-owned application. eMASS is a web-based Government off-the-shelf (GOTS) solution that automates a broad range of services for comprehensive, fully integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of RMF for DoD. R-SAT was developed with full recognition and appreciation for what eMASS provides and serves to advance the overall ecosystem supporting the DoD, rather than complicating DoD FRCS Owner's decision paths with alternative tool sets. In kind, several commercial software tools exist with the intent of aiding users in the completion of RMF security assessments. However, a review of these tools indicated that many are not tailored to FRCS which causes misalignment and complexity in addressing specific DoD policy. A summary of existing software tools is provided in Appendix B.

To accelerate R-SAT development and lower thresholds for user adoption, the software leverages the capability and widespread use of Microsoft Excel. Building upon the Excel application's technology, R-SAT includes an extensive set of customized Visual Basic macros in order to execute automated aspects and perform various R-SAT functions. Ease of use is accomplished as the software's structure displays a familiar tab-based Excel workbook layout and each tab guides the user through basic input questions and utilizes embedded databases to autofill eMASS importable templates.

R-SAT's workflow applies user inputs against a series of condition-specific integrated databases to produce data for additional tailoring and subsequent eMASS upload. Associated artifacts, including Policy & Procedure documentation with cross references to applicable Control Correlation Identifiers (CCIs), round out the user's interaction with R-SAT. A schematic of this process around utilization of R-SAT is provided in Figure 1. An overview of the processes is provided in the R-SAT User Guide in Appendix C.

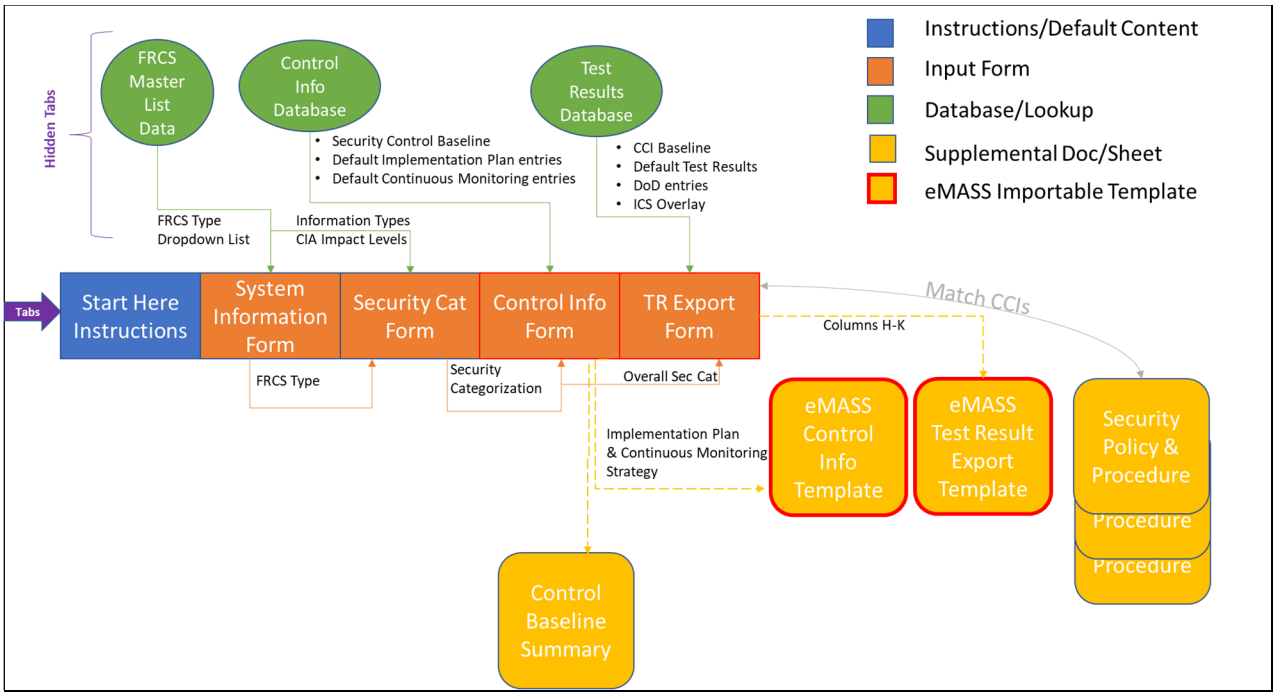


Figure 1 - Schematic of the R-SAT Process Flow

The chronology of R-SAT development followed a typical Software Development Life Cycle (SDLC) model, shaped by the Suppliers, Inputs, Process, Outputs, Customers (SIPOC) Process (elaborated upon in the next section of this document). While development of R-SAT officially started with the ESTCP award for R-SAT's development, the Planning and Analysis phases pre-dated the ESTCP award as early as 2014 with the introduction of the Federal Information Security Modernization Act. Since that time and with subsequent policy advances including but not limited to Executive Order 13800 for Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, DoD FRCS Owners have been observed grappling with how to improve the security posture of the FRCS under their management and advance through RMF to ATO.

The Concept phase officially began as the ESTCP proposal team, made up of NVESD and IPERC, put the idea of automating some of the repeated aspects common to the development of FRCS RMF packages. The team leveraged their own experience with obtaining ATOs for FRCS in their footprints or for their customers and drew upon participation in the Office of the Secretary of Defense (OSD) policy and guidance efforts[4] for FRCS cybersecurity and risk management.

Design and Implementation stages of the SDLC advanced iteratively throughout the ESTCP project period of performance until alpha versions were revealed to focus groups during April and June of 2019. R-SAT was demonstrated through an actual FRCS Self-Assessment and was validated by an Army Security Control Assessor Validator (SCA-V). Demonstration validation documentation is provided in Appendix D. The feedback received during this period (and subsequent refinements) set the stage for more extensive *Testing* of R-SAT beta versions which

[4] https://rmfks.osd.mil/rmf/

were circulated in August 2019 to a targeted population of users. Iterative development has accompanied that testing through November 2019 with *Analysis* of feedback and findings, *Design* of more refinements, and subsequent *Implementation* of those refinements for further testing – including extensive regression testing to ensure that R-SAT database integrations and automation routines maintained their functional integrity.

In conjunction with the issuance of this Final Report and ESTCP Symposium demonstrations of R-SAT, the tool package will be made available in December 2019 for full distribution through the ESTCP website. A training video will also accompany the software.

2.2 TECHNOLOGY DEVELOPMENT

R-SAT concepts were organized using the SIPOC tool[5] to summarize the relevant elements of process improvement by identifying Suppliers, Inputs, Process, Outputs and Customers. Figure 2 depicts this design process with respect to R-SAT. The technology is discussed in greater detail in the sections that follow.

Figure 2 - SIPOC Design Process

SIPOC elements in R-SAT include:

- **Suppliers:** R-SAT users.
- **Inputs:** user inputs, FRCS guidance (e.g., FRCS Master List, related National Institute of Standards and Technology (NIST) publications). It is fully anticipated that R-SAT generated responses will be further tailored by the user. The minimal level of user input required to generate a preliminary RMF package is, however, a valuable feature of R-SAT. Additionally, various policies and publications serve as "Input" and are foundational elements for RMF.
- **Process:** the auto-population by customized macros based on inputs.
- **Outputs**: R-SAT outputs include partially tailored RMF self-assessment documents, including:
    - C-I-A and Overall Security Categorization
    - Control Information and System Level Continuous Monitoring (SLCM) Plan (System Security Plan (SSP))
    - CCI Test Results
    - Baseline Control Summary

[5] In process improvement, a SIPOC (sometimes COPIS) is a tool that summarizes the inputs and outputs of one or more processes in table form. It is used to define a business process from beginning to end before work begins. Used today in Six Sigma, lean manufacturing, and business process management.

- **Customers**: the Authorizing Official (AO), Facility Managers, and roles in the Package Approval Chain who review and ultimately accept the residual risk of the FRCS.

2.2.1 Federal and DoD Policy and Publication Inputs

Federal and DoD policies and publications are the foundational elements which drive R-SAT processes. Applicable information has been entered into R-SAT (hidden tab databases), including:

- **CNSSI No. 1253**[6]**:** provides the common foundation for selection of security controls. CNSSI 1253 Table D-1 will be used to generate the preliminary selection of security controls in R-SAT.
- **FRCS Overlay**[7]**:** applies to FRCS with a Moderate-Moderate-Moderate Confidentiality-Integrity-Availability level. Refer to the Risk Management Framework (RMF) Knowledge Service (KS)[8] portal for additional information regarding the development, background, tailoring, and applicability of the FRCS Overlay. If selected, the FRCS MMM control list is used to further tailor the security controls in R-SAT.
- **NIST SP 800-82/ICS Overlay**[9]**:** provides a tailored baseline of security controls to secure Industrial Control Systems (ICS) based on the CNSSI No 1253. This ICS overlay is used to tailor the preliminary list of security controls in R-SAT.
- **NIST SP 800-53**[10]**:** provides descriptions of security controls to populate databases with standard responses in R-SAT.
- **NIST SP 800-60 Vol 1 & 2**[11&12]**:** provides a complete list of Information Types and their provisional Impact Levels. The selected Information Types (based on the selected FRCS Type from the FRCS Master List[13] in the R-SAT System Information Form) will be used to tailor the preliminary security categorization.
- **Unified Facilities Criteria (UFC) 4-010-06**[2]**:** describes requirements for incorporating cybersecurity into the design of FRCS for implementation at DoD installations. Table H-2 in UFC 4-010-06 provides guidance on controls that may be impractical or not applicable for FRCS implementation. This data will be used to tailor the security control baseline in R-SAT.
- **Tier 1 Common Controls:** addresses security controls that have requirements met by existing DoD policies (e.g., the Army Policy Record (APR) in eMASS). These common controls are auto-populated in R-SAT forms.

---

[6] Committee on National Security Systems Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014, as amended

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

[8] htpps://rmfks.osd.mil

[9] NIST SP 800-82 Revision 2, "Guide to Industrial Control Systems (ICS) Security," May 2015, as amended

[10] NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 30, 2013

[11] NIST SP 800-60 Volume 1 Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," Aug 2008

[12] 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

[13] RMF FRCS Master List, Final: June 23, 2018; posted on SERDP-ESTCP Portal https://www.serdp-estcp.org

2.2.2 System Information Form

The System Information Form serves as an offline repository where data that is useful during eMASS System Registration can be collected for future manual entry. Input fields include:

- **FRCS Type:** The DoD FRCS assets from the FRCS Master List are presented in a drop-down field list as a database of DoD FRCS assets. The assets have defined nomenclature and are mapped to the NIST 800-60 Categorized Information Types (NIST 800-60 Vol 1&2). The user selects the most appropriate FRCS Type and R-SAT generates a primary security categorization based on this selection.
- **ISO/PM Name:** The Information System Owner/Project Manager (ISO/PM) is auto-populated in various R-SAT forms to document responsibility for the self-assessment and security control implementation.
- **Component:** The DoD Component is the entity that has authorization responsibility for the system (example: Department of Navy). This entry is auto-filled on R-SAT forms to identify the Responsible Entity applicable to Component policies (Tier 2).
- **System Name:** The System Name is auto populated in various R-SAT forms as a reference.
- **Estimated Date of Self-Assessment Submission:** This date is auto populated in various R-SAT forms to document security control implementation date.

2.2.3 Security Categorization Form

This R-SAT form will generate a security categorization based on the FRCS Information Type entered by the user. R-SAT automatically selects Information Type Identifiers and Provisional Impact Levels to generate a Security Categorization for the system, based on the user-selected FRCS type selected on the System Information Form. The resulting Security Categorization can be further tailored to add/delete Information Types or manually adjust Impact Levels. The resulting Security Impact Level is used to generate the security baseline in subsequent steps in the RMF Process (Control Information Form).

2.2.4 Control Information Form - Implementation Plan/Continuous Monitoring

The Control Information Form is the baseline control set of all controls applicable to the system (RMF Step 2) based on the Overall System Security Category identified on the Security Categorization Form. Applicable controls are imported as rows in the form. The user has the option to further tailor the baseline control set by applying the ICS or FRCS-MMM overlay to set the *Implementation Status* of controls removed by the overlay to "Not Applicable". The resulting Control Information-Implementation Plan/Continuous Monitoring Plan can be exported into an offline eMASS template for further tailoring.

2.2.5 Test Result Export Form

R-SAT automatically generates the list of applicable CCIs based on the Overall System Security Category identified on the Security Categorization Form. Options for further tailoring include:

- **UFC 4-010-06:** to document controls that are not applicable according to Appendix H of the UFC. The *Compliance Status* of these controls is adjusted to "Not Applicable" and the Test Results will be populated with UFC guidance for FRCSs.
- **Policy and Procedure Templates:** The user has the option to implement Policy and Procedure (P&P) templates that accompany R-SAT that address general procedures related to organizational-level implementation of security controls. These templates are tailored to

a Low and/or Moderate Impact Level FRCS system with the ICS Overlay implemented; High Impact Level Controls are not addressed. Tailoring of results to document these templates will update R-SAT with default "Test Results" text to point to the policy document of the applicable policy template. If this option is selected, the P&P templates must be tailored, signed and implemented within the organization.

- **Tier 1 and Tier 2 DoD Inherited Controls:** addresses security controls that have requirements met by common DoD and DoD Component policies (e.g., the Army Policy Record in eMASS). The *Compliance Status* of controls covered by this inheritance will be adjusted to "Compliant" with auto-population *Date Tested (*APR Date), *Tested By* and *Test Results*.
- **Apply ICS or FRCS-MMM Overlay:** to document controls that are not applicable because of applied overlays. The *Compliance Status* of these controls will be adjusted to "Not Applicable." Test Results will document the application of the overlay.

2.2.6 Supplemental Information

Supplemental Templates and other documentation are additional outputs that accompany R-SAT. These RMF P&P templates are a collection of templates that document basic organizational procedural requirements and policies related to system cybersecurity, for "Low" or "Moderate" FRCS. A separate P&P Template is available for each NIST control family, as well as an Overview document that summaries organizational management roles and responsibility. Compliance is traced by noting the applicable CCIs collocated within the template with the policy covering the specific requirement. The documentation also includes useful information for the user, including:

- A checklist of system monitoring/operational steps related to cybersecurity
- Templates for logging important system details (authorized users, maintenance, access, audit log review)
- Documentation and configuration requirements for security standards or objectives, related to system specific controls.

2.3 ADVANTAGES AND LIMITATIONS OF TECHNOLOGY

A variety of software tools exist to support the RMF Process. Additionally, a number of customized data collection and processing software solutions are being used by or on behalf of the served audience. Although the pervasiveness of network-enabled FRCS and prevalence of cybersecurity threats within that vector are sufficiently high, uniqueness of DoD requirements and FRCS-specific nuances result in a fragmented landscape where no technology platform has a particularly dominant position.

R-SAT is unique in that it proactively seeks to position itself as a complement to the existing government-owned eMASS system. Other RMF software tools – a summary of which is provided in Appendix B – attempt to provide an end-to-end solution with varying degrees of success while others are less suited for the needs of FRCS (e.g., calibrated for higher impact levels, no application of ICS overlays).

In addition to the strategic positioning of R-SAT as described above, other advantages include:

- Users can generate a preliminary RMF package with minimal information
- User can start work on eMASS templates prior to registration of system

- RMF documentation is populated with standard responses related to FRCS and DoD inherited policy
- Overlay-driven standard responses related to FRCS and DoD policies can be used to inform responsible parties about RMF materials as "example" output
- Standard responses can easily be tailored to specific FRCS needs due to forms and output being present in the robust and familiar Microsoft Excel application
- Community-wide endorsement, advancement, and collaboration through ESTCP underwriting of R-SAT's development
- Free, no license fee utilization

Relative to alternative technologies, R-SAT has limitations including:

- Only Low and Moderate Impact level controls are address by the supplemental templates
- Narrowly defined focus on FRCS, not including individual organizational nuances

3.0 PERFORMANCE OBJECTIVES

The performance objectives and findings focused on the measurement of R-SAT's contribution in time savings and value to FRCS stakeholders. The performance objectives and findings are summarized in Table 1 and described in the section that follow. Raw data is provided in Appendix E and a detailed discussion of the findings is provided in Section 6.

Performance Objective	Metric	Data Requirements	Success Criteria	Findings
Quantitative Performance Objectives				
RMF Self-Assessment	Labor Hours	Tracking of hours to perform pilot self-assessment	>20% reduction in hours of effort, compared to past similar efforts	**Achieved** 80% based self-assessment demonstration project
CCI Baseline	Number	Untailored NIST 800-82 Low/Mod/High baselines	33% reduction of CCIs requiring manual review	**Achieved** Low Impact Level (87%) Moderate Impact Level (71%) High Impact Level (64%)
eMASS Data Entry	Time	Time required to perform manual/auto eMASS entries	>50% reduction of this duration.	**Achieved** Average reduction in time for tailored eMASS entries from 3.5 hours to 20 min. (90% reduction)
Qualitative Performance Objectives				
Usefulness	Degree of Usefulness	Likert Scale Survey	Average responses of 3.5 on survey	**Achieved** Overall Weighted Average of 3.64
User Acceptance	Customer/SME Endorsement	Written confirmation of intent to use; Targeted roles (e.g., customer, SME)	Two endorsements from personnel with RMF experience	**Not Achieved** One endorsement (Report format) was prepared by Spectrum Solutions, Inc summarized the advantages of R-SAT.

Table 1 - Performance Objectives

3.1 QUANTITATIVE – RMF SELF ASSESSMENT

This metric measures the potential time (therefore cost) savings in the activities required of a system owner in performing an RMF Self-Assessment (RMF Steps 1-3) with R-SAT vs. without it. Several stake-holders in the FRCS RMF community were asked to provide historical data for FRCS RMF efforts (without the use of R-SAT). A summary of the FRCS Stakeholder contacted to obtain data is provided in Appendix E.

The same stake-holders were also provided a copy of R-SAT and the User Guide along with a video webinar/presentation detailing the capabilities of R-SAT. Users were asked to utilize R-SAT for any future RMF Self-Assessment projects and track the hours. Additionally, an estimate of the amount of time required to familiarize themselves with R-SAT software was tracked separately.

The R-SAT software was utilized to complete an RMF Self-Assessment by IPERC for the demonstration project (Described in Section 4). The labor hours to complete the R-SAT demonstration were compared to labor hours for previously completed RMF Self-Assessments for similar (low impact level) facilities by IPERC. Additional data was not obtained by additional FRCS Stakeholders for the following reasons:

- FRCS Stakeholders did not have sufficient data to provide an estimate of the hours to complete RMF Steps 1-3.
- FRCS Stakeholder were not familiar enough with the RMF steps to use the software. Many were interested in more training on the RMF process as part of the R-SAT demonstration.
- FRCS Stakeholder did not have a pending FRCS Self-Assessment within the time window required to obtain data.

3.2 QUANTITATIVE –CCI BASELINE

The Test Results Export Form documents implementation of all controls applicable to a system (RMF Step 3) and is an artifact required in eMASS. Each of the CCIs represents a specific security requirement that the SO must address and document. A summary of the number of CCIs applicable to the CNSSI for a Low, Moderate and High Impact Level Security Categorization are 1401, 1665 and 1889, respectively.

The R-SAT software auto-populated the Test Results Export Form with standard responses based on user input options that are address by the following:

- DoD or Service Specific Policy; Document Compliance based on existing published policy
- ICS or FRCS MMM Overlay; Document Non-Applicability based on application of overlay
- Unified Facility Criteria Cybersecurity of Facility-Related Control Systems (UFC 4-010-06); Document Non-Applicability based on Appendix H-2
- Policy and Procedures documentation developed to supplement the R-SAT software; Document Compliance based on supplemental documents.

The overall number of CCIs addressed by R-SAT auto population was summarized to estimate the time savings recognized by R-SAT addressing a portion of these CCIs. This reduction in the number of CCIs to address will be used demonstrate the reduction of work to develop an RMF package.

3.3 QUANTITATIVE – eMASS DATA ENTRY

This time estimate for manual data entry into eMASS will be compared to the amount of time to auto-populate the same number of controls with the R-SAT automated method. Users must access a dashboard for eMASS input. The amount of time for a user to complete the data entry for an individual control from the eMASS dashboard was estimated by IPERC staff to take 20 seconds

for each entry. The amount of time required to perform a single entry was multiplied by the number of R-SAT populated CCIs, described in the previous section, to obtain an estimate of the time to manually enter data into eMASS.

R-SAT has the capability to export data into an eMASS Control Information Form, SLCM Form and Test Results Export Form. This time estimate for a user to complete the R-SAT forms, export of the R-SAT data into the eMASS template and import the eMASS template was also recorded. The purpose of these measurements will be used to demonstrate a reduction of time to enter data into eMASS with the use of the export feature in R-SAT.

3.4 QUALITATIVE – USEFULNESS

Several stake-holders in the FRCS RMF community were asked to provide an evaluation of the usefulness of R-SAT. This solicitation was done through outreach efforts between August 2019 and November 2019 and following a short course demonstration of R-SAT at the ESTCP Symposium in December 2019. A summary of the data obtained is provided in Appendix E.

Participants were asked to complete questions using a Likert scale survey (1=negative to 5=positive) to assess the usefulness of R-SAT. Survey questions are summarized below:

- Did/Would the FRCS A&A Framework save you time doing your RMF Self-Assessment?
  (1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
- Did/Would the FRCS A&A Framework help you assess risk in your control system?
  (1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
- Did/Would the FRCS A&A Framework help you reduce risk in your control system environment?
  (1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
- Did/Would the FRCS A&A Framework facilitate or accelerate obtaining Authorization to Operate?
  (1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
- How would you rate the overall usefulness of the FRCS A&A Framework?
  (1) Not useful; (2) A little useful; (3) Useful; (4) Very useful; (5) Indispensable
- Do you intend to use the FRCS A&A Framework for future projects?

  Yes/No

3.5 QUALITATIVE – USER ACCPTANCE

Written customer/SME endorsement provide data to confirmation of intent to socialize/use in specific FRCS footprints. Endorsements of R-SAT inherently establishes a comparison to the current state. Additionally, positive comments received during outreach efforts (demonstrations, ESTCP Symposium Poster session and Short-course) demonstrate user acceptance. A simple count of endorsements and analysis of endorsement content will be used as the source for quality of commitment (e.g., from SME with large FRCS owner following, glowing review, total number of endorsements void of significant suggestions for change).

4.0 FACILITY/SITE DESCRIPTION

The proposed framework was demonstrated by using it during a Self-Assessment (RMF Steps 1-3) of the US Army Garrison Kwajalein-Atoll (USAG-KA) Meck Island Microgrid. Specifically, R-SAT was used to develop the Security Categorization, tailor this categorization and populate the Control Information (System Security Plan) and Test Result eMASS templates. The control baseline was further tailored then approved by the AO. The eMASS Test Results template was imported to eMASS, and system validation occurred in September 2019. The generated templates, control baseline approval memo and excerpt from SCA-V out-brief showing the team as being "well prepared for the assessment" are provided in Appendix D. An ATO is pending for this system.

4.1 FACILITY/SITE LOCATION AND OPERATIONS

The selected USAG-KA Meck Microgrid is representative of other military DoD FRCS which require an ATO. Specific details and maps of the facility operations and microgrid control system are Sensitive and are not relevant to the scope of the R-SAT demonstration.

4.2 FACILITY/SITE CONDITIONS

The selected USAG-KA Meck Microgrid was determined to have provisional impact levels of Low for Confidentiality, Integrity and Availability. The USAG-KA Meck Microgrid operates in a Closed Restricted Network (CRN) consisting of the microgrid controllers, networked photovoltaics and energy storage, and various other monitoring equipment and microgrid end devices. The facility is representative of a Microgrid Control System as identified on the FRCS Master List. The control system is comprised of GridMaster® Intelligent Power Controllers (IPCs) that coordinate all microgrid activity, communicating with each other using a proprietary, encrypted protocol. System data and control is accessed through a graphical user interface (GUI) using a web browser on the networked human machine interface (HMI) computers. Control communication with the end devices is exclusively Modbus/Transmission Control Protocol. Based on the components present in the Microgrid Control System, the ICS overlay was applicable.

5.0 TEST DESIGN

5.1 CONCEPTUAL TEST DESIGN

The Conceptual Test Design for R-SAT involved identifying test conditions, test cases, and test data and applying quantitative and qualitative analysis to gauge the extent to which pre-determined Performance Objectives, summarized in Section 3, were achieved.

Performance Measurement involved collecting data from DoD FRCS Owners and representatives with RMF responsibilities. The scope of FRCS Types eligible for inclusion match those which had previously been identified by DASD-E via the FRCS Master List. Data collection processes were made consistent through use of a survey form whether the respondent provided the feedback directly or as part of a structured interview.

Performance metrics from outside users was collected between August 2018 through the Short Course demonstration at the ESTCP Symposium on December 5, 2019. A summary of the data collected is provided in Appendix E. Through collection of this data, the test sought to delineate respondent perspectives involving:

- Comparative analysis of RMF Process when engaging WITH and WITHOUT the R-SAT software
- Efficacy of Security Categorization selection and provisional impact levels based on NIST SP 800-60
- Population of a baseline Implementation Plan and Continuous Monitoring Strategy
- The Test Results Export using the Security Categorization to populate the eMASS Test Results Export Template from NIST SP 800-82
- Autofill of the eMASS Import Template populated by R-SAT and readied for import into eMASS

5.2 BASELINE CHARACTERIZATION

To quantify a baseline for some of the time savings metrics of the R-SAT demonstration, the number of sites[14] per military service (just in the United States) and Washington Headquarters Service (WHS) was pulled from the DoD Base Structure Report FY 2018 Baseline. A conservative assumption was made there are just three FRCS RMF Authorization Boundaries per site (some sites have no facilities) consisting of unique FRCS types (e.g., Utility Monitoring & Control System (UMCS), Physical Access Control System (PACS)), and an average of three different system Designers for each type. This equals an estimated number of self-assessments to be performed and maintained just in the DoD, let alone the entire Federal footprint. These estimates, summarized in Table 2, may be used to get an overall picture per R-SAT demonstration metric of the potential benefits of its use.

[14] Site: A specific geographic location that has individual land parcels or facilities assigned to it. Physical (geographic) location that is, or was owned by, leased to, or otherwise under the jurisdiction of a DoD Component on behalf of the United States. A site may be contiguous to another site but cannot geographically overlap or be within another site. A site may exist in one of three forms: land only – where no facilities are present; facility or facilities only – where there the underlying land is neither owned nor controlled by the government, and land with facilities – where both are present.

Branch	# of Sites	# of FRCS RMF	# FRCS Types/Designers
Army	1,565	4,695	14,085
Navy	785	2,355	7,065
Air Force	1,535	4,605	13,815
Marines	190	570	1,710
WHS	75	225	675
Total:	**4,150**	**12,450**	**37,350**

Table 2 - Estimate of FY 2018 DoD FRCS RMF Self-Assessments

5.3 DESIGN AND LAYOUT OF TECHNOLOGY COMPONENTS

The technology of R-SAT is an end-to-end framework focused on FRCS Owner's in-practice duties for RMF ATO such that roles, processes, available tools and resources are clear and assist with the integration of automation and streamlining techniques where possible. Individual elements of R-SAT are described below.

5.3.1 R-SAT User Guide

The User Guide (Appendix C) describes in detail how a series of tools, guidance, instructions, forms and templates integrated within R-SAT facilitate and accelerate the System Owner's RMF Self-Assessment including:

- Security Categorization
- Applying the ICS or FRCS MMM Overlay to the security control baseline and other tailoring
- Development and guided implementation of FRCS-specific security policies and procedures

5.3.2 R-SAT Software

The underlying technology of R-SAT is an Excel macro-enabled workbook with several Worksheets. The Visual Basic programming of the macros applies user selections to content from R-SAT's integrated databases. The result is auto-population of eMASS templates with "standard" responses based on FRCS characteristics. This auto-population and production of RMF artifacts for eMASS helps system owners comply with eMASS documentation requirements by providing security controls broken down into specific objectives identified by CCIs. Furthermore, the R-SAT generated forms mirror DoD eMASS templates in order to facilitate and expedite subsequent uploading of completed templates into eMASS.

Components within R-SAT include:

- Instructions tab (color coded blue) and popup menus which, in conjunction with the R-SAT User Guide and training videos, guide the user through the necessary input selections and options to tailor the auto populated data.
- User Input forms on R-SAT's orange color-coded tabs (also shown in Figure 1)
- R-SAT data summary on yellow-coded tabs
- Five "hidden" worksheets containing lookup tables and databases used by R-SAT to auto-populate templates. These tabs have fixed data and are not modifiable by the user.

Field-level entries are color-coded as well in order to highlight values which are to be provided by R-SAT users in order to direct corresponding form output.

- *Orange* cells are fields that require data entry by user. The data in these fields is used in subsequent R-SAT forms.
- *Green* cells are fields that are optional data entry by user. These fields aid in documentation of the RMF process but do not require input.
- *Grey* cells are data fields that are not in applicable given the current entries in other R-SAT fields; the color of these data fields may change to Orange (required) based on information entered by user.

5.3.3 R-SAT Supplemental Templates

Supplemental Security P&P Templates accompany the R-SAT software. These optional documents address security control best practices that are typically implemented at the organizational level. These supporting templates serve as a starting point to implement and document organization-level implementation of security controls (i.e., acceptable use restrictions or assurance requirements). This set of documents includes:

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

5.3.4 R-SAT Training Video

A training video provides a demonstration of the forms in R-SAT and is intended to accompany the software to provide an example of the functionality.

5.4 OPERATIONAL TESTING

This sectional is largely not applicable to R-SAT. "Operational phases" of R-SAT are described in Section 2.2. "Operational testing" consisted simply of performing R-SAT processes to ensure macros function as expected and by importing R-SAT-populated eMASS templates into eMASS to ensure no unexpected errors occurred.

5.5 SAMPLING PROTOCOL

The R-SAT software was presented and promoted at the 2019 Energy Exchange Conference. In addition, the points of contact listed in Appendix A, promoted and shared the R-SAT software with professional contacts. Based on this outreach, outside users (FRCS Stakeholders) were sampled to obtain data for performance metrics between August 2018 through the Short Course demonstration at the ESTCP Symposium on December 5, 2019.

5.6 SAMPLING RESULTS

Feedback received during outreach efforts identified that many FRCS Stakeholders are unfamiliar with the RMF Process. Many potential users that were asked to evaluate R-SAT were unable to provide quantitative feedback because of unfamiliarity with the process. Some potential users requested additional training on the RMF process, during the demonstration of R-SAT. The R-SAT User Guide and training video were modified during the design phase to partially address this issue and better guide R-SAT users through the RMF-Self Assessment process; however, use of R-SAT assumes a basic understanding of RMF.

6.0 PERFORMANCE ASSESSMENT

6.1 QUANTITATIVE – RMF SELF ASSESSMENT

The estimated labor hour savings was used to determine the Cost/Benefit of R-SAT Specifically, a measure of the potential time (therefore cost) savings in the activities required of a system owner in performing an RMF Self-Assessment (RMF Steps 1-3) with the framework vs. without it. A summary of the data collected during the demonstration (described in Section 4) is provided in Table 3. The time savings was 80%. For the purpose of this performance objective, a 20% decrease in labor hours was determined to demonstrate success; therefore, this metric was achieved. The data for this metrics demonstrates a time savings for a user that was familiar with the RMF process and R-SAT software.

Activity	**Labor Hours**	
	without R-SAT	**with R-SAT**
Tool familiarization		2
System Information Collection	5	1
Preliminary Security Categorization	5	2
Implementation Plan	12	5
Strategy for Continuous Monitoring	12	5
Security Control Selection Baseline	63	4
TOTAL	97	17
Percent Difference	80%	

Table 3 - Summary of RMF Labor Hours for R-SAT Demonstration Project

6.2 QUANTITATIVE –CCI BASELINE

A summary of the CCIs address by various user options in the R-SAT process is summarized in

SCENARIO	IMPACT LEVEL		
	Low	Mod	High
CNSSI (Baseline)	1401	1665	1889
UFC [CCIs addressed by R-SAT]	36	53	53
Percent Reduction	**2.6%**	**3.2%**	**2.8%**
Policy and Procedures documentation [CCIs addressed by R-SAT]	366	389	389
Percent Reduction	**26%**	**23%**	**21%**
DoD/Service Specific Policy [CCIs addressed by R-SAT]	415	457	486
Percent Reduction	**30%**	**27%**	**26%**
ICS overlay [CCIs addressed by R-SAT]	395	278	273
Percent Reduction	**28%**	**17%**	**14%**
FRCS overlay [CCIs addressed by R-SAT]	13	32	32
Percent Reduction	**0.9%**	**1.9%**	**1.7%**
Cumulative CCIs addressed by R-SAT: (ICS Overlay+DoD/Service Specific + Policy Templates + UFC)	1212	1177	1201
Cumulative Percent reduction (ICS Overlay+DoD/Service Specific + Policy Templates + UFC)	**87%**	**71%**	**64%**
Cumulative Percent reduction (UFC + FRCS MMM Overlay)	3.5%	5.1%	4.5%
Cumulative Percent reduction (UFC + FRCS MMM Overlay+ P&P)	30%	28%	25%
Cumulative Percent reduction (UFC + FRCS MMM Overlay+ P&P+ DoD/Service)	59%	56%	51%
Cumulative Percent reduction (UFC + ICS Overlay)	31%	20%	17%
Cumulative Percent reduction (UFC + ICS Overlay+ P&P)	57%	43%	38%
Cumulative Percent reduction (UFC + ICS Overlay+ P&P+ DoD/Service)	87%	71%	64%
Percent Reduction Average of All Scenarios	**44%**	**37%**	**33%**

Table 4. A description of each scenario is provided in the User Guide (Appendix C).

SCENARIO	IMPACT LEVEL		
	Low	Mod	High
CNSSI (Baseline)	1401	1665	1889
UFC [CCIs addressed by R-SAT]	36	53	53
Percent Reduction	**2.6%**	**3.2%**	**2.8%**
Policy and Procedures documentation [CCIs addressed by R-SAT]	366	389	389
Percent Reduction	**26%**	**23%**	**21%**

DoD/Service Specific Policy [CCIs addressed by R-SAT]	415	457	486
Percent Reduction	**30%**	**27%**	**26%**
ICS overlay [CCIs addressed by R-SAT]	395	278	273
Percent Reduction	**28%**	**17%**	**14%**
FRCS overlay [CCIs addressed by R-SAT]	13	32	32
Percent Reduction	**0.9%**	**1.9%**	**1.7%**
Cumulative CCIs addressed by R-SAT: (ICS Overlay+DoD/Service Specific + Policy Templates + UFC)	1212	1177	1201
Cumulative Percent reduction (ICS Overlay+DoD/Service Specific + Policy Templates + UFC)	**87%**	**71%**	**64%**
Cumulative Percent reduction (UFC + FRCS MMM Overlay)	3.5%	5.1%	4.5%
Cumulative Percent reduction (UFC + FRCS MMM Overlay+ P&P)	30%	28%	25%
Cumulative Percent reduction (UFC + FRCS MMM Overlay+ P&P+ DoD/Service)	59%	56%	51%
Cumulative Percent reduction (UFC + ICS Overlay)	31%	20%	17%
Cumulative Percent reduction (UFC + ICS Overlay+ P&P)	57%	43%	38%
Cumulative Percent reduction (UFC + ICS Overlay+ P&P+ DoD/Service)	87%	71%	64%
Percent Reduction Average of All Scenarios	**44%**	**37%**	**33%**

Table 4 - Summary of CCIs Addressed (Percent Reductions) by R-SAT

The percent reduction of CCIs addressed is dependent on the R-SAT input options selected by the user. The total CCIs addressed by various input options ranges from 0.9% (User application of only the FRCS MMM overlay for a Low Security Categorization) to 87% (cumulative application of the UFC, ICS Overlay, DoD/Service Policies and R-SAT Policy & Procedures documents for a Low Security Categorization).

The average percent reduction in the number of CCIs addressed is 44% (Low Impact), 37% (Moderate Impact), and 33% (High Impact). For the purpose of this performance objective, a one-third (33%) decrease in the number of CCIs to address was determined to demonstrate success. Therefore, this metrics demonstrates that the R-SAT is a time savings to the user. The greatest benefit is achieved when the ICS overlay is applied and the full suite of scenarios are selected. The average percent reduction in the number of CCIs addressed for this scenario is 87% (Low Impact), 71% (Moderate Impact), and 64% (High Impact). A visual representation of this scenarios is represented in Figure 3.

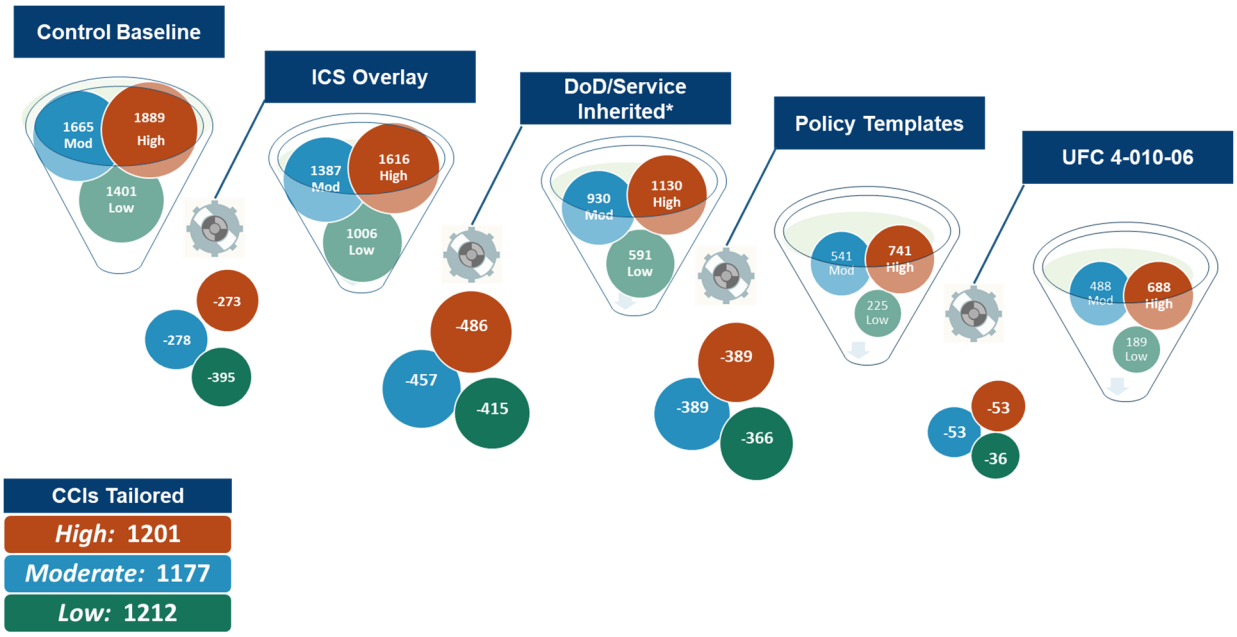


Figure 3 - R-SAT CCI Reduction Representation

6.3 QUANTITATIVE – eMASS DATA ENTRY

This time estimate for the manual entry of data into eMASS will be compared to the amount of time to populate the same number of controls with the automated method (R-SAT). The estimated time to enter data for a single CCI into eMASS is approximately 20-seconds per record. This single data entry estimate was multiplied by the number CCIs address by various user options in the R-SAT process. The overall time savings is presented in Table 5.

SCENARIO	IMPACT LEVEL		
	Low	Mod	High
CNSSI (Baseline)	1401	1665	1889
Level of Effort (Hrs)	**7.8**	**9.3**	**10.5**
UFC	36	53	53
Time savings	**0.2**	**0.3**	**0.3**
Policy and Procedures documentation	366	389	389
Time savings	**2.0**	**2.2**	**2.2**
DoD/Service Specific Policy	415	457	486
Time savings	**2.3**	**2.5**	**2.7**
ICS overlay	395	278	273
Time savings	**2.2**	**1.5**	**1.5**
FRCS overlay	13	32	32
Time savings	**0.1**	**0.2**	**0.2**
Overall (with ICS Overlay)	1212	1177	1201
Time savings	**6.7**	**6.5**	**6.7**
Cumulative Times Savings (Hrs) (UFC + FRCS MMM Overlay)	0.3	0.5	0.5
Cumulative Times Savings (Hrs) (UFC + FRCS MMM Overlay+ P&P)	2.3	2.6	2.6
Cumulative Times Savings (Hrs) (UFC + FRCS MMM Overlay+ P&P+ DoD/Service)	4.6	5.2	5.3
Cumulative Times Savings (Hrs) (UFC + ICS Overlay)	2.4	1.8	1.8
Cumulative Times Savings (Hrs) (UFC + ICS Overlay+ P&P)	4.4	4.0	4.0
Cumulative Times Savings (Hrs) (UFC + ICS Overlay+ P&P+ DoD/Service)	6.7	6.5	6.7
Cumulative Times Savings (Hrs) Average of All Scenarios	3.5	3.4	3.5

Table 5 - Summary Time (Hours) Required to Manually Address R-SAT tailored CCIs

The time savings is dependent on the R-SAT input options selected by the user. The time savings ranges from 6-minutes (User application of only the FRCS MMM overlay for a Low Security Categorization) to 6.7-hours (cumulative application of the UFC, ICS Overlay, DoD/Service Policies and R-SAT Policy & Procedures documents for a Low or High Security Categorization). The average time savings, based on a reduction in the number of CCIs is 3.5-hours (Low and High Impact) and 3.4-hours (Moderate Impact).

An estimate of the time for a user to enter data into R-SAT and generate a Test Result form with populated data was determined to be 20-minutes for a user familiar with the software and tailoring options. For the purpose of this performance objective, a decrease in the level of effort as measured by time duration to complete an eMASS data entry of 50% or greater was determined to demonstrate success; therefore this metrics demonstrates a time savings with the use of R-SAT. It is recognized that this time savings does not account for the remaining CCIs that must be manually tailored by the user.

6.4 QUALITATIVE – USEFULNESS

A summary of the collected survey data is summarized in Table 6.

Name and Organization	Years of Experience with RMF Process:	Questions - See notes at bottom of table for stated question; Responses are based on scale from lowest (1) to greatest (5)					
		A	B	C	D	E	F
Bianca Nacu; Peregrine Technical Solutions	Beginner (<1 yr)	2	2	2	5	2	3
Alex Gordon; Peregrine Technical Solutions	Experienced (6 yrs)	2	2	3		1	3
Chinook Systems *	Experienced (5 yr)	2	2	1	5	1	2
Fred Parry; Dominion Energy	Beginner	4	4	4	4		
Doug Van Werdon; Rock Island Arsenal	Beginner	5	5	5	5		
Tapan Patel; USACE	Expert	5	4	5	5		
Jim Lee; Cimetrics Inc.	Beginner	5	5	5	5		
Charles Morris; KBR, Inc.	Expert	3	3	3	4		
Chuck Purcell; Noblis	Beginner		4	4			
Joe Zhou; Slipstream Group	Beginner	4	4	4	4		
Chuck Hammock; Andrews, Hammock & Powell	Beginner	4	4	4	4		
Bryan Urban; Fraunhofer USA	Beginner	5	5	5	5		
Average		4	4	4	5	1	3
Weight Factor (based on total number of responses)		21%	23%	23%	19%	7%	7%
Overall Weighted Average	3.64						

Note: Blank entries indicate no response or no opportunity to answer
QUESTION A: Did/Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?
QUESTION B: Did/Would the FRCS RMF Tool help you assess risk in your control system?
QUESTION C: Did/Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?
QUESTION D: What is the likelihood that you intend to use the RMF Tool for future projects?
QUESTION E: Did/Would the FRCS RMF Tool help you reduce risk in your control system environment?
QUESTION F: How would you rate the overall usefulness of the FRCS RMF Tool?

Table 6 - Summary of R-SAT User Survey Responses

Some of the respondents selected to not answer certain survey questions; these are the blank entries in Table 6. In addition, some of the questions were deemed inappropriate for the users that attended the ESTCP Short Course demonstration of R-SAT; these are the shaded entries in the table. The response values were averaged for the analysis of usefulness. A weight factor was applied to the responses based on the total number of data points collected for each question. The overall average for each response questions is summarized in the final row of Table 6. The weighted average for all response questions is 3.64. For the purpose of this performance objective, an average answer of >3.5 was determined to demonstrate success; therefore this metrics demonstrates the usefulness of R-SAT.

6.5 QUALITATIVE – USER ACCPTANCE

A summary of written endorsements is provided in Table 7. A written report summarizing a review of the RFCS RMF Tool (R-SAT) was received from Bethany Hill, CISSP of Spectrum Solutions, Inc and is included as Appendix E. The report offers a subjective evaluation of R-SAT by an experienced user. Additionally, comments obtained from attendees of the ESTCP Symposium short-course are summarized to document user acceptance.

User		**Summary of Comments** Original Documents provided in App E:
Beth Hill, CISSP Spectrum Solutions, Inc.		Excerpts from Evaluation: • The FRCS RMF Self-Assessment Tool can help an inexperienced individual to navigate through the first three steps of the RMF process. Also, the FRCS RMF Self-Assessment Tool can save time in completing the self-assessment. • The FRCS RMF Self-Assessment tool can be used by someone when the user does not have an eMASS account. • There are few disadvantages of using a tool like the FRCS RMF Self-Assessment Tool and the advantages far outweigh the disadvantages.
Mike Chipley, PhD GICSP PMP LEED AP PMC Group		With the tool, it should shave off at least 8 days of manual copy paste (to complete RMF Self Assessments), but I have not been able to do a test run import to see that it actually works, or if any import errors/bugs appear.
User Feedback Summary		Useful as a reference document; almost a dynamic textbook
Symposium Short Course Comments		Awesome!! Will be able to point other users to this tool.

Table 7 – Summary of R-SAT User Written Endorsements

An analysis of endorsement content and source for quality of commitment demonstrates an excitement among FRCS stakeholders. For the purpose of this performance objective, two "quality" endorsements from personnel familiar with RMF process will be used to demonstrate success; therefore, this performance objective was not met. One written endorsement was obtained in addition to several positive comments on user surveys. Opportunities for future enhancements and updates to R-SAT's integrated databases exist for R-SAT, but – based upon feedback received through alpha and beta period – the December 2019-released software is expected to be widely accepted by the RMF FRCS community for the support and contributions R-SAT offers to reduce the time for RMF Self-Assessment Steps 1-3.

7.0 COST ASSESSMENT

7.1 COST MODEL

R-SAT is free for public use and performance metrics in terms of labor hours have already been provided in other sections of this report, so rather than assessing costs for the implementation of R-SAT, cost estimates for ongoing maintenance of R-SAT by a designated Federal organization are provided. A summary of annual maintenance costs is provided in Table 8.

Cost Element	Data Analysis/Assumptions	Estimated Annual Costs
Hardware capital costs	Assumes use of existing workstation.	$0
Initial Familiarization	Average of labor hours required to learn to use R-SAT based on metrics gathered during demonstration	$1,120 7 hours*fully burdened labor rate
Maintenance	Estimate based on labor hours required to incorporate pilot user feedback into R-SAT during demonstration and testing.	$16,000 100 hours*fully burdened labor rate
Additional feature implementation	Estimate based on 50% labor hours required to identify, assess, and engineer R-SAT features during design phase	$27,200 170 hours*fully burdened labor rate
User training and materials update	Estimate based on development of user guide, webinar, and course materials during demonstration	$20,560 128.5 hours*fully burdened labor rate
Publishing	Estimate based on labor hours to coordinate initial publishing of R-SAT and associated documents to two different websites.[1]	$1,600 10 hours*fully burdened labor rate

[1] rmfks.osd.mil; https://www.serdp-estcp.org/

Table 8 - Cost Model for Annual R-SAT Maintenance

7.1.2 Cost Elements

Hardware Capital Costs:
The cost model assumes a workstation is available to run Microsoft Office, so no capital costs are anticipated.

Initial Familiarization:
The cost model provides an estimate of the number of hours needed for maintainer of R-SAT to become familiar with R-SAT, its design, functionality and underlying database. Estimated hours are based on development team interviews of partner and pilot user time required to familiarize themselves with R-SAT. The estimate represents an average to account for varying familiarity with RMF process from novice to expert.

Maintenance:
Some maintenance will be required for upkeep of R-SAT. Estimated annual hours are based on labor hours required to incorporate pilot user feedback into R-SAT during demonstration. This includes validation and testing of the recommended changes. It is assumed that continual updates to R-SAT will be required to keep in step with eMASS and RMF policy changes.

Additional Feature Implementation:
Some recommended feature updates are included in this report. It is anticipated that additional desired features will be identified over time. The labor hours estimate provided is based on labor hours required to identify, assess, and engineer R-SAT features during the design phase.

User Training and Materials Update:
User instructions and training materials have been provided. These items will need a periodic refresh aligned with R-SAT updates over time. The cost model estimate is based on labor hours applied in development of the User Guide, webinar, and Symposium course materials development during the demonstration and outreach phases.

Publishing:
R-SAT will be published to two websites: 1) the RMF-KS, and 2) the ESTCP portal, Cybersecurity page. These postings must be maintained. The cost model estimate is based on labor hours to coordinate initial publishing of R-SAT and associated documents to these two websites.

7.2 COST DRIVERS
Implementations of R-SAT carry little to no costs. However, it is recommended that a Federal organizational owner of R-SAT be identified to manage the ongoing maintenance in accordance with the Cost Model.

7.3 COST ANALYSIS AND COMPARISON
Operationally, there are no additional costs for implementation. The cost elements described are for optional, Federal life-cycle costs for overall maintenance and updates to R-SAT. Annual cost estimate are provided in the cost model. These costs, in comparison to manual RMF Self-Assessment processes are eclipsed by time savings for users of R-SAT.

8.0 IMPLEMENTATION ISSUES
User feedback and input on R-SAT was not realized at the expected level. Lack of participation is somewhat attributed to the short timeline for the project. The software development phase was extended to address several comments received by users throughout the demonstration phase. This ensured that the R-SAT software and corresponding User Guide addressed the needs of the FRCS

stakeholders. In addition, a training video was developed to ensure that potential users have visual resources to facilitate the use of R-SAT.

R-SAT 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 R-SAT via email should be avoided. Download of R-SAT from the RMF-KS and ESTCP portals should be facilitated by the appropriate government personnel and process.

R-SAT is a tool that requires a learning curve for users in order to understand the functionality and tailoring options. The software was designed to be intuitive and user friendly; however, users must be willing to invest upfront time in learning the software. This unwillingness to invest time in learning a new program was recognized by the team when attempting to obtain metrics for R-SAT's time savings and usefulness. The User Guide and training video are provided to decrease the user's investment in learning R-SAT.

R-SAT functionality may be impacted by updates to eMASS or FRCS policy and guidance. Updates to R-SAT will be necessary to keep pace. Additionally, there were several design choices to not implement certain features for a variety of reasons, such as uncertainty of user acceptance, keeping R-SAT useful for a broad number of users, and the level of complexity of implementation. These features are summarized below and could be incorporated in future versions:

- Organizational Policy templates are included as a supplemental resource with R-SAT. The text for these documents could be incorporated into R-SAT databases to allow system specific Organizational Policy documents to be generated based on user selections.

- Privacy Controls are not currently addressed by R-SAT. A version 5 update to NIST 800-53 includes a major change to fully integrate the privacy controls into the security control catalog and create a mapping and summary for these controls. After NIST 800-53 v5 is published, Privacy Controls could be incorporated into R-SAT databases and allow an optional feature for users to select privacy and include any applicable controls.

- Overlays are specialized sets of controls tailored for specific types of mission/business functions, technologies or environments. R-SAT applies the ICS or FRCS MMM Overlay. Future version of R-SAT could incorporate additional standardized and approved overlays applicable to FRCS. Example: R-SAT could provide the CCI specifications for the Designer based on this list from the UFC.

Appendix A: Points of Contact

POINT OF CONTACT Name	ORGANIZATION Name Address	Phone Fax E-mail	Role in Project
Aura Lee Keating	IPERC 4321 Mulligan Street, Longmont, CO 80504	Skype: (405) 294-3566 iMsg, Cell: +49 152 29884654 AuraLee.Keating@IPERC.com www.IPERC.com	Lead Designer
William Horner	Operations Division C5ISR Center, NVESD U.S. Army Combat Capabilities Development Command (DEVCOM)	DSN 654-2855 william.h.horner4.civ@mail.mil william.h.horner4.civ@mail.smil.mil	Principal Investigator
William Elliott, CTR	Master Planner Facilities & Energy Army Futures Command CCDC, C5ISR Ft. Belvoir, VA	Office: 703-704-2698 Cell: 202-391-9564 e-mail: william.j.elliott60.ctr@mail.mil	DoD Partner
Kevin Brady	Special Staff to the Garrison Commander for Energy and Special Projects Fort Belvoir, VA 22060 AFC, CCDC, C5ISR, Operations Div	Work Cell: 703-946-7418 Primary Work NIPR email: kevin.w.brady.civ@mail.mil SIPR email: kevin.w.brady@us.army.smil.mil	DoD Partner
Bethany Hill, CISSP	Spectrum Solutions, Inc 114 Castle Drive Madison, AL 35758	Phone: (256) 799-2437 Email Address: bhill@spectrumsi.com Email Address: Bethany.s.hill2.ctr@mail.mil	Demonstration Participant

Appendix B: Summary of Existing RMF Tools

eMASS, MC-CAMS

eMASS is a web-based Government off-the-shelf (GOTS) solution that automates a broad range of services for comprehensive, fully integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) for Department of Defense (DoD). The features are tailored to DoD RMF requirements, DOD Information Assurance Certifications, and applicable Federal Information Security Management Act (FISMA) reporting. All functionality in eMASS is derived from the RMF policy established in the National Institute of Standards and Technology (NIST) Special Publications as well as the respective RMF Knowledge Services (KS) and Technical Advisory Groups (TAGs) of each organization. Users must access a dashboard for eMASS input; however, many of the eMASS reporting fields can be exported to Excel spreadsheets. R-SAT will be designed to auto populate the eMASS exported spreadsheets and streamline the process.

CSET

CSET is a widely used, web-based tool that guides the user through a series of questions to collect facility-specific information. The questions are tailored using relevant security standards and regulations, specific industry considerations, and user selected security assurance levels (low, mod, high). The output reports summarizing facility compliance, with recommendations for improving cybersecurity posture. CSET has robust options, however, there are limitations for eMASS applications for DoD FRCS. DoD requirements are not filtered from the CSET question set and a user must manually enter comments for each of these control fields when using the software. CSET 9.0 does allow an option for a user to import modules to tailor a questions/requirement set; however, it is unclear if the module would be useful to RMF templates or relevant in future versions of the software. CSET uses a unique catalog number for control requirements. This is due to the numerous security standards included in the software. The existing CSET catalog numbers do not appear to correlate well to the RMF fields. It does not appear that CSET controls are granular enough for the eMASS CCI correlation. For these reasons, the CSET software will not be modified to compliment the eMASS system as a component of this contract.

Quicx

Quicx is a browser-based application which provides electronic record for centralized documentation and database management of project and commissioning tasks throughout each stage of the project; i.e., pre-design/design phase, construction, transition, and facility assessment.

RMF Eagle Toolset

The RMF Eagle Tool was created by CACI to automate and streamline Assessment and Authorization. The tool automates continuous monitoring procedures, and aids in program management visibility. RMF Eagle Toolset contains all NIST and DoD standards and is customizable to suit individual program needs. This tool is only available to CACI personnel can only be accessed through CACI-owned laptops for cyber services rendered. For this reason, the RMF Eagle Toolset is not a viable option for ease of access and utilization by all FRCS System Owners.

Keystone RMF Workflow Enhancement Tool

The Keystone RMF Workflow Enhancement Tool was designed to support the RMF assessment process and optimize workflow for System Owners, Self-Assessment, and Validation. The tool provides an efficient means to manage the RMF process and its CCIs. The tool runs offline and has export/import capabilities that support instant population of eMASS test results.

Xacta 360

Xacta 360 enables risk management and compliance of cloud-based, on premises, and hybrid systems. The tool automates processes for A&A, remediation, and ongoing compliance. Xacta is available as an on-premises, hosted, or SaaS solution, however, it only covers cloud compliance. Xacta would not cover Facility Related Control Systems.

TFIMS

The Department of Treasury's (DoT) Treasury Directive Publication (TD P) 85-01, and DoT's Information Technology (IT) Security Program, requires DoT bureaus to upload required artifacts into the "Treasury Federal Information Security Modernization Act of 2014 (FISMA) Inventory Management System" (TFIMS).

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The FedRAMP package includes many Excel Checklists and Templates specific to assessing compliance with NIST controls, which are applicable to FRCSs. Existing FedRAMP Checklists and Templates will be reviewed to collect relevant data fields. For example, the FedRAMP Security Assessment Plan Template has assessment procedures broken into three categories (examine, interview, test) and may be useful to build an assessment related questions within R-SAT. The FedRAMP templates are not easily tailorable to a specific organization or system. Additionally, this software is not user-friendly for control system owners without a cybersecurity or risk management background. Finally, the FedRAMP software does not allow the user to apply the ICS or FRCS MMM overlay.

ESTCP - CS Cyber docs –

ESTCP provides focused, step-by-step guidance and tools specific to the FRCS RMF Self-Assess. These tools are intended to facilitate and accelerate eMASS package assembly

Appendix C: R-SAT User Guide

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

User Guide

Prepared for:
Federal FRCS System Owners and other Stakeholders

December 10, 2019

Table of Contents

Revision History

Revision	Date	Name	Description
1.0	12/2019	IPERC	Initial Draft

Introduction

Purpose

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

R-SAT objectives include:

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

Scope

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

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

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

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

R-SAT Overview

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

Structure

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

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

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

Supplemental documents external to R-SAT include:

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

Form Layout

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

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

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

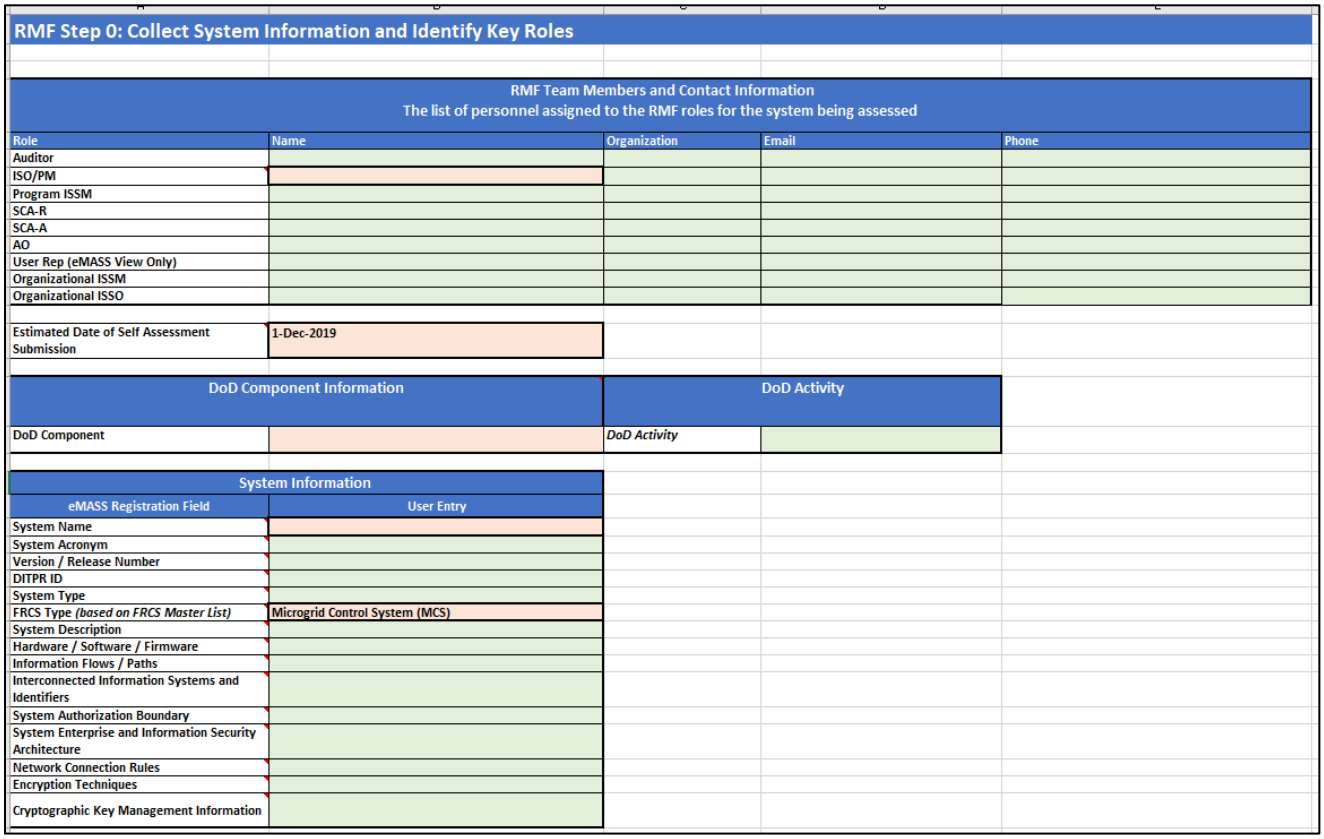
Informational Popups and Alerts

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

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

System Information Form

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



RMF Step 0: Collect System Information and Identify Key Roles

RMF Team Members and Contact Information
The list of personnel assigned to the RMF roles for the system being assessed

Role	Name	Organization	Email	Phone
Auditor				
ISO/PM				
Program ISSM				
SCA-R				
SCA-A				
AO				
User Rep (eMASS View Only)				
Organizational ISSM				
Organizational ISSO				

Estimated Date of Self Assessment Submission	1-Dec-2019

DoD Component Information		DoD Activity	
DoD Component		*DoD Activity*	

System Information

eMASS Registration Field	User Entry
System Name	
System Acronym	
Version / Release Number	
DITPR ID	
System Type	
FRCS Type *(based on FRCS Master List)*	Microgrid Control System (MCS)
System Description	
Hardware / Software / Firmware	
Information Flows / Paths	
Interconnected Information Systems and Identifiers	
System Authorization Boundary	
System Enterprise and Information Security Architecture	
Network Connection Rules	
Encryption Techniques	
Cryptographic Key Management Information	

Optional Entries (green cells)

RMF role requirements are defined in DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT) (Reference (c)). System Information fields are defined on the eMASS Step-by Step Instructions Document[2] on the SERDP-ESTCP Portal.

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

Required Entries (orange cells)

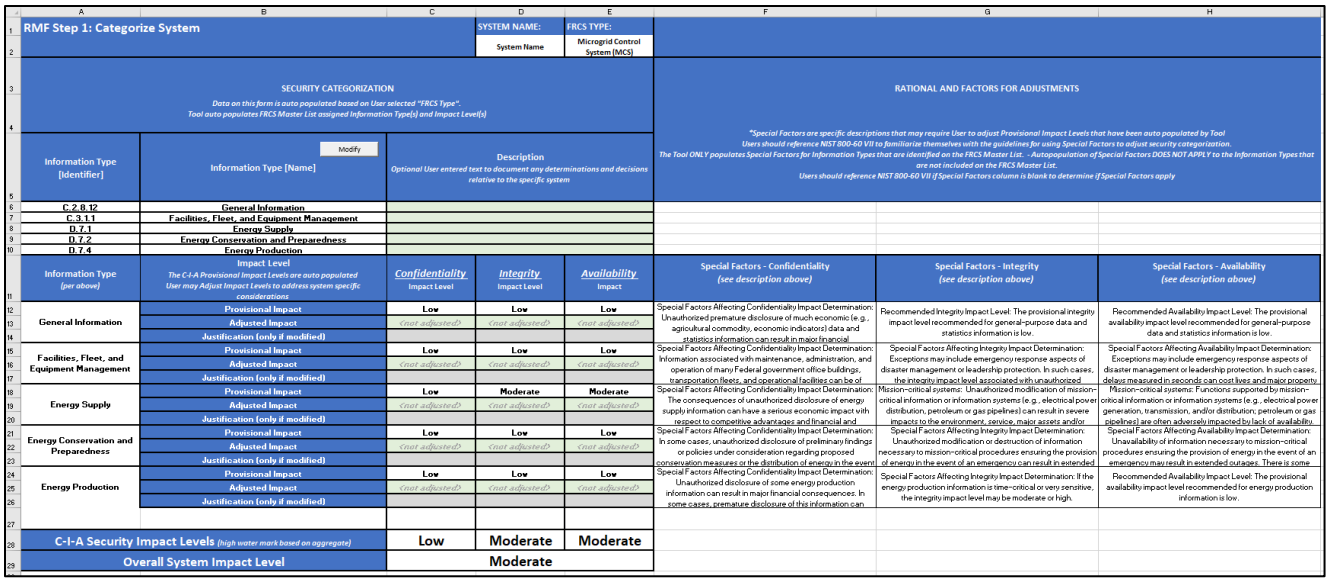
- **ISO/PM**: Enter the name of the Information System Owner/Project Manager performing the self-assessment. This data will auto-fill the eMASS Test Result Export form (column J) as "Tested By" for auto-filled Control Correlation Identifiers (CCIs).
- **Estimated Date of Self-Assessment Submission**: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

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

[3] https://rmf.ks.osd.mil/rmf/general/IT/PlatformIT/EIEControlSystems/Pages/default.aspx

Security Categorization Form

System Categorization is RMF Step 1. This form will auto-fill Information Types[4] identified in the FRCS Master List as being applicable to the FRCS Type selected in the System Info Form drop-down. The Provisional Impact Levels for each Information Type are also populated. R-SAT will calculate the aggregate and overall Security Impact Levels (Low, Moderate or High) for Confidentiality, Integrity and Availability (CIA). The Overall System Impact Level is the "high water mark" of the Security Impact Levels and will be used to build the security baseline on subsequent R-SAT forms. This form does not import data into the eMASS system. The Security Categorization is required to complete the system registration in eMASS.



RMF Step 1: Categorize System

SYSTEM NAME: System Name | FRCS TYPE: Microgrid Control System (MCS)

SECURITY CATEGORIZATION

Data on this form is auto populated based on User selected "FRCS Type".
Tool auto populates FRCS Master List assigned Information Type(s) and Impact Level(s)

RATIONAL AND FACTORS FOR ADJUSTMENTS

**Special Factors are specific descriptions that may require User to adjust Provisional Impact Levels that have been auto populated by Tool*
Users should reference NIST 800-60 VII to familiarize themselves with the guidelines for using Special Factors to adjust security categorization.
The Tool ONLY populates Special Factors for Information Types that are identified on the FRCS Master List. - Autopopulation of Special Factors DOES NOT APPLY to the Information Types that are not included on the FRCS Master List.
Users should reference NIST 800-60 VII if Special Factors column is blank to determine if Special Factors apply

Information Type [Identifier]	Information Type [Name] (Modify)	Description *Optional User entered text to document any determinations and decisions relative to the specific system*
C.2.8.12	General Information	
C.3.1.1	Facilities, Fleet, and Equipment Management	
D.7.1	Energy Supply	
D.7.2	Energy Conservation and Preparedness	
D.7.4	Energy Production	

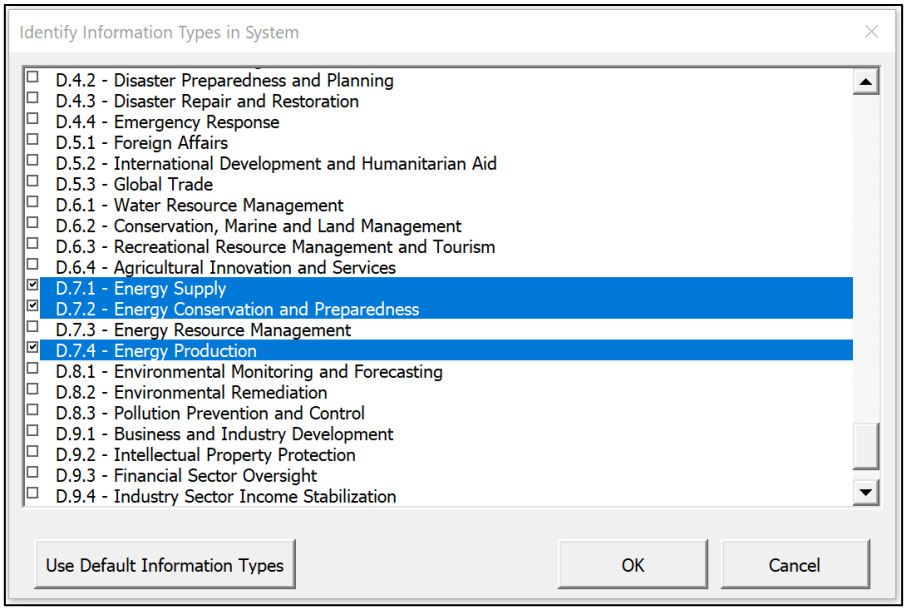
Information Type *(per above)*	Impact Level *The C-I-A Provisional Impact Levels are auto populated User may Adjust Impact Levels to address system specific considerations*	*Confidentiality* Impact Level	*Integrity* Impact Level	*Availability* Impact	Special Factors - Confidentiality *(see description above)*	Special Factors - Integrity *(see description above)*	Special Factors - Availability *(see description above)*
General Information	Provisional Impact	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Unauthorized premature disclosure of much economic (e.g., agricultural commodity, economic indicators) data and statistics information can result in major financial	Recommended Integrity Impact Level: The provisional integrity impact level recommended for general-purpose data and statistics information is low.	Recommended Availability Impact Level: The provisional availability impact level recommended for general-purpose data and statistics information is low.
	Adjusted Impact	<not adjusted>	<not adjusted>	<not adjusted>			
	Justification (only if modified)						
Facilities, Fleet, and Equipment Management	Provisional Impact	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Information associated with maintenance, administration, and operation of many Federal government office buildings; transportation fleets; and operational facilities can be of	Special Factors Affecting Integrity Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, the integrity impact level associated with unauthorized	Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, delays measured in seconds can cost lives and major property
	Adjusted Impact	<not adjusted>	<not adjusted>	<not adjusted>			
	Justification (only if modified)						
Energy Supply	Provisional Impact	Low	Moderate	Moderate	Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of energy supply information can have a serious economic impact with respect to competitive advantages and financial and	Mission-critical systems: Unauthorized modification of mission-critical information or information systems (e.g., electrical power distribution, petroleum or gas pipelines) can result in severe impacts to the environment, service, major assets and/or	Mission-critical systems: Functions supported by mission-critical information or information systems (e.g., electrical power generation, transmission, and/or distribution; petroleum or gas pipelines) are often adversely impacted by lack of availability.
	Adjusted Impact	<not adjusted>	<not adjusted>	<not adjusted>			
	Justification (only if modified)						
Energy Conservation and Preparedness	Provisional Impact	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed conservation measures or the distribution of energy in the event	Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency may result in extended	Special Factors Affecting Availability Impact Determination: Unavailability of information necessary to mission-critical procedures ensuring the provision of energy in the event of an emergency may result in extended outages. There is some
	Adjusted Impact	<not adjusted>	<not adjusted>	<not adjusted>			
	Justification (only if modified)						
Energy Production	Provisional Impact	Low	Low	Low	Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some energy production information can result in major financial consequences. In some cases, premature disclosure of this information can	Special Factors Affecting Integrity Impact Determination: If the energy production information is time-critical or very sensitive, the integrity impact level may be moderate or high.	Recommended Availability Impact Level: The provisional availability impact level recommended for energy production information is low.
	Adjusted Impact	<not adjusted>	<not adjusted>	<not adjusted>			
	Justification (only if modified)						
C-I-A Security Impact Levels *(high water mark based on aggregate)*		Low	Moderate	Moderate			
Overall System Impact Level		Moderate					

Buttons

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

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

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



Optional Entries (green cells)

- **Information Type Description:** Users are encouraged to enter a description of how the Information Type is present on the FRCS. Modifying the Information Types is described below.
- **Adjusted Impact:** Users must review the auto-filled information Types, the FRCS Master List Special Factors[6] provided (if it exists) for each Information Type and other known considerations to adjust Provisional Impact levels as appropriate. When adjustments are made, the User Adjusted Impact level will override the Provisional Impact level in the Overall System Impact Level determination.

Required Entries (orange cells)

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

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

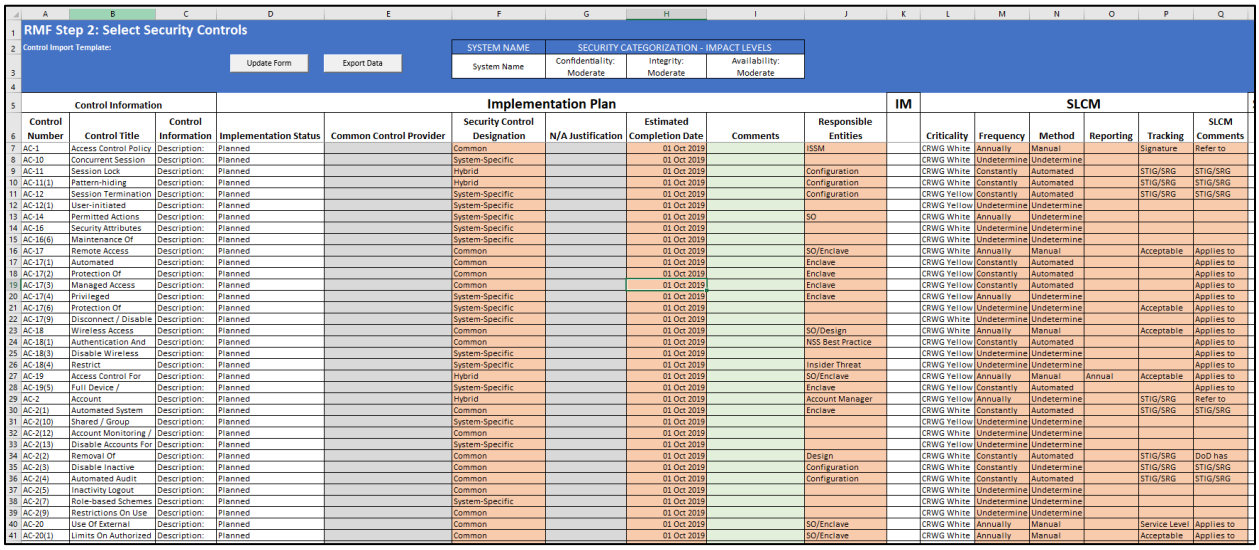
Note: National Security Information and National Security Systems, such as Defense and National Security Information Types (D.1) and Intelligence Operations Information Types (D.3), are outside of the scope of NIST 800-60 Vol II and are not fully supported by R-SAT.

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

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

Control Information Form

Select Security Controls is RMF Step 2. The Control Information Form is where the baseline control set is generated based on the current Security Categorization and Committee on National Security Systems Instruction (CNSSI) No 1253, Appendix D-1 (Reference (a)). The CNSS baseline includes the NIST 800-53 (Reference (h)) baseline. The System Name and the Security Categorization Impact Levels of the FRCS being assessed are indicated at the top. The Control Information Form uses the same general format as the eMASS template of the same name.



RMF Step 2: Select Security Controls

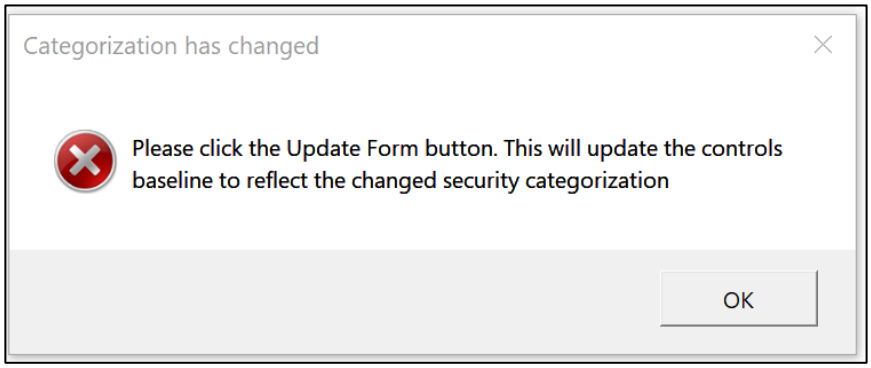
Control Import Template: | Update Form | Export Data

SYSTEM NAME	SECURITY CATEGORIZATION - IMPACT LEVELS		
System Name	Confidentiality: Moderate	Integrity: Moderate	Availability: Moderate

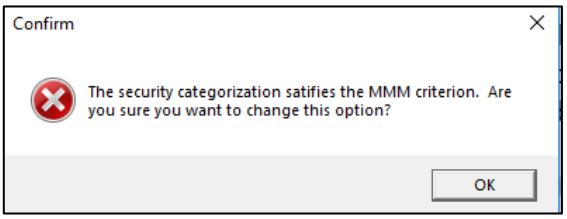
Control Information			Implementation Plan							IM	SLCM					
Control Number	Control Title	Control Information	Implementation Status	Common Control Provider	Security Control Designation	N/A Justification	Estimated Completion Date	Comments	Responsible Entities		Criticality	Frequency	Method	Reporting	Tracking	SLCM Comments
AC-1	Access Control Policy	Description:	Planned		Common		01 Oct 2019		ISSM		CRWG White	Annually	Manual		Signature	Refer to
AC-10	Concurrent Session	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-11	Session Lock	Description:	Planned		Hybrid		01 Oct 2019		Configuration		CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
AC-11(1)	Pattern-hiding	Description:	Planned		Hybrid		01 Oct 2019		Configuration		CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
AC-12	Session Termination	Description:	Planned		System-Specific		01 Oct 2019		Configuration		CRWG Yellow	Constantly	Automated		STIG/SRG	STIG/SRG
AC-12(1)	User-initiated	Description:	Planned		System-Specific		01 Oct 2019				CRWG Yellow	Undetermine	Undetermine			
AC-14	Permitted Actions	Description:	Planned		System-Specific		01 Oct 2019		SO		CRWG White	Annually	Undetermine			
AC-16	Security Attributes	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-16(6)	Maintenance Of	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-17	Remote Access	Description:	Planned		Common		01 Oct 2019		SO/Enclave		CRWG White	Annually	Manual		Acceptable	Applies to
AC-17(1)	Automated	Description:	Planned		Common		01 Oct 2019		Enclave		CRWG Yellow	Constantly	Automated			Applies to
AC-17(2)	Protection Of	Description:	Planned		Common		01 Oct 2019		Enclave		CRWG Yellow	Constantly	Automated			Applies to
AC-17(3)	Managed Access	Description:	Planned		Common		01 Oct 2019		Enclave		CRWG Yellow	Constantly	Automated			Applies to
AC-17(4)	Privileged	Description:	Planned		System-Specific		01 Oct 2019		Enclave		CRWG Yellow	Annually	Undetermine			Applies to
AC-17(6)	Protection Of	Description:	Planned		System-Specific		01 Oct 2019				CRWG Yellow	Undetermine	Undetermine		Acceptable	Applies to
AC-17(9)	Disconnect / Disable	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			Applies to
AC-18	Wireless Access	Description:	Planned		Common		01 Oct 2019		SO/Design		CRWG White	Annually	Manual		Acceptable	Applies to
AC-18(1)	Authentication And	Description:	Planned		Common		01 Oct 2019		NSS Best Practice		CRWG Yellow	Constantly	Automated			Applies to
AC-18(3)	Disable Wireless	Description:	Planned		System-Specific		01 Oct 2019				CRWG Yellow	Undetermine	Undetermine			Applies to
AC-18(4)	Restrict	Description:	Planned		System-Specific		01 Oct 2019		Insider Threat		CRWG Yellow	Undetermine	Undetermine			Applies to
AC-19	Access Control For	Description:	Planned		Hybrid		01 Oct 2019		SO/Enclave		CRWG Yellow	Annually	Manual	Annual	Acceptable	Applies to
AC-19(5)	Full Device /	Description:	Planned		System-Specific		01 Oct 2019		Enclave		CRWG Yellow	Constantly	Automated			Applies to
AC-2	Account	Description:	Planned		Hybrid		01 Oct 2019		Account Manager		CRWG Yellow	Annually	Undetermine		STIG/SRG	Refer to
AC-2(1)	Automated System	Description:	Planned		Common		01 Oct 2019		Enclave		CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
AC-2(10)	Shared / Group	Description:	Planned		System-Specific		01 Oct 2019				CRWG Yellow	Undetermine	Undetermine			
AC-2(12)	Account Monitoring /	Description:	Planned		Common		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-2(13)	Disable Accounts For	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-2(2)	Removal Of	Description:	Planned		Common		01 Oct 2019		Design		CRWG White	Constantly	Automated		STIG/SRG	DoD has
AC-2(3)	Disable Inactive	Description:	Planned		Common		01 Oct 2019		Configuration		CRWG White	Constantly	Undetermine		STIG/SRG	STIG/SRG
AC-2(4)	Automated Audit	Description:	Planned		Common		01 Oct 2019		Configuration		CRWG White	Constantly	Automated		STIG/SRG	STIG/SRG
AC-2(5)	Inactivity Logout	Description:	Planned		Common		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-2(7)	Role-based Schemes	Description:	Planned		System-Specific		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-2(9)	Restrictions On Use	Description:	Planned		Common		01 Oct 2019				CRWG White	Undetermine	Undetermine			
AC-20	Use Of External	Description:	Planned		Common		01 Oct 2019		SO/Enclave		CRWG White	Annually	Manual		Service Level	Applies to
AC-20(1)	Limits On Authorized	Description:	Planned		Common		01 Oct 2019		SO/Enclave		CRWG White	Annually	Manual		Acceptable	Applies to

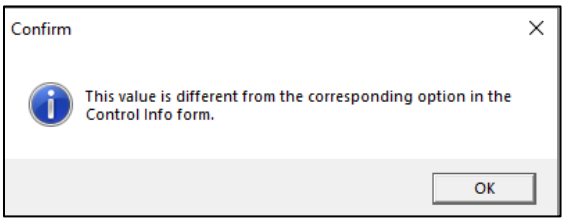
Popup Alerts

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



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





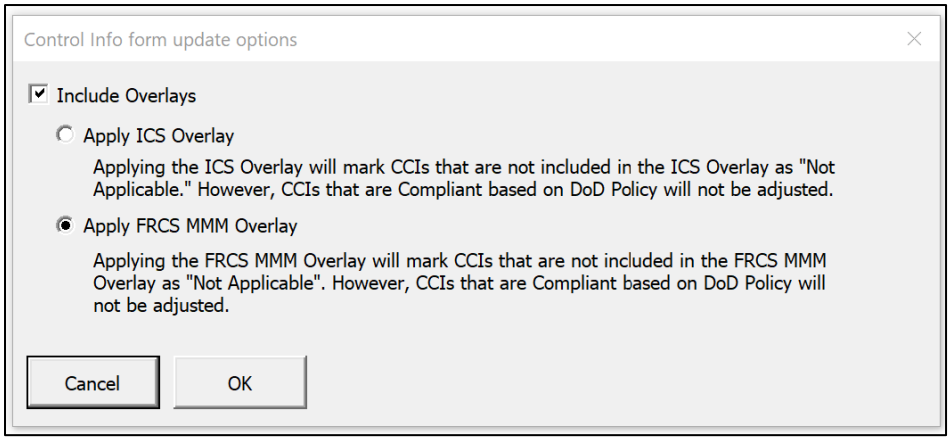
A popup will alert the User if 1) The Security Categorization is M-M-M, but the ICS Overlay was chosen, or 2) The selected overlay on one form does not match the selected overlay on the other form. For best results, the same overlay should be selected on the Control Information and Test Results forms.

Buttons

Update Form

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

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



Export Data

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

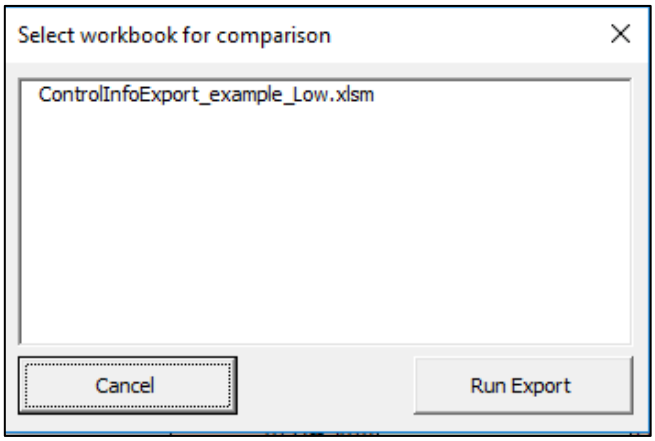
Note: Generic templates or templates from eMASS records other than the FRCS undergoing the Self-Assessment may not successfully import to eMASS. See eMASS Import Errors Section.

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

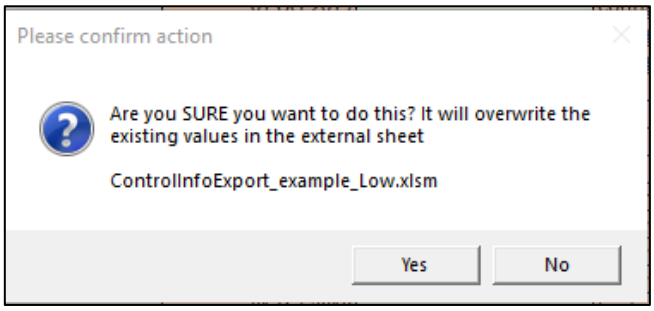
Export steps are:

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

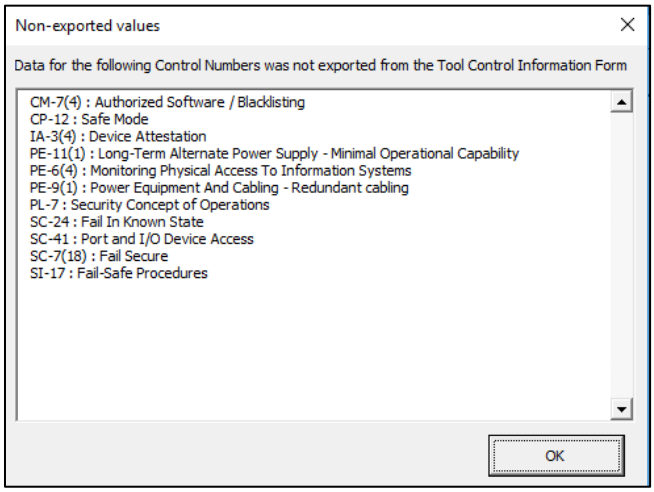
1. Export the Control Information Form from eMASS.
2. Open the eMASS template file and Enable Content.
3. Select <Export Data> from the top menu on the R-SAT Form. This will open a list of open Excel files in the "Select workbook for comparison" window (see below).



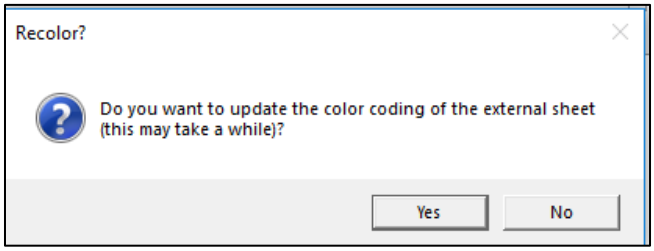
4. Select the appropriate Excel Worksheet (eMASS template file). If you do not see the desired worksheet, Cancel the export and ensure the exported eMASS template is open.
5. Select <Run Export> to populate the eMASS template with the R-SAT form data. A popup will appear to verify the execution of the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



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



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



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

Auto-filled Fields

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

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

Table 1 Implementation Status - Auto-fill Data

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

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

Auto-filled field descriptions:

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

Optional Entries (green cells)

These non-required cells may be populated as appropriate.

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

Required Entries (orange cells)

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

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

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

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

eMASS Import Errors

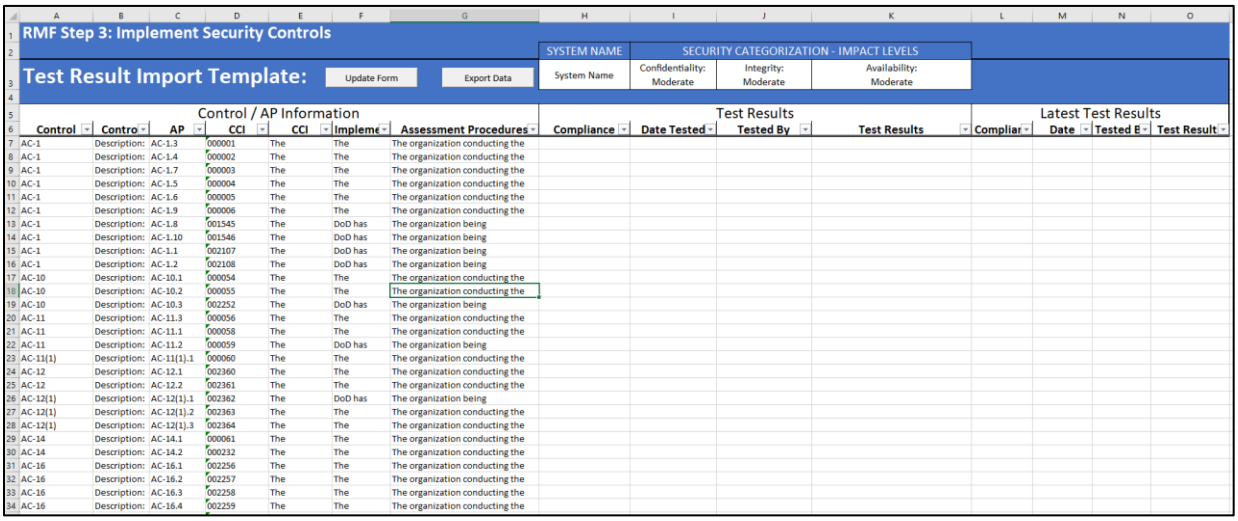
The Import of actual templates, exported from eMASS and populated by R-SAT, have been tested. If there are errors in the import process of your R-SAT populated (and manually tailored) template, consider the following:

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

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

Test Results Form

Implement Security Controls is RMF Step 3. At this step, evidence and implementation descriptions for CCIs (the decomposition of security control requirements into singular, actionable statements) are documented. The System Name and the Security Categorization of the FRCS being assessed is indicated on the top of the form. The Test Results Form uses the same format as the eMASS template of the same name.



RMF Step 3: Implement Security Controls

Test Result Import Template: [Update Form] [Export Data]

SYSTEM NAME	SECURITY CATEGORIZATION - IMPACT LEVELS		
System Name	Confidentiality: Moderate	Integrity: Moderate	Availability: Moderate

Control / AP Information							Test Results				Latest Test Results			
Control	Contro	AP	CCI	CCI	Impleme	Assessment Procedures	Compliance	Date Tested	Tested By	Test Results	Compliar	Date	Tested B	Test Result
AC-1	Description:	AC-1.3	000001	The	The	The organization conducting the								
AC-1	Description:	AC-1.4	000002	The	The	The organization conducting the								
AC-1	Description:	AC-1.7	000003	The	The	The organization conducting the								
AC-1	Description:	AC-1.5	000004	The	The	The organization conducting the								
AC-1	Description:	AC-1.6	000005	The	The	The organization conducting the								
AC-1	Description:	AC-1.9	000006	The	The	The organization conducting the								
AC-1	Description:	AC-1.8	001545	The	DoD has	The organization being								
AC-1	Description:	AC-1.10	001546	The	DoD has	The organization being								
AC-1	Description:	AC-1.1	002107	The	DoD has	The organization being								
AC-1	Description:	AC-1.2	002108	The	DoD has	The organization being								
AC-10	Description:	AC-10.1	000054	The	The	The organization conducting the								
AC-10	Description:	AC-10.2	000055	The	The	The organization conducting the								
AC-10	Description:	AC-10.3	002252	The	DoD has	The organization being								
AC-11	Description:	AC-11.3	000056	The	The	The organization conducting the								
AC-11	Description:	AC-11.1	000058	The	The	The organization conducting the								
AC-11	Description:	AC-11.2	000059	The	DoD has	The organization being								
AC-11(1)	Description:	AC-11(1).1	000060	The	The	The organization conducting the								
AC-12	Description:	AC-12.1	002360	The	The	The organization conducting the								
AC-12	Description:	AC-12.2	002361	The	The	The organization conducting the								
AC-12(1)	Description:	AC-12(1).1	002362	The	DoD has	The organization being								
AC-12(1)	Description:	AC-12(1).2	002363	The	The	The organization conducting the								
AC-12(1)	Description:	AC-12(1).3	002364	The	The	The organization conducting the								
AC-14	Description:	AC-14.1	000061	The	The	The organization conducting the								
AC-14	Description:	AC-14.2	000232	The	The	The organization conducting the								
AC-16	Description:	AC-16.1	002256	The	The	The organization conducting the								
AC-16	Description:	AC-16.2	002257	The	The	The organization conducting the								
AC-16	Description:	AC-16.3	002258	The	The	The organization conducting the								
AC-16	Description:	AC-16.4	002259	The	The	The organization conducting the								

Popup Alerts

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

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

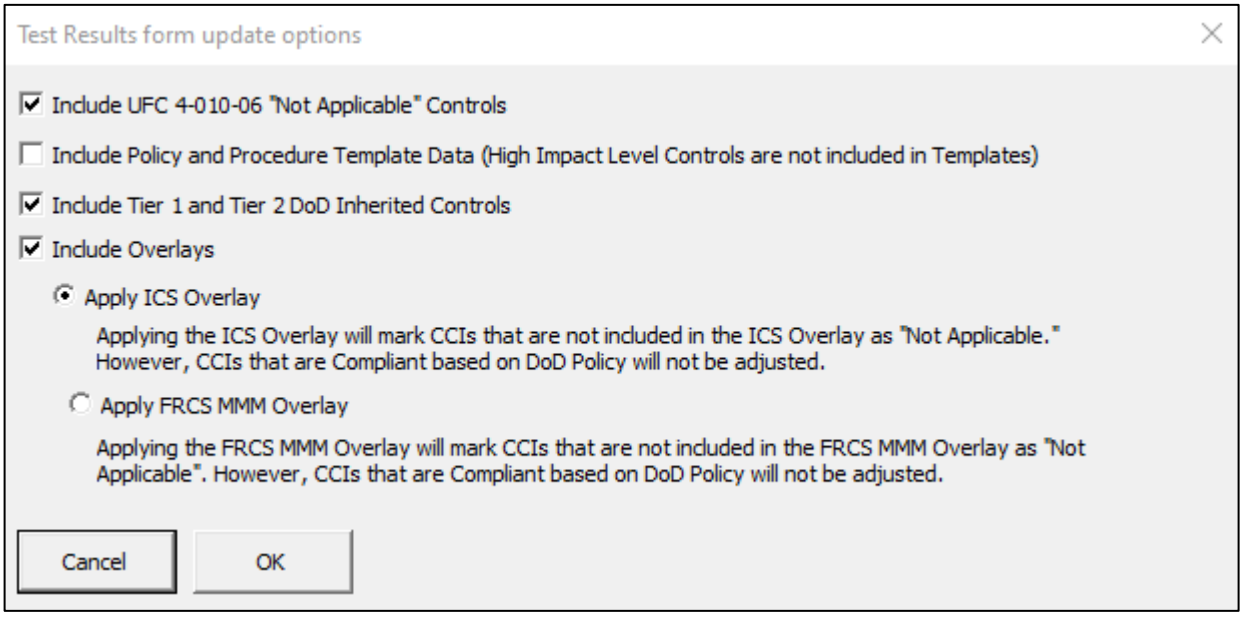
See Popup Alerts in the Control Information Form section for graphical examples.

Buttons

Update Form

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

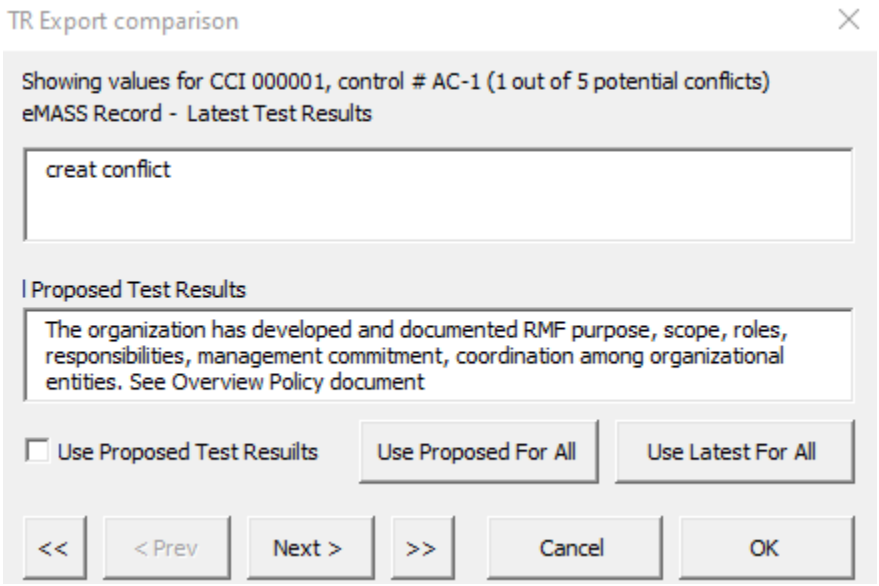
- **Include UFC 4-010-06:** Check this box to auto-fill CCIs as “Not Applicable” in accordance with Table H-2 of the UFC.
- **Include Policy and Procedure Template Data:** select the checkbox if you intend to use the security policy and procedure templates provided with R-SAT. See ***Security Policies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



Export Data

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

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



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

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

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

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

Auto-filled Fields

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

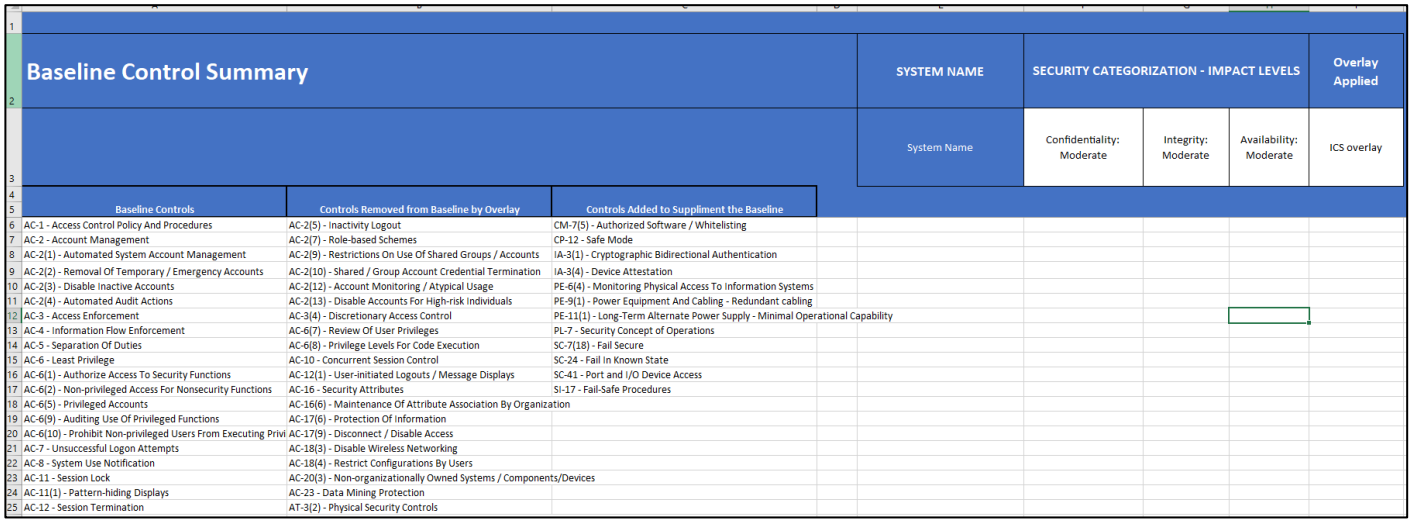
Note: These are suggested entries that must be reviewed for additional tailoring.

Table 2 Test Results - Auto-fill Data

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

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

Baseline Control Summary



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

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

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

Security Policies & Procedure Templates

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

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

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

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

Implementation Instructions: System Specific Requirements List

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

Implementation Instructions: ISSM Checklist

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

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

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

Appendix 1: References

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

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

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

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

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

e. RMF FRCS Master List, Final: June 23, 2018 posted on SERDP-ESTCP Portal, https://www.serdp-estcp.org

f. Federal Information Processing Standard Publication (FIPS Pub) 199, "Standards for Security Categorization of Federal Information Systems," eb 2004.

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

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

i. NIST Special Publication (SP) 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," Dec 18, 2014

j. NIST Special Publication (SP) 800-60 Volume 1 Revision 1, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," Aug 2008.

k. NIST (SP) 800-60 Volume 2 Revision 1, "Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories," Aug 2008.

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

m. DoD RMF Knowledge Service portal, https://rmf.ks.osd.mil

n. SERDP-ESTCP Portal, https://www.serdp-estcp.org

o. UFC 4-010-06, Unified Facilities Criteria, "Cybersecurity of Facility-Related Control Systems," January 18, 2017 as amended.

Appendix 2: Acronyms

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

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

Appendix D: Demonstration Documentation and Data

Preliminary Observations

- Overall
  - Alerts for audit failures unable to be configured
  - Multifactor/PKI authentication not configured
  - Group accounts used
  - Virus scans and updates accomplished quarterly
  - No HBSS
  - Meck Island team well prepared for the assessment
- Nessus
  - No critical vulnerabilities
  - Switches few high vulnerabilities relating to compatibility with SSHv1
  - HMIs/WPC/IPC few medium vulnerabilities
  - Ubuntu clean

***** UNCLASSIFIED//FOR OFFICIAL USE ONLY *****

Control Import Template: IPERC

Exported on 23-May-2019 by AURA KEATING

(System Type: Platform IT System, DoD Component: OSD)

Control Information			Implementation Plan							IM	SLCM						SLC	Risk Assessment								RA
Control Numbe	Control Title	Control Inform	Implementatio	Common	Security	N/A Justific	Estimated Completio	Comments	Responsible		Criticality	Frequency	Method	Reporting	Tracking	SLCM Comme		Severity	Relevance of	Likelihood	Impact	Residual Risk	Vulnerability	Impact Descrip	Recommendat	
AC-1	Access Control	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM										
AC-2	Account Managem	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM										
AC-2(1)	Automate	Descriptio n:																								
AC-2(2)	Removal Of	Descriptio n:																								
AC-2(3)	Disable Inactive	Descriptio n:																								
AC-2(4)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-2(5)	Inactivity Logout	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-2(7)	Role-based	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-2(9)	Restrictio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-2(10)	Shared / Group	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-2(12)	Account Monitorin	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-2(13)	Disable Accounts	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-3	Access Enforcem	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Authorized Use										
AC-3(4)	Discretion	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-4	Informati	Descriptio n:																								
AC-5	Separatio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6	Least Privilege	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(1)	Authorize	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(2)	Non-privileged	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(5)	Privileged	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(7)	Review Of User	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(8)	Privilege Levels For	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-6(9)	Auditing Use Of	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-6(10)	Prohibit Non-	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-7	Unsuccess	Descriptio n:	Planned		Hybrid		10/20/2019					Quarterly	Manual	Non-compliant	POA&M will be	STIG/SRG; Report										
AC-8	System Use	Descriptio n:	Planned		Hybrid		10/20/2019					Constantly	Manual	Non-compliant	POA&M will be	STIG/SRG; Report										
AC-10	Concurre	Descriptio n:																								
AC-11	Session Lock	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-11(1)	Pattern-hiding	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-12	Session Terminati	Descriptio n:																								
AC-12(1)	User-initiated	Descriptio n:																								
AC-14	Permitted	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Report non-										
AC-16	Security Attributes	Descriptio n:																								
AC-16(6)	Maintena	Descriptio n:																								
AC-17	Remote Access	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applies to Remote										
AC-17(1)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-17(2)	Protectio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-17(3)	Managed	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-17(4)	Privileged	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-17(6)	Protectio	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-17(9)	Disconnec	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
AC-18	Wireless Access	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to Wireless										
AC-18(1)	Authentic	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-18(3)	Disable Wireless	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-18(4)	Restrict Configura	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																				
AC-19	Access Control	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to Mobile										
AC-19(5)	Full Device /	Descriptio n:																								
AC-20	Use Of External	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to External										
AC-20(1)	Limits On	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-20(2)	Portable Storage	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-20(3)	Non-organizati	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
AC-21	Informati	Descriptio n:	Planned		Common		10/20/2019					Annually	Undetermined	Non-compliant	POA&M will be	Applies to Informati										
AC-22	Publicly Accessible	Descriptio n:	Not Applicabl		Common	Not Applicabl		Not Applicabl								Applies to Publicly										
AC-23	Data Mining	Descriptio n:																								
AT-1	Security Awarenes	Descriptio n:	Inherited	DoD	Common		12/1/2016	Inherited by DoD	DoD CIO																	
AT-2	Security Awarenes	Descriptio n:	Inherited	DoD	Common		12/1/2016	Inherited by DoD	DoD CIO																	
AT-2(2)	Insider Threat	Descriptio n:	Inherited	DoD	Common		12/1/2016	Inherited by DoD	DoD CIO																	
AT-3	Role-based	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Training Records										
AT-3(2)	Physical Security	Descriptio n:	Not Applicabl		Common	Controls N/A for																				

AT-3(4)	Suspicious	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AT-4	Security Training	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-1	Audit And	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-2	Audit Events	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-2(3)	Reviews And	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AU-3	Content Of Audit	Descriptio n:	Planned		Hybrid		10/20/2019					Undetermined	Manual	Non-compliant	POA&M will be	Audit download														
AU-3(1)	Additional	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-4	Audit Storage	Descriptio n:	Planned		Hybrid		10/20/2019					Weekly	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-4(1)	Transfer To	Descriptio n:	Planned		Hybrid		10/20/2019					Weekly	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-5	Response	Descriptio n:	Planned		Hybrid		10/20/2019					Undetermined	Manual	Non-compliant	POA&M will be	Related to System														
AU-5(1)	Audit Storage	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-6	Audit Review,	Descriptio n:	Planned		Common		10/20/2019					Weekly	Undetermined	Non-compliant	POA&M will be	Refer to ISSM														
AU-6(1)	Process Integratio	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AU-6(3)	Correlate Audit	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AU-6(4)	Central Review	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
AU-6(10)	Audit Level	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AU-7	Audit Reduction	Descriptio n:																												
AU-7(1)	Automatic	Descriptio n:																												
AU-8	Time Stamps	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report														
AU-8(1)	Synchroni	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-9	Protectio	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report														
AU-9(4)	Access by Subset	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
AU-10	Non-repudiatio	Descriptio n:																												
AU-11	Audit Record	Descriptio n:	Planned		Common		10/20/2019					Annually	Undetermined	Non-compliant	POA&M will be	Refer to ISSM														
AU-11(1)	Long-Term	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-12	Audit Generatio	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
AU-12(1)	System-Wide /	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-12(3)	Changes by	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
AU-14	Session Audit	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
AU-14(1)	System Start-Up	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
AU-14(2)	Capture/R	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
AU-14(3)	Remote Viewing /	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
CA-1	Security Assessme	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CA-2	Security Assessme	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CA-2(1)	Independ	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CA-3	System Interconn	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CA-3(1)	Unclassifi	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CA-3(5)	Restrictio	Descriptio n:	Not Applicabl		Common	Controls N/A for																								
CA-5	Plan Of Action	Descriptio n:	Planned		Hybrid		10/20/2019					Quarterly	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CA-6	Security Authoriza	Descriptio n:	Inherited	Component	Hybrid		8/21/2017	Inherited DoD Tier	DoD Compone																					
CA-7	Continuou	Descriptio n:	Inherited	DoD	Hybrid		4/15/2019	Inherited by DoD	DoD CIO																					
CA-7(1)	Independ	Descriptio n:																												
CA-9	Internal System	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Internal System														
CM-1	Configura	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-2	Baseline Configura	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-2(1)	Reviews And	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CM-2(3)	Retention	Descriptio n:																												
CM-2(7)	Configure	Descriptio n:																												
CM-3	Configura	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CM-3(2)	Test / Validate /	Descriptio n:																												
CM-3(4)	Security Represent	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
CM-3(6)	Cryptogra	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CM-4	Security Impact	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-4(1)	Separate Test	Descriptio n:																												
CM-5	Access Restrictio	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
CM-5(1)	Automate	Descriptio n:																												
CM-5(2)	Review System	Descriptio n:																												
CM-5(5)	Limit Productio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CM-5(6)	Limit Library	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																								
CM-6	Configura	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-6(1)	Automate	Descriptio n:																												
CM-7	Least Functiona	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-7(1)	Periodic Review	Descriptio n:	Planned		Hybrid		10/20/2019					Monthly	Manual	Non-compliant	POA&M will be	Refer to ISSM														
CM-7(2)	Prevent Program	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								
CM-7(3)	Registrati	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																								

CM-7(5)	Authorize	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																					
CM-8	Informati	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CM-8(1)	Updates During	Descriptio n:																									
CM-8(2)	Automate	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
CM-8(3)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																					
CM-8(5)	No Duplicate	Descriptio n:																									
CM-9	Configura	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
CM-10	Software Usage	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Software Usage											
CM-10(1)	Open Source	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD has defined	DoD CIO																		
CM-11	User-Installed	Descriptio n:	Planned		Hybrid		10/20/2019					Monthly	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CM-11(2)	Prohibit Installatio	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
CP-1	Contingen	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD has defined	DoD CIO																		
CP-2	Contingen	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CP-2(1)	Coordinat	Descriptio n:																									
CP-2(3)	Resume Essential	Descriptio n:																									
CP-2(8)	Identify Critical	Descriptio n:																									
CP-3	Contingen	Descriptio n:	Planned		Hybrid		10/20/2019					Undetermined	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CP-4	Contingen	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CP-4(1)	Coordinat	Descriptio n:																									
CP-6	Alternate	Descriptio n:																									
CP-6(1)	Separatio n From	Descriptio n:																									
CP-6(3)	Accessibili ty	Descriptio n:																									
CP-7	Alternate	Descriptio n:																									
CP-7(1)	Separatio	Descriptio n:																									
CP-7(2)	Accessibili	Descriptio n:																									
CP-7(3)	Priority Of Service	Descriptio n:																									
CP-8	Telecomm	Descriptio n:																									
CP-8(1)	Priority Of Service	Descriptio n:																									
CP-8(2)	Single Points Of	Descriptio n:																									
CP-9	Informati	Descriptio n:	Planned		Hybrid		10/20/2019					Weekly	Manual	Non-compliant	POA&M will be	Refer to ISSM											
CP-9(1)	Testing For	Descriptio n:																									
CP-9(5)	Transfer To	Descriptio n:																									
CP-10	Informati	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	System Recovery											
CP-10(2)	Transacti	Descriptio n:																									
IA-1	Identificat	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD has defined	DoD CIO																		
IA-2	Identificat	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-2(1)	Network Access to	Descriptio n:	Planned		System-Specific		10/20/2019					Constantly	Automated	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-2(2)	Network Access to	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
IA-2(3)	Local Access to	Descriptio n:																									
IA-2(4)	Local Access to	Descriptio n:																									
IA-2(5)	Group Authentic	Descriptio n:	Not Applicabl		Common	Controls N/A for																					
IA-2(8)	Network Access to	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
IA-2(9)	Network Access to	Descriptio n:																									
IA-2(11)	Remote Access -	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																					
IA-2(12)	Acceptanc	Descriptio n:	Planned		System-Specific		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-3	Device Identificat	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Network Diagram;											
IA-3(1)	Cryptogra	Descriptio n:																									
IA-4	Identifier Managem	Descriptio n:	Planned		Common		10/20/2019					Monthly	Undetermined	Non-compliant	POA&M will be	Refer to ISSM											
IA-4(4)	Identify User	Descriptio n:	Not Applicabl		Common	Controls N/A for																					
IA-5	Authentic	Descriptio n:	Planned		Hybrid		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Refer to ISSM											
IA-5(1)	Password-	Descriptio n:	Planned		Hybrid		10/20/2019					Monthly	Manual	Non-compliant	POA&M will be	Refer to ISSM											
IA-5(2)	PKI-Based	Descriptio n:																									
IA-5(3)	In-Person Or	Descriptio n:																									
IA-5(4)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																					
IA-5(7)	No Embedde	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																					
IA-5(8)	Multiple Informati	Descriptio n:	Not Applicabl		Common	Controls N/A for																					
IA-5(11)	Hardware	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-5(13)	Expiration	Descriptio n:	Inherited	Component	Hybrid		10/1/2018	Inherited DoD Tier	DoD Compone																		
IA-5(14)	Managing	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD trust store	DoD CIO																		
IA-6	Authentic	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-7	Cryptogra	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	STIG/SRG; Report											
IA-8	Identificat	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applies to PKI PIV											
IA-8(1)	Acceptanc	Descriptio n:	Planned		System-Specific		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to PKI PIV											
IA-8(2)	Acceptanc	Descriptio n:	Planned		System-Specific		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to PKI PIV											
IA-8(3)	Use Of FICAM-	Descriptio n:	Planned		System-Specific		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to PKI PIV											

IA-8(4)	Use Of FICAM-	Descriptio n:	Planned		System-Specific		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Applies to PKI PIV															
IR-1	Incident Response	Descriptio n:	Inherited	DoD	Common		12/1/2016	Automatically	DoD CIO																						
IR-2	Incident Response	Descriptio n:	Planned		Common		10/20/2019					Quarterly	Manual	Non-compliant	POA&M will be	Refer to ISSM															
IR-3	Incident Response	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-3(2)	Coordinat	Descriptio n:																													
IR-4	Incident Handling	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Incident/Event/Failu															
IR-4(1)	Automate	Descriptio n:																													
IR-4(3)	Continuity	Descriptio n:																													
IR-4(4)	Informati	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-4(6)	Insider Threats -	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
IR-4(7)	Insider Threats -	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-4(8)	Correlatio	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-5	Incident Monitorin	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Manual	Non-compliant	POA&M will be	Incident/Event/Failu															
IR-6	Incident Reporting	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Manual	Non-compliant	POA&M will be	Refer to ISSM															
IR-6(1)	Automate	Descriptio n:																													
IR-6(2)	Vulnerabil	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
IR-7	Incident Response	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Incident Response															
IR-7(1)	Automati	Descriptio n:																													
IR-7(2)	Coordinat	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
IR-8	Incident Response	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
IR-9	Informati	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-9(1)	Responsib	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-9(2)	Training	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-9(3)	Post-spill Operation	Descriptio n:																													
IR-9(4)	Exposure To	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
IR-10	Integrate	Descriptio n:																													
MA-1	System Maintena	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
MA-2	Controlle	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
MA-3	Maintena	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
MA-3(1)	Inspect Tools	Descriptio n:																													
MA-3(2)	Inspect Media	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
MA-3(3)	Prevent Unauthori	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
MA-4	Nonlocal Maintena	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
MA-4(1)	Auditing And	Descriptio n:																													
MA-4(2)	Document	Descriptio n:																													
MA-4(3)	Comparab	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
MA-4(6)	Cryptogra	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
MA-4(7)	Remote Disconnec	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
MA-5	Maintena	Descriptio n:	Planned		Common		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
MA-6	Timely Maintena	Descriptio n:																													
MP-1	Media Protectio	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoDI 5200.01	DoD CIO																						
MP-2	Media Access	Descriptio n:	Planned		Hybrid		10/20/2019					Constantly	Automated	Non-compliant	POA&M will be	Refer to ISSM															
MP-3	Media Marking	Descriptio n:																													
MP-4	Media Storage	Descriptio n:																													
MP-5	Media Transport	Descriptio n:																													
MP-5(4)	Cryptogra	Descriptio n:																													
MP-6	Media Sanitizati	Descriptio n:	Planned		Common		10/20/2019					Annually	Undetermined	Non-compliant	POA&M will be	Refer to ISSM															
MP-7	Media Use	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applies to portable															
MP-7(1)	Prohibit Use	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
PE-1	Physical And	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoDI 5200.08	DoD CIO																						
PE-2	Physical Access	Descriptio n:	Planned		Common		10/20/2019					Quarterly	Undetermined	Non-compliant	POA&M will be	Refer to ISSM															
PE-3	Physical Access	Descriptio n:	Planned		Common		10/20/2019					Annually	Undetermined	Non-compliant	POA&M will be	Refer to ISSM															
PE-3(1)	Informati	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
PE-4	Access Control	Descriptio n:																													
PE-5	Access Control	Descriptio n:																													
PE-6	Monitorin	Descriptio n:	Planned		Common		10/20/2019					Monthly	Undetermined	Non-compliant	POA&M will be	Refer to ISSM															
PE-6(1)	Intrusion Alarms /	Descriptio n:																													
PE-8	Visitor Access	Descriptio n:	Planned		Common		10/20/2019					Monthly	Undetermined	Non-compliant	POA&M will be	Refer to ISSM															
PE-9	Power Equipmen	Descriptio n:																													
PE-10	Emergenc	Descriptio n:																													
PE-11	Emergenc	Descriptio n:	Not Applicabl		Common	Applicable only to		Applicable only to																							
PE-12	Emergenc	Descriptio n:	Not Applicabl		Common	Not Applicabl		Not Applicabl																							
PE-13	Fire Protectio	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Inspect as needed															
PE-13(3)	Automatic	Descriptio n:																													
PE-14	Temperat	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Inspect as needed															

PE-15	Water Damage	Descriptio n:	Planned		Common		10/20/2019					Undeterm ined	Undeterm ined	Non-compliant	POA&M will be	Inspect as needed															
PE-16	Delivery And	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Refer to ISSM															
PE-17	Alternate	Descriptio n:																													
PL-1	Security Planning	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoDI 8510.01	DoD CIO																						
PL-2	System Security	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PL-2(3)	Plan / Coordinat	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Agreemen ts with															
PL-4	Rules Of Behavior	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PL-4(1)	Social Media	Descriptio n:																													
PL-8	Informati	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
PL-8(1)	Defense-In-Depth	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
PL-8(2)	Supplier Diversity	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
PM-1	Informati	Descriptio n:	Inherited	DoD	Common		12/1/2016	Inherited at the	DoD CIO																						
PM-2	Senior Informati	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD organizati	DoD CIO																						
PM-3	Informati	Descriptio n:	Inherited	DoD	System-Specific		12/1/2016	DoD planning	DoD CIO																						
PM-4	Plan Of Action	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PM-5	Informati	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PM-6	Informati	Descriptio n:	Inherited	DoD	Hybrid		12/1/2016	The Federal	DoD CIO																						
PM-7	Enterprise	Descriptio n:	Inherited	DoD	Common		12/1/2016	The applicatio	DoD CIO																						
PM-8	Critical Infrastruc	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoDD 3020.40	DoD CIO																						
PM-9	Risk Managem	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD Risk Managem	DoD CIO																						
PM-10	Security Authoriza	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoDI 8510.01	DoD CIO																						
PM-11	Mission/b	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applicabl e to															
PM-12	Insider Threat	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Service Level															
PM-13	Informati	Descriptio n:	Inherited	DoD	Common		4/18/2016	DoD 8570.01-	DoD CIO																						
PM-14	Testing, Training,	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Refer to ISSM															
PM-15	Contacts With	Descriptio n:	Inherited	Compone nt	Hybrid		10/1/2018	Inherited DoD Tier	DoD Compone																						
PM-16	Threat Awarenes	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Treat Awarenes															
PS-1	Personnel	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD 5200.2-R	DoD CIO																						
PS-2	Position Risk	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PS-3	Personnel	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Refer to ISSM															
PS-4	Personnel	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PS-4(1)	Post-employm	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
PS-5	Personnel	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Personnel records; ;															
PS-6	Access Agreemen	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
PS-6(3)	Post-employm	Descriptio n:	Not Applicabl		Common	Controls N/A for																									
PS-7	Third-party	Descriptio n:	Planned		Common		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	Refer to ISSM															
PS-8	Personnel	Descriptio n:	Planned		Common		10/20/2019					Undeterm ined	Undeterm ined	Non-compliant	POA&M will be	Personnel records															
RA-1	Risk Assessme	Descriptio n:	Inherited	DoD	Common		12/1/2016	NIST SP 800-30	DoD CIO																						
RA-2	Security Categoriz	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	System Security															
RA-3	Risk Assessme	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM															
RA-5	Vulnerabil	Descriptio n:	Planned		Hybrid		10/20/2019					Monthly	Manual	Non-compliant	POA&M will be	Refer to ISSM															
RA-5(1)	Update Tool	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
RA-5(2)	Update By Frequency	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
RA-5(4)	Discovera ble	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
RA-5(5)	Privileged Access	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-1	System And	Descriptio n:	Inherited	DoD	Common		12/1/2016	DoD has defined	DoD CIO																						
SA-2	Allocation	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Report non-															
SA-3	System Developm	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	POA&M															
SA-4	Acquisitio	Descriptio n:	Planned		System-Specific		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Contract Requirem															
SA-4(1)	Functiona	Descriptio n:																													
SA-4(2)	Design / Implemen	Descriptio n:																													
SA-4(7)	NIAP-approved	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
SA-4(9)	Functions	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
SA-4(10)	Use Of Approved	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	applies to use of															
SA-5	Informati	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	review SAR,															
SA-8	Security Engineeri	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
SA-9	External Informati	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applicabl e to															
SA-9(1)	Risk Assessme	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-9(2)	Identificat	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-10	Developer	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-10(1)	Software /	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									
SA-11	Developer	Descriptio n:																													
SA-12	Supply Chain	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-15	Developm	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																									
SA-15(9)	Use Of Live Data	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																									

SA-19	Compone	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																						
SC-1	System And	Descriptio n:	Inherited	DoD	Common		4/11/2016	DoD Compone	DoD CIO																			
SC-2	Applicatio	Descriptio n:																										
SC-4	Informati	Descriptio n:																										
SC-5	Denial Of Service	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Denial of Service												
SC-5(1)	Restrict Internal	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-5(2)	Excess Capacity /	Descriptio n:																										
SC-5(3)	Detection	Descriptio n:																										
SC-7	Boundary	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Network diagram;												
SC-7(3)	Access Points	Descriptio n:	Not Applicabl		Common	Controls N/A for																						
SC-7(4)	External Telecomm	Descriptio n:	Not Applicabl		Common	Controls N/A for																						
SC-7(5)	Deny By Default /	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(7)	Prevent Split	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																						
SC-7(8)	Route Traffic To	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(9)	Restrict Threateni	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(10)	Prevent Unauthori	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(11)	Restrict Incoming	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(12)	Host-based	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(13)	Isolation Of	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-7(14)	Protects Against	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-8	Transmiss	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-8(1)	Cryptogra	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-8(2)	Pre / Post	Descriptio n:																										
SC-10	Network Disconnec	Descriptio n:																										
SC-12	Cryptogra	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Applies to PKI												
SC-13	Cryptogra	Descriptio n:	Planned		Hybrid		10/20/2019	Applicabl e only to				Annually	Manual	Non-compliant	POA&M will be	Applicabl e only to												
SC-15	Collabora	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Undeterm ined	Non-compliant	POA&M will be	STIG/SRG; Report												
SC-17	Public Key	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-18	Mobile Code	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-18(1)	Identify Unaccept	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-18(2)	Acquisitio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-18(3)	Prevent Download	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-18(4)	Prevent Automatic	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-19	Voice Over	Descriptio n:	Not Applicabl		Hybrid	Not Applicabl		Not Applicabl								Applies to VoIP												
SC-20	Secure Name /	Descriptio n:	Not Applicabl		Hybrid	Not Applicabl		Not Applicabl								Applies to DNS												
SC-21	Secure Name /	Descriptio n:	Planned		Hybrid		10/20/2019					Undeterm ined	Manual	Non-compliant	POA&M will be	STIG/SRG; DNS Logs												
SC-22	Architectu	Descriptio n:	Not Applicabl		Hybrid	Not Applicabl		Not Applicabl						Non-compliant	POA&M will be	Applies to DNS												
SC-23	Session Authentici	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																						
SC-23(1)	Invalidate	Descriptio n:	Not Applicabl		System-Specific	Controls N/A for																						
SC-23(3)	Unique Session	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-23(5)	Allowed Certificat	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-28	Protectio	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-28(1)	Cryptogra	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-38	Operation	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SC-39	Process Isolation	Descriptio n:	Planned		System-Specific		10/20/2019					Undeterm ined	Manual	Non-compliant	POA&M will be	STIG/SRG; Report												
SI-1	System And	Descriptio n:	Inherited	DoD	Common		12/1/2016	Inherited by DoD	DoD CIO																			
SI-2	Flaw Remediati	Descriptio n:	Planned		Hybrid		10/20/2019					Undeterm ined	Manual	Non-compliant	POA&M will be	Refer to ISSM												
SI-2(1)	Central Managem	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-2(2)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-2(3)	Time To Remediat	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-2(6)	Removal Of	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-3	Malicious	Descriptio n:	Planned		Hybrid		10/20/2019					Undeterm ined	Manual	Non-compliant	POA&M will be	Refer to ISSM												
SI-3(1)	Central Managem	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-3(2)	Automatic	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-3(10)	Malicious	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4	Informati	Descriptio n:	Planned		Hybrid		10/20/2019					Constantl y	Manual	Non-compliant	POA&M will be	Refer to ISSM												
SI-4(1)	System-wide	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4(2)	Automate	Descriptio n:																										
SI-4(4)	Inbound And	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4(5)	System-generated	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4(10)	Visibility Of	Descriptio n:																										
SI-4(11)	Analyze Communi	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4(12)	Automate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						
SI-4(14)	Wireless Intrusion	Descriptio n:	Not Applicabl		Common	Controls N/A for																						
SI-4(15)	Wireless To	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																						

SI-4(16)	Correlate	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-4(19)	Individual	Descriptio n:	Not Applicabl		Common	Controls N/A for																				
SI-4(20)	Privileged	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-4(22)	Unauthori	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-4(23)	Host-based	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-5	Security Alerts,	Descriptio n:	Planned		Hybrid		10/20/2019					Annually	Manual	Non-compliant	POA&M will be	Refer to ISSM										
SI-7	Software,	Descriptio n:																								
SI-7(1)	Integrity Checks	Descriptio n:																								
SI-7(7)	Integratio	Descriptio n:																								
SI-7(8)	Auditing Capability	Descriptio n:																								
SI-7(14)	Binary Or	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-8	Spam Protectio	Descriptio n:																								
SI-8(1)	Central Managem	Descriptio n:																								
SI-8(2)	Automatic	Descriptio n:																								
SI-10	Informati	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-10(3)	Predictabl	Descriptio n:																								
SI-11	Error Handling	Descriptio n:	Not Applicabl		Hybrid	Controls N/A for																				
SI-12	Informati	Descriptio n:	Planned		Common		10/20/2019					Undetermined	Undetermined	Non-compliant	POA&M will be	Record retention										
SI-16	Memory Protectio	Descriptio n:																								

***** Unclassified//For Official Use Only *****

Exported on 27-Dec-2018 by AURA KEATING

Test Result Import Template: Test for Moderate vs High

Provided by eMASS

(System Type: Platform IT System, DoD Component: USCG)

Control / AP Information							Enter Test Results Here				Latest Test Results			
Control Number	Control Information	AP Acronym	CCI	CCI Definition	Implementation Guidance	Assessment Procedures	Compliance Status	Date Tested	Tested By	Test Results	Compliance Status	Date Tested	Tested By	Test Results
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.3	000001	The organization develops and documents an access control policy that addresses purpose, scope, roles	The organization being inspected/assessed develops and documents an access control policy that addresses purpose,	The organization conducting the inspection/assessment obtains and examines the access control policy to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.4	000002	The organization disseminates the access control policy to organization-defined	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. DoD	The organization conducting the inspection/assessment examines the access control policy via the organization's information sharing	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.5	000004	The organization develops and documents procedures to facilitate the implementation of the	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the access control	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.6	000005	The organization disseminates the procedures to facilitate access control policy and associated access	The organization being inspected/assessed disseminates via an information sharing capability to all personnel. The	The organization conducting the inspection/assessment examines the procedures to facilitate access control policy and associated access controls via	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.7	000003	The organization reviews and updates the access control policy in accordance with organization-defined	The organization being inspected/assessed annually reviews and updates the access control policy. The oranization	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the oranization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AC-1.9	000006	The organization reviews and updates the access control procedures in accordance with organization-defined	The organization being inspected/assessed annually reviews and updates the access control procedures. The	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the oranization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document				
AC-2(5)	Description: The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].	AC-2(5).1	002133	The organization defines other conditions when users are required to log out.	The organization being inspected/assessed defines and documents the other conditions when users are required to log	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(5)	Description: The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].	AC-2(5).2	000019	The organization requires that users log out in accordance with the organization-defined time	The organization being inspected/assessed documents in the user policies that users are required to log out at the end of	The organization conducting the inspection/assessment obtains and examines the user policies to ensure that users are required to log out at the end of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(7)	Description: The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes	AC-2(7).1	001958	The organization establishes privileged user accounts in accordance with a role-based access scheme that organizes	The organization being inspected/assessed documents and implements a process to establish privileged user	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(7)	Description: The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes	AC-2(7).2	001407	The organization administers privileged user accounts in accordance with a role-based access scheme that organizes	The organization being inspected/assessed documents and implements a process to administer privileged user	The organization conducting the inspection/assessment obtains and examines documented processes for privileged user account creation to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(7)	Description: The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes	AC-2(7).3	001360	The organization monitors privileged role assignments.	The organization being inspected/assessed implements a process to monitor privileged role assignments. The	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(7)	Description: The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes	AC-2(7).5	002137	The organization takes organization-defined actions when privileged role assignments are no longer	The organization being inspected/assessed documents and implements a process to disable (or revoke) the privileged	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of actions taken to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(9)	Description: The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].	AC-2(9).1	002140	The organization defines the conditions for establishing shared/group accounts.	The organization being inspected/assessed defines and documents the conditions for establishing shared/group	The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure they have been defined. DoD has	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(9)	Description: The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].	AC-2(9).2	002141	The organization only permits the use of shared/group accounts that meet organization-defined	The organization being inspected/assessed only permits the use of shared/group accounts that meet the	The organization conducting the inspection/assessment examines the shared/group accounts to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(10)	Description: The information system terminates shared/group account credentials when members leave the group.	AC-2(10).1	002142	The information system terminates shared/group account credentials when members leave the group.	The organization being inspected/assessed configures the information system to terminate shared/group account	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(12)	Description: The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]: and	AC-2(12).1	002146	The organization defines atypical usage for which the information system accounts are to be monitored.	The organization being inspected/assessed defines and documents atypical usage for which the information system	The organization conducting the inspection/assessment obtains and examines the documented atypical usage to ensure it has been defined. DoD has	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(12)	Description: The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]: and	AC-2(12).2	002147	The organization monitors information system accounts for organization-defined atypical use.	The organization being inspected/assessed monitors information system accounts for atypical use defined in AC-2 (12)	The organization conducting the inspection/assessment obtains and examines the audit trail of monitoring to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(12)	Description: The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]: and	AC-2(12).4	002149	The organization reports atypical usage of information system accounts to organization-defined	The organization being inspected/assessed documents and implements a process to resort atypical usaee defined in	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reporting to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-2(13)	Description: The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.	AC-2(13).2	002151	The organization disables accounts of users posing a significant risk within organization-defined time	The organization being inspected/assessed documents and implements a process to disable accounts of users posing	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-3(4)	Description: The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject	AC-3(4).1	002163	The organization defines the discretionary access control policies the information system is to enforce over	The organization being inspected/assessed defines and documents the discretionary access control policies the	The organization conducting the inspection/assessment obtains and examines the documented access control policies to ensure they have been	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-3(4)	Description: The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject	AC-3(4).2	002164	The organization specifies in the discretionary access control policies that a subject which has been	The organization being inspected/assessed documents the discretionary access control policies that a subject which has	The organization conducting the inspection/assessment obtains and examines the documented discretionary access control policies to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-3(4)	Description: The information system enforces [Assignment: organization-defined discretionary access control policies] over defined subjects and objects where the policy specifies that a subject	AC-3(4).3	002165	The information system enforces organization-defined discretionary access control policies over defined	The organization being inspected/assessed configures the information system to enforce the discretionary access	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-6(7)	Description: The organization: (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles	AC-6(7).1	002230	The organization reviews the privileges assigned to organization-defined roles or classes of users on an	The organization being inspected/assessed documents and implements a process to review the privileges assigned to	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-6(7)	Description: The organization: (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles	AC-6(7).4	002231	The organization reassigns or removes privileges, if necessary, to correctly reflect organizational	The organization being inspected/assessed documents and implements a process to reassign or remove privileges, if	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-6(8)	Description: The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.	AC-6(8).2	002233	The information system prevents organization-defined software from executing at higher privilege levels	The organization being inspected/assessed configures the information system to any software except software	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
AC-8	Description: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to	AC-8.8	001384	The information system, for publicly accessible systems, displays system use information organization-	The organization being inspected/assessed configures the information system to display the content of DTM 08-	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)				
AC-8	Description: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to	AC-8.10	001385	The information system, for publicly accessible systems, displays references, if any, to monitorine that are	The organization being inspected/assessed configures the information system to display references, if any, to	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)				
AC-8	Description: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to	AC-8.11	001386	The information system for publicly accessible systems displays references, if any, to recordine that are consistent	The organization being inspected/assessed configures the information system to display references, if any, to	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (D/E) (Source: UFC 4-010-06)				
AC-8	Description: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to	AC-8.12	001387	The information system for publicly accessible systems displays references, if any, to auditine that are consistent	The organization being inspected/assessed configures the information system to display references. if any, to	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)				
AC-8	Description: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to	AC-8.13	001388	The information system, for publicly accessible systems, includes a description of the authorized uses of the	The organization being inspected/assessed configures the information system to include a description of the	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)				
AC-10	Description: The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined	AC-10.1	000054	The information system limits the number of concurrent sessions for each organization-defined account	The organization being inspected/assessed configures the information system to limit the number of concurrent	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-10	Description: The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined	AC-10.2	000055	The organization defines the maximum number of concurrent sessions to be allowed for each	The organization being inspected/assessed defines and documents the maximum number of concurrent sessions	The organization conducting the inspection/assessment obtains and examines the documented maximum number to ensure the organization being								
AC-12(1)	Description: The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to	AC-12(1).2	002363	The information system provides a logout capability for user-initiated communications sessions	The organization being inspected/assessed configures the information system to provide a logout capability for	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-12(1)	Description: The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to	AC-12(1).3	002364	The information system displays an explicit logout message to users indicating the reliable termination of	The organization being inspected/assessed configures the information system to display an explicit logout	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.1	002256	The organization defines security attributes having organization-defined types of security attribute values	The organization being inspected/assessed defines and documents the security attributes having organization-	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.2	002257	The organization defines security attributes having organization-defined types of security attribute values	The organization being inspected/assessed defines and documents the security attributes having organization-	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.3	002258	The organization defines security attributes, having organization-defined types of security attribute values,	The organization being inspected/assessed defines and documents the security attributes having organization-	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.4	002259	The organization defines security attribute values associated with organization-defined types of security	The organization being inspected/assessed defines and documents the security attributes values associated with	The organization conducting the inspection/assessment obtains and examines the documented security attributes values to ensure the								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.5	002260	The organization defines security attribute values associated with organization-defined types of security	The organization being inspected/assessed defines and documents the security attributes values associated with	The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.6	002261	The organization defines security attribute values associated with organization-defined types of security	The organization being inspected/assessed defines and documents the security attributes values associated with	The organization conducting the inspection/assessment obtains and examines the documented security attribute values to ensure the								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.7	002262	The organization provides the means to associate organization-defined types of security attributes having	The organization being inspected/assessed configures the information system to provide the means to associate	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.8	002263	The organization provides the means to associate organization-defined types of security attributes having	The organization being inspected/assessed configures the information system to provide the means to associate	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.9	002264	The organization provides the means to associate organization-defined types of security attributes having	The organization being inspected/assessed configures the information system to provide the means to associate	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.10	002265	The organization ensures that the security attribute associations are made with the information.	The organization being inspected/assessed documents and implements a process to ensure that the security	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the oranization being								
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.11	002266	The organization ensures that the security attribute associations are retained with the information.	The organization being inspected/assessed documents and implements a process to ensure that the security	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being								

AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.14	002269	The organization establishes the permitted organization-defined security attributes for organization-defined	The organization being inspected/assessed establishes and documents the permitted security attributes for all	The organization conducting the inspection/assessment obtains and examines the documented list of permitted security attributes to ensure							
AC-16	Description: The organization: a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment:	AC-16.16	002271	The organization determines the permitted organization-defined values or ranges for each of the established	The organization being inspected/assessed establishes and documents the permitted values or ranges for each of the	The organization conducting the inspection/assessment obtains and examines the documented permitted values or ranges to ensure the							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).1	002291	The organization defines the security policies to be followed by personnel when associating organization-	The organization being inspected/assessed defines and documents the security policies to be followed by personnel	The organization conducting the inspection/assessment obtains and examines the documented security policies to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).2	002292	The organization defines the security attributes which are to be associated with organization-defined subjects	The organization being inspected/assessed defines and documents the security attributes which are to be	The organization conducting the inspection/assessment obtains and examines the documented security attributes to ensure the organization							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).3	002293	The organization defines the subjects to be associated, and that association maintained, with	The organization being inspected/assessed defines and documents the subjects to be associated, and that association	The organization conducting the inspection/assessment obtains and examines the documented subjects to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).4	002294	The organization defines the objects to be associated, and that association maintained, with organization-defined	The organization being inspected/assessed defines and documents the objects to be associated, and that association	The organization conducting the inspection/assessment obtains and examines the documented objects to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).5	002295	The organization allows personnel to associate organization-defined security attributes with organization-	The organization being inspected/assessed documents and implements a process requiring personnel to associate	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).6	002296	The organization allows personnel to associate organization-defined security attributes with organization-	The organization being inspected/assessed documents and implements a process requiring personnel to associate	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).7	002297	The organization allows personnel to maintain the association of organization-defined security attributes	The organization being inspected/assessed documents and implements a process requiring personnel to maintain	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being							
AC-16(6)	Description: The organization allows personnel to associate, and maintain the association of [Assignment: organization-defined security attributes] with [Assignment: organization-defined subjects and	AC-16(6).8	002298	The organization allows personnel to maintain the association of organization-defined security attributes	The organization being inspected/assessed documents and implements a process requiring personnel to maintain	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being							
AC-17(6)	Description: The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.	AC-17(6).1	000072	The organization ensures that users protect information about remote access mechanisms from	The organization being inspected/assessed implements and documents a process to ensure that users protect	The organization conducting the inspection/assessment obtains and examines the documented process to ensure that the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AC-17(9)	Description: The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period]	AC-17(9).2	002322	The organization provides the capability to expeditiously disconnect or disable remote access to the	The organization being inspected/assessed configures the information system to provide the capability to	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AC-18(3)	Description: The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and	AC-18(3).1	001449	The organization disables, when not intended for use, wireless networking capabilities internally	The organization being inspected/assessed documents and implements a process to disable wireless networking	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AC-18(4)	Description: The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	AC-18(4).1	002324	The organization identifies and explicitly authorizes users allowed to independently configure	The organization being inspected/assessed identifies and explicitly authorizes users allowed to independently	The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AC-20(3)	Description: The organization [Selection: restricts; prohibits] the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit	AC-20(3).1	002338	The organization restricts or prohibits the use of non-organizationally owned information systems, system	The organization being inspected/assessed documents and implements a process to restrict or prohibit the use of	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AC-22	Description: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;	AC-22.1	001473	The organization designates individuals authorized to post information onto a publicly accessible	The organization being inspected/assessed identifies and documents individuals authorized to post information	The organization conducting the inspection/assessment obtains and examines the list of individuals to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
AC-22	Description: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;	AC-22.2	001474	The organization trains authorized individuals to ensure that publicly accessible information does	The organization being inspected/assessed documents and implements a process to train authorized individuals to	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of the training	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
AC-22	Description: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;	AC-22.3	001475	The organization reviews the proposed content of information prior to posting onto the publicly accessible	The organization being inspected/assessed documents and implements a process to review the proposed content of	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
AC-22	Description: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;	AC-22.4	001476	The organization reviews the content on the publicly accessible information system for nonpublic	The organization being inspected/assessed documents and implements a process to review the content on the	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
AC-22	Description: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;	AC-22.6	001478	The organization removes nonpublic information from the publicly accessible information system, if	The organization being inspected/assessed documents and implements a process to remove nonpublic information	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
AC-23	Description: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to	AC-23.1	002343	The organization defines the data mining prevention techniques to be employed to adequately protect	The organization being inspected/assessed defines and documents the data mining prevention techniques to be	The organization conducting the inspection/assessment obtains and examines the documented data mining prevention techniques to ensure the							
AC-23	Description: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to	AC-23.2	002344	The organization defines the data mining detection techniques to be employed to adequately detect data	The organization being inspected/assessed defines and documents the data mining detection techniques to be	The organization conducting the inspection/assessment obtains and examines the documented data mining detection techniques to ensure the							
AC-23	Description: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to	AC-23.3	002345	The organization defines the data storage objects that are to be protected against data minine attempts	The organization being inspected/assessed defines and documents the data storage objects that are to be protected	The organization conducting the inspection/assessment obtains and examines the documented data storage objects to ensure the organization being							
AC-23	Description: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to	AC-23.4	002346	The organization employs organization-defined data mining prevention techniques for organization-	The organization being inspected/assessed configures the information system to emstov data minine prevention	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
AC-23	Description: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to	AC-23.5	002347	The organization employs organization-defined data mining detection techniques for organization-defined data	The organization being inspected/assessed configures the information system to emstov data minine detection	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
AT-3	Description: The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or	AT-3.2	000109	The organization provides role-based security training to personnel with assigned security roles and	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Awareness Training policy. See AT Policy document			
AT-3	Description: The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or	AT-3.3	000110	The organization provides refresher role-based security training to personnel with assigned security roles and	Privileged user type Security-related education/training available through DISA IASE (e.g. VTE, Skill Soft, other professional	The organization conducting the inspection/assessment obtains and examines documented records (IAW AT-4) of their privileged users training.	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Awareness Training policy. See AT Policy document			
AT-3(2)	Description: The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation	AT-3(2).1	001566	The organization provides organization-defined personnel or roles with initial training in the employment	The organization being inspected/assessed: 1. Identifies and documents physical security controls that	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AT-3(2)	Description: The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation	AT-3(2).2	001567	The organization provides organization-defined personnel or roles with refresher training in the	The organization being inspected/assessed: 1. Identifies and documents physical security controls that	The organization conducting the inspection/assessment obtains and examines: 1. Documentation of physical security	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AT-3(2)	Description: The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation	AT-3(2).4	002051	The organization defines the personnel or roles to whom initial and refresher training in the employment and	The organization being inspected/assessed defines and documents the personnel or roles to whom initial and	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AT-3(4)	Description: The organization provides training to its personnel on [Assignment: organization-defined indicators of malicious code] to recognize suspicious communications and anomalous	AT-3(4).1	002053	The organization provides training to its personnel on organization-defined indicators of malicious code	The organization being inspected/assessed provides training to its personnel on indicators of malicious code	The organization conducting the inspection/assessment obtains and examines the training materials and indicators of malicious code defined in AT	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AT-3(4)	Description: The organization provides training to its personnel on [Assignment: organization-defined indicators of malicious code] to recognize suspicious communications and anomalous	AT-3(4).2	002054	The organization defines indicators of malicious code to recognize suspicious communications and	The organization being inspected/assessed defines and documents indicators of malicious code to recognize	The organization conducting the inspection/assessment obtains and examines the documented indicators to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AT-4	Description: The organization: a. Documents and monitors individual information system security training activities including basic security awareness	AT-4.1	000113	The organization documents individual information system security training activities, including basic	The organization being inspected/assessed identifies and documents training activities to include basic	The organization conducting the inspection/assessment obtains and examines the security awareness training activities to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The role based security training activities are defined. See AT Policy document			
AT-4	Description: The organization: a. Documents and monitors individual information system security training activities including basic security awareness	AT-4.3	001336	The organization retains individual training records for an organization-defined time period	The organization being inspected/assessed will maintain records training records for at least 5 years or 5 years after	The organization conducting the inspection/assessment obtains and examines training records to ensure records have been maintained for at least	Compliant	06-Nov-2019	Derek Miller	The organization tracks RMF Awareness Training. See AT Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.1	001930	The organization defines the organizational personnel or roles to whom the audit and accountability policy is to be	The organization being inspected/assessed defines and documents any personnel or roles. in addition to the ISSO or	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.2	001931	The organization defines the organizational personnel or roles to whom the audit and accountability procedures	The organization being inspected/assessed defines and documents any personnel or roles. in addition to the ISSO or	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to whom the audit and	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.3	000117	The organization develops and documents an audit and accountability policy that addresses purpose. scope.	The organization being inspected/assessed develops and documents an audit and accountability policy that	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy to ensure that the audit and	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.4	001832	The organization disseminates the audit and accountability policy to [Assignment: organization-defined	The organization being inspected/assessed disseminates, via an information sharing capability, to the ISSO	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.5	000120	The organization develops and documents procedures to facilitate the implementation of the audit	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures to ensure that the procedures	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.6	001834	The organization disseminates to organization-defined personnel or roles procedures to facilitate the	The organization being inspected/assessed disseminates, via an information sharing capability, to the ISSO	The organization conducting the inspection/assessment obtains and examines the audit and accountability procedures via the inspected	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.7	000119	The organization reviews and updates the audit and accountability policy on an organization-defined	The organization being inspected/assessed reviews and updates the audit and accountability policy annually.	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	AU-1.9	000122	The organization reviews and updates the audit and accountability procedures on an organization-defined	The organization being inspected/assessed reviews and updates the audit and accountability procedures	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
AU-2	Description: The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-	AU-2.3	000124	The organization coordinates the security audit function with other organizational entities requiring audit-	The organization being inspected/assessed documents and implements within the audit and accountability policy and	The organization conducting the inspection/assessment obtains and examines the audit and accountability policy and procedures as well as artifacts	Compliant	06-Nov-2019	Derek Miller	Auditable events coordinated amongst other organizational entities. See AU Policy document			
AU-2	Description: The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-	AU-2.5	000126	The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to	The organization being inspected/assessed documents as well as audit logs to ensure	The organization conducting the inspection/assessment reviews the documented audit process as well as audit logs to ensure that the organization	Compliant	06-Nov-2019	Derek Miller	Information system auditable events defined. See AU Policy document			
AU-2(3)	Description: The organization reviews and updates the audited events [Assignment: organization-defined frequency].	AU-2(3).1	000127	The organization reviews and updates the list of organization-defined audited events on an organization-	The organization being inspected/assessed will conduct reviews of the list of auditable events as defined in AU-2 (d). CO	The organization conducting the inspection/assessment reviews the audit trail showing reviews and updates to the list of audited events to ensure that the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-3(1)	Description: The information system generates audit records containing the following additional information: [Assignment: organization-defined additional. more detailed information].	AU-3(1).2	001488	The organization defines additional, more detailed information to be included in the audit records.	The organization being inspected/assessed defines and documents additional, more detailed information to be	The organization conducting the inspection/assessment obtains and examines the documented list of additional more detailed information to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-4	Description: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].	AU-4.1	001848	The organization defines the audit record storage requirements.	The organization being inspected/assessed defines and documents the required audit record storage capacity. DoD	The organization conducting the inspection/assessment obtains and examines the documented audit record storage requirements to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-5	Description: The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure: and	AU-5.1	000139	The information system alerts designated organization-defined personnel or roles in the	The organization being inspected/assessed configures the information system to alert at a minimum. the SCA and ISSO	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-5	Description: The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure: and	AU-5.2	001572	The organization defines the personnel or roles to be alerted in the event of an audit processing failure.	The organization being inspected/assessed defines and documents any personnel or roles. in addition to the SCA and	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should be alerted	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-5(1)	Description: The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated	AU-5(1).1	001852	The organization defines the personnel, roles and/or locations to receive a warning when allocated	The organization being inspected/assessed defines and documents any personnel or roles. in addition to the	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive a	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-5(1)	Description: The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated	AU-5(1).4	001855	The information system provides a warning to organization-defined personnel. roles. and/or	The organization being inspected/assessed configures the information system to immediately provide a warning	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

AU-6	Description: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of	AU-6.1	000148	The organization reviews and analyzes information system audit records on an organization defined	The organization being inspected/assessed documents and implements a process to review and analyze information	The organization conducting the inspection/assessment obtains and examines the documented process for audit trail reviews as well as the audit	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-6	Description: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of	AU-6.3	001862	The organization defines the types of inappropriate or unusual activity to be reviewed and analyzed in the	The organization being inspected/assessed defines and documents the types of inappropriate or unusual activity	The organization conducting the inspection/assessment obtains and examines the documented types of inappropriate or unusual activity to	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-6	Description: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of	AU-6.4	000149	The organization reports any findings to organization-defined personnel or roles for indications of	The organization being inspected/assessed documents and implements a process for reporting any findings of	The organization conducting the inspection/assessment obtains and examines the documented process for reporting findings as well as a sampling of	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-6	Description: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of	AU-6.5	001863	The organization defines the personnel or roles to receive the reports of organization-defined inappropriate or	The organization being inspected/assessed defines and documents any personnel or roles, in addition to the ISSO and	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles who should receive the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-6(1)	Description: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to	AU-6(1).1	001864	The organization employs automated mechanisms to integrate audit review and analysis to support	The organization being inspected/assessed identifies and implements automated mechanisms to integrate audit	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-6(1)	Description: The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to	AU-6(1).2	001865	The organization employs automated mechanisms to integrate reporting processes to support organizational	The organization being inspected/assessed identifies and implements automated mechanisms to integrate	The organization conducting the inspection/assessment obtains and examines documentation identifying automated mechanisms to integrate	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-6(3)	Description: The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	AU-6(3).1	000153	The organization analyzes and correlates audit records across different repositories to gain organization-wide	The organization being inspected/assessed documents and implements a process to analyse and correlate audit	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of analysis to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-6(4)	Description: The information system provides the capability to centrally review and analyze audit records from multiple components within the system.	AU-6(4).1	000154	The information system provides the capability to centrally review and analyze audit records from multiple	The organization being inspected/assessed configures the information system to provide a capability to centrally	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-6(10)	Description: The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information.	AU-6(10).1	001872	The organization adjusts the level of audit review and analysis within the information system when	The organization being inspected/assessed documents and implements a process for adjusting the level of audit	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-6(10)	Description: The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information.	AU-6(10).2	001874	The organization adjusts the level of audit reporting within the information system when there is a	The organization being inspected/assessed documents and implements a process for adjusting the level of audit	The organization conducting the inspection/assessment obtains and examines the documented process and supporting records to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-8	Description: The information system: a. Uses internal system clocks to generate time stamps for audit records; and	AU-8.3	001889	The information system records time stamps for audit records that meets organization-defined	The organization being inspected/assessed configures the information system to generate time in the time	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed							
AU-9	Description: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	AU-9.6	001495	The information system protects audit tools from unauthorized deletion.	The organization being inspected/assessed configures the information system to disallow unauthorized deletion	The organization conducting the inspection/assessment examines the information system to ensure that the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-9(4)	Description: The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].	AU-9(4).1	001894	The organization defines the subset of privileged users who will be authorized access to the management of	The organization being inspected/assessed defines and documents the subset of privileged users to be authorized	The organization conducting the inspection/assessment obtains and examines the documented subset of privileged users to be authorized access	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-9(4)	Description: The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].	AU-9(4).2	001351	The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset	The organization being inspected/assessed authorizes access to the management of audit functionality to only the	The organization conducting the inspection/assessment obtains and examines the documentation of access authorizations for the management of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-10	Description: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be	AU-10.1	000166	The information system protects against an individual (or process acting on behalf of an individual) falsely	The organization being inspected/assessed configures the information system to protect against an individual	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
AU-11	Description: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact	AU-11.1	000167	The organization retains audit records for an organization defined time period to provide support for	The organization being inspected/assessed will take action to ensure it retains audit records for 5 years for SAMI-	The organization conducting the inspection/assessment reviews the information system audit records and any other relevant documents or records to	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Audit and Accountability policy. See AU Policy document			
AU-11(1)	Description: The organization employs [Assignment: organization-defined measures] to ensure that long-term audit records generated by the information system can be retrieved.	AU-11(1).1	002044	The organization defines measures to be employed to ensure that long-term audit records generated by the	The organization being inspected/assessed defines and documents measures to be employed to ensure that long-	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-11(1)	Description: The organization employs [Assignment: organization-defined measures] to ensure that long-term audit records generated by the information system can be retrieved.	AU-11(1).2	002045	The organization employs organization-defined measures to ensure that long-term audit records generated	The organization being inspected/assessed employs the measures defined in AU-11 (1), CCI 2044 to ensure that long-	The organization conducting the inspection/assessment obtains and examines the documented measures to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12	Description: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined	AU-12.3	000171	The information system allows organization-defined personnel or roles to select which auditable events are	The organization being inspected/assessed configures the information system to ensure that only the ISSM or	The organization conducting the inspection/assessment examines a sampling of information system components and confirms that the	Compliant	06-Nov-2019	Derek Miller	DoD has defined the personnel or roles as the ISSM or individuals appointed by the ISSM. See AU Policy document			
AU-12(1)	Description: The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail	AU-12(1).2	000174	The information system compiles audit records from organization-defined information system	The organization being inspected/assessed configures the information system to compile audit records from	The organization conducting the inspection/assessment examines the information system to ensure the information system is configured to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(1)	Description: The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail	AU-12(1).3	001577	The organization defines the information system components from which audit records are to be	The organization being inspected/assessed will define components and document the information system components from which	The organization conducting the inspection/assessment obtains and examines the system-wide audit trail documentation to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(3)	Description: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the audittime to be performed on [Assignment:	AU-12(3).1	001911	The organization defines the selectable event criteria to be used as the basis for changes to the auditime to be	The organization being inspected/assessed defines and documents the selectable event criteria for which chaneed	The organization conducting the inspection/assessment obtains and examines the documented selectable event criteria to ensure the oranization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(3)	Description: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditime to be performed on [Assignment:	AU-12(3).2	001912	The organization defines the time thresholds for organizational-defined individuals or roles to change	The organization being inspected/assessed defines and documents the time thresholds for individuals or roles to change	The organization conducting the inspection/assessment obtains and examines the documented time thresholds to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(3)	Description: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditime to be performed on [Assignment:	AU-12(3).3	001913	The organization defines the individuals or roles that are to be provided the capability to change the auditime to be	The organization being inspected/assessed defines and documents the individuals or roles that are to be provided the	The organization conducting the inspection/assessment obtains and examines the documented individuals or roles to ensure the oranization beine	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(3)	Description: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditime to be performed on [Assignment:	AU-12(3).4	001914	The information system provides the capability for organization-defined individuals or roles to change	The organization being inspected/assessed configures the information system to provide the capability for	The organization conducting the inspection/assessment examines the information system to ensure the organization beine inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-12(3)	Description: The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment:	AU-12(3).5	002047	The organization defines the information system components on which the auditing that is to be	The organization being inspected/assessed defines and documents the information system components on which	The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-14	Description: The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	AU-14.1	001919	The information system provides the capability for authorized users to select a user session to	The organization being inspected/assessed configures the information system to provide the capability for	The organization conducting the inspection/assessments examines the information system to ensure the organization beine inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-14(1)	Description: The information system initiates session audits at system start-up.	AU-14(1).1	001464	The information system initiates session audits at system start-up.	The organization being inspected/assessed configures the information system to initiate session audits at system	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-14(2)	Description: The information system provides the capability for authorized users to capture/record and log content related to a user session.	AU-14(2).1	001462	The information system provides the capability for authorized users to capture/record and log	The organization being inspected/assessed configures the information system to provide the capability for	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
AU-14(3)	Description: The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	AU-14(3).1	001920	The information system provides the capability for authorized users to remotely view/hear all content related	The organization being inspected/assessed configures the information system to provide the capability for	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CA-1.5	000242	The organization develops and documents procedures to facilitate the implementation of the	The organization being inspected/assessed develops and documents, IAW DoDI 8510.01, procedures to facilitate the	The organization conducting the inspection/assessment obtains and examines the procedures to ensure the organization beine inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CA-1.6	000243	The organization disseminates to organization-defined personnel or roles procedures to facilitate the	The organization being inspected/assessed will require all personnel to register at the DTIC website to receive update	The organization conducting the inspection/assessment obtains and examines the AUP (Acceptable Use Policy), appointment orders, or written	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CA-1.9	000244	The organization reviews and updates the current security assessment and authorization procedures in	The organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and	The organization conducting the inspection/assessment obtains and examines the audit trail of review and update actvities to ensure the oranization	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CA-3(1)	Description: The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, national security system] to an external network without the use of	CA-3(1).1	000262	The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, national security system] to an	The organization being inspected/assessed documents in its policy and procedures addressing information system	The organization conducting the inspection/assessment obtains and examines policy document prohibiting direct connection of all unclassified NSS	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CA-3(1)	Description: The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, national security system] to an external network without the use of	CA-3(1).3	002073	The organization defines the boundary protection device to be used to connect oranization-defined	The organization being inspected/assessed defines and documents the boundary protection device to be used to	The organization conducting the inspection/assessment obtains and examines the documented boundary protection device to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.3	000287	The organization develops and documents a configuration management policy that addresses	The organization being inspected/assessed develops and documents a configuration management policy that	The organization conducting the inspection/assessment obtains and examines the configuration management policy that addresses purpose, scope	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.4	001822	The organization disseminates the configuration management policy to oranization	The organization being inspected/assessed disseminates a configuration management policy via an information sharing	The organization conducting the inspection/assessment obtains and examines the configuration management policy via the inspected oranization's	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.5	000290	The organization develops and documents procedures to facilitate the implementation of the	The organization being inspected/assessed develops and documents procedures to facilitate the implementation of	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.6	001825	The organization disseminates to organization-defined personnel or roles the procedures to facilitate	The organization being inspected/assessed disseminates the procedures to facilitate the implementation of the	The organization conducting the inspection/assessment obtains and examines the procedures to facilitate the implementation of the configuration	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.8	000289	The organization reviews and updates, on an organization defined frequency, the configuration management	The organization being inspected/assessed reviews and updates, annually, the configuration management	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	CM-1.9	000292	The organization reviews and updates, on an organization defined frequency, the procedures to facilitate the	The organization being inspected/assessed reviews and updates, annually, the procedures to facilitate the	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
CM-2(1)	Description: The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency];	CM-2(1).1	000296	The organization reviews and updates the baseline configuration of the information system at an	The organization being inspected/assessed reviews and updates the baseline configuration of the information	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-2(1)	Description: The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency];	CM-2(1).3	000297	The organization reviews and updates the baseline configuration of the information system when	The organization being inspected/assessed reviews and updates the baseline configuration of the information	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-2(1)	Description: The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency];	CM-2(1).5	000298	The organization reviews and updates the baseline configuration of the information system at an	The organization being inspected/assessed reviews and updates the baseline configuration of the information	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-2(1)	Description: The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency];	CM-2(1).6	000299	The organization reviews and updates the baseline configuration of the information system as an	The organization being inspected/assessed reviews and updates the baseline configuration of the information	The organization conducting the inspection/assessment obtains and examines documentation of organizational reviews and update	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-2(3)	Description: The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.	CM-2(3).1	000304	The organization retains organization-defined previous versions of baseline configurations of the	The organization being inspected/assessed retains the previous approved baseline configuration of IS components	The organization conducting the inspection/assessment obtains and examines the documentation of the previous version of the baseline							
CM-2(7)	Description: The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment:	CM-2(7).3	001739	The organization issues organization-defined information systems, system components, or devices with	The organization being inspected/assessed issues information systems, system components, or devices as	The organization conducting the inspection/assessment interviews organizational personnel with configuration management							
CM-2(7)	Description: The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment:	CM-2(7).4	001815	The organization defines the security safeguards to be applied to devices when they return from areas of	The organization being inspected/assessed defines and documents, in the configuration management policy, the security	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the oranization beine							
CM-2(7)	Description: The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment:	CM-2(7).5	001816	The organization applies organization-defined security safeguards to devices when individuals return from areas	The organization being inspected/assessed applies security safeguards as defined in CM-2 (7) CCI 1835 to devices	The organization conducting the inspection/assessment interviews organizational personnel with configuration management							
CM-3	Description: The organization: a. Determines the types of changes to the information system that are configuration-controlled:	CM-3.1	000313	The organization determines the types of changes to the information system that are configuration controlled.	The organization being inspected/assessed determines the types of changes to the information system that are to	The organization conducting the inspection/assessment obtains and examines the configuration management policy and plan to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CM-3	Description: The organization: a. Determines the types of changes to the information system that are configuration-controlled:	CM-3.5	001819	The organization implements approved configuration-controlled changes to the information system	The organization being inspected/assessed implements approved configuration-controlled changes to the	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the implementation of approved	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

CM-3	Description: The organization: a. Determines the types of changes to the information system that are configuration-controlled;	CM-3.6	000316	The organization retains records of configuration-controlled changes to the information system for an	The organization being inspected/assessed retains records of all configuration-controlled changes to the	The organization conducting the inspection/assessment obtains and examines the records of all configuration-controlled changes to the information	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-3	Description: The organization: a. Determines the types of changes to the information system that are configuration-controlled;	CM-3.8	000318	The organization audits and reviews activities associated with configuration controlled changes to the system.	The organization being inspected/assessed audits and reviews activities associated with configuration-controlled	The organization conducting the inspection/assessment obtains and examines the audit trail documenting the review activities associated with	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-3	Description: The organization: a. Determines the types of changes to the information system that are configuration-controlled;	CM-3.10	000320	The organization defines frequency to convene configuration change control element.	The organization being inspected/assessed defines within their CCB Charter, the frequency for configuration	The organization conducting the inspection/assessment obtains and examines the CCB Charter to ensure the frequency for configuration change	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-3(2)	Description: The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	CM-3(2).2	000328	The organization validates changes to the information system before implementing the changes on the	The organization being inspected/assessed documents and implements a process to validate changes to the	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of validation								
CM-3(2)	Description: The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	CM-3(2).3	000329	The organization documents changes to the information system before implementing the changes on the	The organization being inspected/assessed documents and implements a process to document changes to the	The organization conducting the inspection/assessment obtains and examines the documented process as well as documentation of changes to the								
CM-3(4)	Description: The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].	CM-3(4).1	000332	The organization requires an information security representative to be a member of the organization-	The organization being inspected/assessed requires an information security representative to be a member	The organization conducting the inspection/assessment obtains and examines the membership list of the organization's configuration control	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-3(6)	Description: The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.	CM-3(6).2	001746	The organization ensures that cryptographic mechanisms used to provide organization-defined security	The organization being inspected/assessed ensures that cryptographic mechanisms used to provide all security safeguards	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure that cryptographic	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-4(1)	Description: The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to	CM-4(1).1	001817	The organization, when analyzing changes to the information system, looks for security impacts due to	The organization being inspected/assessed documents within their process for analyzing changes to the	The organization conducting the inspection/assessment obtains and examines the documented process and record of analysis to ensure the								
CM-4(1)	Description: The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to	CM-4(1).2	001818	The organization analyzes changes to the information system in a separate test environment before	The organization being inspected/assessed documents and employs a policy to analyze changes to the information	The organization conducting the inspection/assessment obtains and examines the documented policy for analyzing changes as well as records of								
CM-5(1)	Description: The information system enforces access restrictions and supports auditing of the enforcement actions.	CM-5(1).1	001813	The information system enforces access restrictions.	The organization being inspected/assessed documents and implements a process to enforce access restrictions	The organization conducting the inspection/assessment obtains and examines the documented process as well as the configuration of the								
CM-5(1)	Description: The information system enforces access restrictions and supports auditing of the enforcement actions.	CM-5(1).2	001814	The Information system supports auditing of the enforcement actions.	The organization being inspected/assessed leverages only information systems which support auditing of enforcement	The organization conducting the inspection/assessment reviews vendor documentation to ensure the information system supports auditing of the								
CM-5(2)	Description: The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether	CM-5(2).2	000349	The organization reviews information system changes per organization defined frequency to determine	The organization being inspected/assessed documents in the configuration management policy and	The organization conducting the inspection/assessment obtains and examines the documented process for information system change review as well								
CM-5(2)	Description: The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether	CM-5(2).3	000350	The organization reviews information system changes upon organization-defined circumstances to determine	The organization being inspected/assessed documents and implements a process to review the information system	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of reviews to ensure								
CM-5(5)	Description: The organization: (a) Limits privileges to change information system components and system-related information within a production or	CM-5(5).1	001753	The organization limits privileges to change information system components within a	The organization being inspected/assessed documents and implements a process to limit privileges to change	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-5(5)	Description: The organization: (a) Limits privileges to change information system components and system-related information within a production or	CM-5(5).2	001754	The organization limits privileges to change system-related information within a production or operational	The organization being inspected/assessed documents and implements a process to limit privileges to change systems	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-5(5)	Description: The organization: (a) Limits privileges to change information system components and system-related information within a production or	CM-5(5).5	001829	The organization reviews information system privileges per organization defined frequency.	The organization being inspected/assessed reviews information system privileges every 90 days. The organization	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-5(5)	Description: The organization: (a) Limits privileges to change information system components and system-related information within a production or	CM-5(5).6	001830	The organization reevaluates information system privileges per organization defined frequency.	The organization being inspected/assessed reevaluates information system privileges every 90 days. The organization	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-5(6)	Description: The organization limits privileges to change software resident within software libraries.	CM-5(6).1	001499	The organization limits privileges to change software resident within software libraries.	The organization being inspected/assessed documents and implements a process to limit privileges to accounts	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-6	Description: The organization: a. Establishes and documents configuration settings for information technology products employed within the	CM-6.10	001756	The organization defines the operational requirements on which the configuration settings for the organization	The organization being inspected/assessed must define and document in the system security plan, the requirements	The organization conducting the inspection/assessment obtains and examines the system security plan to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document				
CM-6	Description: The organization: a. Establishes and documents configuration settings for information technology products employed within the	CM-6.11	001502	The organization monitors changes to the configuration settings in accordance with organizational policies and	The organization being inspected/assessed develops and documents a process for monitoring changes to the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy for monitoring to the configuration settings. See CM Policy document				
CM-6	Description: The organization: a. Establishes and documents configuration settings for information technology products employed within the	CM-6.12	001503	The organization controls changes to the configuration settings in accordance with organizational policies and	The organization being inspected/assessed develops and documents a process for controlling changes to the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy for monitoring to the configuration settings. See CM Policy document				
CM-6(1)	Description: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system	CM-6(1).1	000370	The organization employs automated mechanisms to centrally manage configuration settings for	The organization being inspected/assessed identifies, documents in the configuration management policy, and	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being								
CM-6(1)	Description: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system	CM-6(1).2	000371	The organization employs automated mechanisms to centrally apply configuration settings for organization-	The organization being inspected/assessed identifies, documents in the configuration management policy, and	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being								
CM-6(1)	Description: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system	CM-6(1).3	000372	The organization employs automated mechanisms to centrally verify configuration settings for organization-	The organization being inspected/assessed identifies, documents in the configuration management policy, and	The organization conducting the inspection/assessment obtains and examines the configuration management policy to ensure the organization being								
CM-6(1)	Description: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system	CM-6(1).4	002059	The organization defines the information system components for which the [Assignment: organization-defined information system	The organization being inspected/assessed defines and documents the information system components for which	The organization conducting the inspection/assessment obtains and examine the documented information system components to ensure the								
CM-7(1)	Description: The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure	CM-7(1).1	000384	The organization reviews the information system per organization defined frequency to identify	The organization being inspected/assessed documents and implements a process to review the information system	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail of reviews to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document				
CM-7(3)	Description: The organization ensures compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].	CM-7(3).2	000388	The organization ensures compliance with organization-defined registration requirements for	The organization being inspected/assessed implements DoDI 8551.01. DoD has defined the registration requirements as	The organization conducting the inspection/assessment obtains and examines a documented listing of ports, protocols, and services in use, and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8	Description: The organization: a. Develops and documents an inventory of information system components that:	CM-8.7	001780	The organization reviews and updates the information system component inventory per organization-defined	The organization being inspected/assessed documents and implements a process to review and update the	The organization conducting the inspection/assessment obtains and examines the documented process for reviews and updates as well as the audit	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document				
CM-8(1)	Description: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	CM-8(1).1	000408	The organization updates the inventory of information system components as an integral part of component	The organization being inspected/assessed documents and implements a process to update the inventory of	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of								
CM-8(1)	Description: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	CM-8(1).2	000409	The organization updates the inventory of information system components as an integral part of component	The organization being inspected/assessed documents and implements a process to update the inventory of	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of								
CM-8(1)	Description: The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	CM-8(1).3	000410	The organization updates the inventory of information system components as an integral part of component	The organization being inspected/assessed documents and implements a process to update the inventory of	The organization conducting the inspection/assessment obtains and examines the documented process for updates as well as the audit trail of								
CM-8(2)	Description: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	CM-8(2).1	000411	The organization employs automated mechanisms to help maintain an up-to-date inventory of information	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(2)	Description: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	CM-8(2).2	000412	The organization employs automated mechanisms to help maintain a complete inventory of information	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(2)	Description: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	CM-8(2).3	000413	The organization employs automated mechanisms to help maintain a accurate inventory of information	The organization being inspected/assessed documents and implements automated mechanisms to help maintain an	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(2)	Description: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	CM-8(2).4	000414	The organization employs automated mechanisms to help maintain a readily available inventory of	The organization being inspected/assessed documents and implements automated mechanisms to help maintain a	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanism used to help	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(3)	Description: The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized	CM-8(3).2	000416	The organization employs automated mechanisms, per organization defined frequency, to detect the	The organization being inspected/assessed documents and implements automated mechanisms to detect the	The organization conducting the inspection/assessment obtains and examines the documentation identifying the automated mechanisms and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(3)	Description: The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized	CM-8(3).3	001783	The organization defines the personnel or roles to be notified when unauthorized hardware, software, and	The organization being inspected/assessed defines and documents any personnel or roles. In addition to the ISSO or	The organization conducting the inspection/assessment obtains and examines the documented list of personnel or roles to be notified when	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-8(3)	Description: The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized	CM-8(3).4	001784	When unauthorized hardware, software, and firmware components are detected within the	The organization being inspected/assessed documents and implements a process to take action to disable network	The organization conducting the inspection/assessment obtains and examines the documented process and audit trail for taking action upon	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.1	000421	The organization develops and documents a configuration management plan for the information	The organization being inspected/assessed will develop and document a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it addresses and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.2	000423	The organization implements a configuration management plan for the information system that addresses roles	The organization being inspected/assessed will implement a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.3	001790	The organization develops and documents a configuration management plan for the information	The organization being inspected/assessed will develop and document a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify it establishes and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.4	001792	The organization implements a configuration management plan for the information system that establishes a	The organization being inspected/assessed will implement a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.5	001793	The organization develops and documents a configuration management plan for the information	The organization being inspected/assessed will develop and document a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it establishes and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.6	001795	The organization implements a configuration management plan for the information system that establishes a	The organization being inspected/assessed will implement a configuration management plan that has a	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.7	000424	The organization develops and documents a configuration management plan for the information	The organization being inspected/assessed will develop and document a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure it defines and documents	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.8	000426	The organization implements a configuration management plan for the information system that defines the	The organization being inspected/assessed will implement a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.9	001796	The organization develops and documents a configuration management plan for the information	The organization being inspected/assessed will develop and document a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.10	001798	The organization implements a configuration management plan for the information system that places the	The organization being inspected/assessed will implement a configuration management plan for the	The organization conducting the inspection/assessment obtains and examines the configuration management plan as well as evidence of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.11	001799	The organization develops a configuration management plan for the information system that protects the	The organization being inspected/assessed must develop and document a plan to protect the configuration	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that it identifies the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-9	Description: The organization develops, documents, and implements a configuration management plan for the information system that:	CM-9.12	001801	The organization implements a configuration management plan for the information system that protects the	The organization being inspected/assessed must implement a plan to protect the confiuration manaement plan	The organization conducting the inspection/assessment obtains and examines the configuration management plan to verify that the identified	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
CM-11	Description: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users	CM-11.1	001804	The organization defines the policies for governing the installation of software by users.	The organization being inspected/assessed must define policies governing the installation of software by users	The organization conducting the inspection/assessment obtains and examines policies governing the installation of software by users to e..	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Policy governing the installation of software by users is established by Components.				

CM-11	Description: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;	CM-11.2	001805	The organization establishes organization-defined policies governing the installation of software by users.	The organization being inspected/assessed documents their policies governing the installation of software by users	The organization conducting the inspection/assessment obtains and examines documented policies governing the installation of software by users to e	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Policy governing the installation of software by users is established by Components.			
CM-11	Description: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;	CM-11.3	001806	The organization defines methods to be employed to enforce the software installation policies.	The organization being inspected/assessed must define and document the methods employed to enforce the	The organization conducting the inspection/assessment obtains and examines documentation of the methods employed to ensure the organization	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document			
CM-11	Description: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;	CM-11.4	001807	The organization enforces software installation policies through organization-defined methods.	The organization being inspected/assessed must enforce software installation policies as defined in CM-11 CCI 1804	The organization conducting the inspection/assessment obtains and examines software installation policies defined in CM-11 CCI 1804 and inspects	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document			
CM-11	Description: The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;	CM-11.6	001809	The organization monitors software installation policy compliance per organization-defined frequency.	The organization being inspected/assessed must monitor software installation policy compliance at least	The organization conducting the inspection/assessment obtains and examines the audit trails of monitoring activities to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Configuration Management policy. See CM Policy document			
CM-11(2)	Description: The information system prohibits user installation of software without explicit privileged status	CM-11(2).1	001812	The information system prohibits user installation of software without explicit privileged status.	The organization being inspected/assessed must configure the information system to prevent the	The organization conducting the inspection/assessment obtains and examines the configuration of the information system components to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.2	000444	The organization develops a contingency plan for the information system that identifies essential business	The organization being inspected/assessed must clearly and accurately document essential business functions for	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not business systems (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.8	000450	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining essential missions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Applicable only to CS with essential mission function (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.9	000451	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining business functions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not business systems (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.10	000452	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining essential missions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Applicable only to CS with essential mission function (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.11	000453	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining business functions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not business systems (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.12	000454	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining essential missions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Applicable only to CS with essential mission function (Source: UFC 4-010-06)			
CP-2	Description: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and	CP-2.13	000455	The organization develops a contingency plan for the information system that addresses maintaining	The organization being inspected/assessed must clearly and accurately document maintaining business functions	The organization conducting the inspection/assessment obtains and examines the contingency plan to ensure it clearly and accurately documents	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not business systems (Source: UFC 4-010-06)			
CP-2(3)	Description: The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.	CP-2(3).4	000476	The organization plans for the resumption of essential business functions within the organization-defined time	The organization being inspected/assessed shall document within their contingency plan, procedures for	The organization conducting the inspection/assessment obtains the contingency plan to ensure it contains procedures for resumption of essential							
CP-2(8)	Description: The organization identifies critical information system assets supporting essential missions and business functions.	CP-2(8).2	002829	The organization identifies critical information system assets supporting essential business functions.	The organization being inspected/assessed identifies and documents critical information system assets	The organization conducting the inspection/assessment obtains and examines the documented list of critical information system assets supporting							
CP-7	Description: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of	CP-7.3	000514	The organization establishes an alternate processing site including necessary agreements to permit the	The organization being inspected/assessed documents and gains approval for alternate processing site agreements that	The organization conducting the inspection/assessment obtains and examines the approved alternate processing site agreements to ensure the							
CP-8	Description: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information	CP-8.4	000525	The organization establishes alternate telecommunication services including necessary agreements to permit the	The organization being inspected/assessed documents and gains approval for alternate telecommunication service	The organization conducting the inspection/assessment obtains and examines the approved alternate telecommunications service agreements							
CP-8	Description: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information	CP-8.6	002841	The organization defines the information system operations to be resumed for essential business functions	The organization being inspected/assessed defines and documents the information system operations to be	The organization conducting the inspection/assessment obtains and examines the documented information system operations to ensure the							
CP-9(5)	Description: The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent	CP-9(5).2	000548	The organization transfers information system backup information to the alternate storage site in accordance	The organization being inspected/assessed performs the transfer of information system backup information to the	The organization conducting the inspection/assessment obtains and examines the contingency plan and related logs to ensure the organization							
IA-2(4)	Description: The information system implements multifactor authentication for local access to non-privileged accounts.	IA-2(4).1	000768	The information system implements multifactor authentication for local access to non-privileged	The organization being inspected/assessed configures the information system to implement multifactor	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
IA-2(5)	Description: The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.	IA-2(5).1	000770	The organization requires individuals to be authenticated with an individual authenticator	The organization being inspected/assessed requires individuals or configures the information system to require	The organization conducting the inspection/assessment obtains and examines standard operating procedures or system documentation to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-2(9)	Description: The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	IA-2(9).1	001942	The information system implements replay-resistant authentication mechanisms for network access to non-	The organization being inspected/assessed configures the information system to implement replay-resistant	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
IA-4(4)	Description: The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].	IA-4(4).2	000801	The organization manages individual identifiers by uniquely identifying each individual as organization-	The organization being inspected/assessed documents and implements a process to manage individual identifiers by	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(4)	Description: The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements].	IA-5(4).2	001977	The organization employs automated tools to determine if password authenticators are sufficiently	The organization being inspected/assessed implements automated tools to check passwords strength per the	The organization conducting the inspection/assessment examines the automated tools and inspects the configuration of the automated tools to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(7)	Description: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	IA-5(7).1	000202	The organization ensures unencrypted static authenticators are not embedded in access scripts	The organization being inspected/assessed documents and implements requirements that unencrypted static	The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(7)	Description: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	IA-5(7).2	000203	The organization ensures unencrypted static authenticators are not stored on function keys.	The organization being inspected/assessed documents and implements requirements that unencrypted static	The organization conducting the inspection/assessment obtains and examines the requirements that unencrypted static authenticators not be	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(7)	Description: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	IA-5(7).3	002367	The organization ensures unencrypted static authenticators are not embedded in applications.	The organization being inspected/assessed documents and implements requirements that static authenticators are	The organization conducting the inspection/assessment obtains and examines the requirements that static authenticators are not embedded in	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(8)	Description: The organization implements [Assignment: organization-defined security safeguards] to manage the risk of compromise due to individuals having accounts on multiple information	IA-5(8).2	001621	The organization implements organization-defined security safeguards to manage the risk of compromise due to	The organization being inspected/assessed documents and implements policies and user training including advising	The organization conducting the inspection/assessment obtains and examines the documented policies as well as training records to ensure that the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(13)	Description: The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].	IA-5(13).1	002006	The organization defines the time period after which the use of cached authenticators are prohibited.	The organization being inspected/assessed defines and documents the time period after which the use of cached	The organization conducting the inspection/assessment obtains and examines the documented time period to ensure it has been defined. DoD has	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IA-5(13)	Description: The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].	IA-5(13).2	002007	The information system prohibits the use of cached authenticators after an organization-defined time	The organization being inspected/assessed configures the information system to prohibit the use of cached	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Cached authenticators are prohibited by Component level policy.			
IR-2	Description: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:	IR-2.3	000814	The organization provides refresher incident response training in accordance with organization-defined	The organization being inspected/assessed documents and implements a process to provide incident response	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of	Compliant	06-Nov-2019	Derek Miller	The organization provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. Training is compliant with DoDD 8570.01 requirements for IA awareness training. See IR Policy			
IR-2	Description: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:	IR-2.5	002779	The organization provides incident response training to information system users consistent with assigned	The organization being inspected/assessed documents and implements a process to provide incident response	The organization conducting the inspection/assessment obtains and examines the documented process as well as training records for a sampling of	Compliant	06-Nov-2019	Derek Miller	The organization provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. Training is compliant with DoDD 8570.01 requirements for IA awareness training. See IR Policy			
IR-4(4)	Description: The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	IR-4(4).1	000829	The organization correlates incident information and individual incident responses to achieve an organization-	The organization being inspected/assessed defines procedures to examine incident information gathered and the	The organization conducting the inspection/assessment obtains and examines proof of the analysis (such as minutes from an incident response after	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(6)	Description: The organization implements incident handling capability for insider threats.	IR-4(6).1	002782	The organization implements incident handling capability for insider threats.	The organization being inspected/assessed documents within their incident response plan and implements plans to	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as a sample of incident after action	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(7)	Description: The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].	IR-4(7).1	002783	The organization coordinates incident handling capability within their incident response plan	The organization being inspected/assessed documents within their incident response plan, the responsibilities of each	The organization conducting the inspection/assessment obtains and examines the incident response plan to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(7)	Description: The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].	IR-4(7).2	002784	The organization defines components or elements of the organization in which incident handling capability	The organization being inspected/assessed defines and documents components or elements of the organization in	The organization conducting the inspection/assessment obtains and examines the documented components or elements to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(8)	Description: The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to	IR-4(8).1	002785	The organization coordinates with organization-defined external organizations to correlate and share	The organization being inspected/assessed coordinates with external organizations as defined in IR-4 (8). CCI 2786 to	The organization conducting the inspection/assessment obtains and examines reports, meeting minutes, or other evidence that the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(8)	Description: The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to	IR-4(8).2	002786	The organization defines external organizations to correlate and share organization-defined incident	The organization being inspected/assessed defines and documents external organizations with whom they	The organization conducting the inspection/assessment obtains and examines the documented external organizations to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-4(8)	Description: The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to	IR-4(8).3	002787	The organization defines incident information to correlate and share with organization-defined external	The organization being inspected/assessed defines and documents what incident information will be correlated	The organization conducting the inspection/assessment obtains and examines the documented incident information to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-6(2)	Description: The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].	IR-6(2).1	000838	The organization reports information system vulnerabilities associated with reported security	The organization being inspected/assessed documents and implements a process to report to personnel defined in IR	The organization conducting the inspection/assessment obtains and examines a sample of previous security incidents to ensure the associated	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Reporting shall be conducted IAW CJCSM 6510.01B as defined in Component level policy.			
IR-6(2)	Description: The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].	IR-6(2).2	002792	The organization defines personnel or roles to whom information system vulnerabilities associated	The organization being inspected/assessed defines and documents personnel or roles to whom information system	The organization conducting the inspection/assessment obtains and examines the documented personnel to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-7(2)	Description: The organization (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of	IR-7(2).1	000841	The organization establishes a direct, cooperative relationship between its incident response capability	The organization being inspected/assessed must establish a formal agreement with a computer network	The organization conducting the inspection/assessment obtains and examines the formal agreement document between the organization and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-7(2)	Description: The organization (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of	IR-7(2).2	000842	The organization identifies organizational incident response team members to the external providers	The organization being inspected/assessed must provide and update the list of internal incident response team	The organization conducting the inspection/assessment obtains and examines the list of internal incident response team members to validate it is	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.1	002805	The organization responds to information spills by identifying the specific information involved in the	The organization being inspected/assessed documents within their incident response plan, a process to identify the	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.2	002806	The organization responds to information spills by alerting organization-defined personnel or roles of the	The organization being inspected/assessed documents within their incident response plan, a process to alert at a	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.4	002808	The organization responds to information spills by isolating the contaminated information system or	The organization being inspected/assessed documents within their incident response plan, a process to isolate the	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.5	002809	The organization responds to information spills by eradicating the information from the contaminated	The organization being inspected/assessed documents within their incident response plan, a process to eradicate the	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.6	002810	The organization responds to information spills by identifying other information systems or system	The organization being inspected/assessed documents within their incident response plan, a process to identify other	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.7	002811	The organization responds to information spills by performing other organization-defined actions,	The organization being inspected/assessed documents within their incident response plan, processes to perform	The organization conducting the inspection/assessment obtains and examines the incident response plan as well as after action reports of incidents to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9	Description: The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination;	IR-9.8	002812	The organization defines other actions required to respond to information spills;	The organization being inspected/assessed defines and documents additional actions to be taken in	The organization conducting the inspection/assessment obtains and examines the documented additional actions to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9(1)	Description: The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.	IR-9(1).1	002813	The organization assigns organization-defined personnel or roles with responsibility for responding	The organization being inspected/assessed appoints personnel or roles defined in IR-9 (1). CCI 2815 as having the	The organization conducting the inspection/assessment obtains and examines appointment letters to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9(1)	Description: The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.	IR-9(1).2	002815	The organization defines personnel or roles to whom responsibility for responding to information spills will be	The organization being inspected/assessed defines and documents personnel or roles to whom responsibility for	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

IR-9(2)	Description: The organization provides information spillage response training [Assignment: organization-defined frequency].	IR-9(2).1	002816	The organization provides information spillage response training according to an organization-defined	The organization being inspected/assessed documents and implements a process to provide information spillage	The organization conducting the inspection/assessment obtains and examines the documented process as well as the training records for a sameline	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9(3)	Description: The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out	IR-9(3).1	002818	The organization implements organization-defined procedures to ensure that organizational personnel	The organization being inspected/assessed implements procedures defined in IR-9 (3), CCI 2819 to ensure that	The organization conducting the inspection/assessment obtains and examines the documented procedures defined in IR-9 (3), CCI 2819 as well as							
IR-9(3)	Description: The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out	IR-9(3).2	002819	The organization defines procedures to implement to ensure that organizational personnel impacted by	The organization being inspected/assessed defines and documents procedures to implement to ensure that	The organization conducting the inspection/assessment obtains and examines the documented procedures to ensure the organization being							
IR-9(4)	Description: The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.	IR-9(4).1	002820	The organization employs organization-defined security safeguards for personnel exposed to information not	The organization being inspected/assessed documents and implements a process to employ security safeguards	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-9(4)	Description: The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.	IR-9(4).2	002821	The organization defines security safeguards to employ for personnel exposed to information not	The organization being inspected/assessed defines and documents security safeguards to employ for personnel exposed	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
IR-10	Description: The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	IR-10.1	002822	The organization establishes an integrated team of forensic/malicious code analysts, tool developers	The organization being inspected/assessed establishes an integrated team of forensic/malicious code	The organization conducting the inspection/assessment obtains and examines appointments to the integrated team as well as the documented roles							
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.3	000852	The organization develops and documents a system maintenance policy that addresses purpose, scope	The organization being inspected/assessed develops and documents a system maintenance policy that	The organization conducting the inspection/assessment obtains and examines the documented maintenance policy to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.4	000853	The organization disseminates to organization-defined personnel or roles a system maintenance policy	The organization being inspected/assessed ensures the maintenance policy is disseminated to the SCA, ISSO	The organization conducting the inspection/assessment obtains and examines the maintenance policy via the inspected organization's information	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.5	000855	The organization develops and documents procedures to facilitate the implementation of the	The organization being inspected/assessed documents the maintenance procedures within the Security Plan. The	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure maintenance procedures are documented	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.6	000856	The organization disseminates to organization-defined personnel or roles procedures to facilitate the	The organization being inspected/assessed ensures the maintenance procedures are disseminated to the SCA, ISSO	The organization conducting the inspection/assessment examines the maintenance procedures via the inspected organization's information	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.8	000854	The organization reviews and updates the current system maintenance policy in accordance with	The organization being inspected/assessed reviews the current system maintenance policy every 5 years and revises	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	MA-1.9	000857	The organization reviews and updates the current system maintenance procedures in accordance with	The organization being inspected/assessed reviews the current system maintenance procedures annually and revises	The organization conducting the inspection/assessment obtains and examines documentation of occurrence of reviews and update actions for the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. See Overview Policy document			
MA-2	Description: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in	MA-2.4	002869	The organization reviews records of maintenance on information system components in accordance	The organization being inspected/assessed documents and implements a process to review records of maintenance	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy. All maintenance is reviewed per the RMF Maintenance policy to include manufacturer or vendor specifications and/or organizational requirements. See MA Policy document			
MA-2	Description: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in	MA-2.8	002873	The organization reviews records of repairs on information system components in accordance	The organization being inspected/assessed documents and implements a process to review records of repairs on	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy. All maintenance is reviewed per the RMF Maintenance policy to include manufacturer or vendor specifications and/or organizational requirements. See MA Policy document			
MA-2	Description: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in	MA-2.9	000859	The organization approves and monitors all maintenance activities, whether performed on site	The organization being inspected/assessed approves and monitors all maintenance activities, whether performed on	The organization conducting the inspection/assessment obtains and examines records of all approvals and monitoring activities to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy and records maintenance activities on log sheets. See MA Policy document			
MA-2	Description: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in	MA-2.10	000860	The organization requires that organization-defined personnel or roles explicitly approve the removal of the	The organization being inspected/assessed documents within their risk management strategy personnel or roles	The organization conducting the inspection/assessment obtains and examines: 1. the organization's risk management	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy and records maintenance activities on log sheets. See MA Policy document			
MA-2	Description: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in	MA-2.12	000861	The organization sanitizes equipment to remove all information from associated media prior to removal from	The organization being inspected/assessed sanitizes equipment to remove all information from associated	The organization conducting the inspection/assessment obtains and examines written records of media sanitization to ensure the organization	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy and records media sanitation activities on log sheets. See MA Policy document			
MA-3	Description: The organization approves, controls, and monitors information system maintenance tools.	MA-3.2	000866	The organization controls information system maintenance tools.	The organization being inspected/assessed controls information system maintenance tools that are	The organization conducting the inspection/assessment: 1. obtains and examines the Security Plan to identify the list of approved	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-3	Description: The organization approves, controls, and monitors information system maintenance tools.	MA-3.3	000867	The organization monitors information system maintenance tools.	The organization being inspected/assessed develops and implements procedures to monitor the use of the approved	The organization conducting the inspection/assessment obtains and examines: 1. the Security Plan to identify the list of	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-3(3)	Description: The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:	MA-3(3).1	000871	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:	The organization being inspected/assessed documents and implements a process to take one of the followine actions	The organization conducting the inspection/assessment obtains and examines the documented process and record of maintenance equipment	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-3(3)	Description: The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:	MA-3(3).2	002882	The organization defines the personnel or roles who can provide an exemption that explicitly authorizes removal	The organization being inspected/assessed defines and documents the personnel or roles who can provide an	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(1)	Description: The organization: (a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]: and	MA-4(1).1	002884	The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit	The organization being inspected/assessed configures the information system to audit nonlocal maintenance and	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
MA-4(1)	Description: The organization: (a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]: and	MA-4(1).2	002885	The organization defines the nonlocal maintenance and diagnostic session audit events to audit	The organization being inspected/assessed defines and documents the nonlocal maintenance and diagnostic	The organization conducting the inspection/assessment obtains and examines the documented audit events to ensure the organization being							
MA-4(1)	Description: The organization: (a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]: and	MA-4(1).3	002886	The organization reviews the records of the nonlocal maintenance and diagnostic sessions.	The organization being inspected/assessed documents and implements a process to review the records of the	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure							
MA-4(3)	Description: The organization (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a	MA-4(3).1	000882	The organization requires that nonlocal maintenance and diagnostic services to be performed from an	The organization being inspected/assessed clearly defines in its contracts and/or service level agreements the	The organization conducting the inspection/assessment obtains and examines contracts and/or service level agreements for all non-local maintenance	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(3)	Description: The organization (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a	MA-4(3).2	000883	The organization removes the component to be serviced from the information system and prior	The organization being inspected/assessed removes the component to be serviced from the information system and	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(3)	Description: The organization (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a	MA-4(3).3	001631	The organization, before removal from organizational facilities, and after the service is performed, inspects	The organization being inspected/assessed sanitizes and inspects serviced components prior to reusing	The organization conducting the inspection/assessment obtains and examines maintenance procedures for all non-local maintenance and diagnostic	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(6)	Description: The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.	MA-4(6).1	002890	The information system implements cryptographic mechanisms to protect the integrity of nonlocal	The organization being inspected/assessed configures the information system to implement cryptographic	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(6)	Description: The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.	MA-4(6).2	001123	The information system implements cryptographic mechanisms to protect the confidentiality of nonlocal	The organization being inspected/assessed configures the information system to implement cryptographic	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-4(7)	Description: The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	MA-4(7).1	002891	The information system implements remote disconnect verification at the termination of nonlocal	The organization being inspected/assessed configures the information system to implement remote disconnect	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
MA-5	Description: The organization a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance	MA-5.1	000890	The organization establishes a process for maintenance personnel authorization.	The organization being inspected/assessed clearly defines, documents, and establishes a process for the	The organization conducting the inspection/assessment obtains and examines procedures addressing maintenance personnel to ensure that	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Maintenance policy to record and track maintenance personnel on log sheets. See MA Policy document			
MP-2	Description: The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	MP-2.1	001003	The organization restricts access to organization-defined types of digital and/or non-digital media to	The organization being inspected/assessed restricts access to all types of digital and/or non-digital media	The organization conducting the inspection/assessment interviews organizational personnel with information system media protection	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media, as defined in DoD regulations, and has developed and documented a Media Protection policy. See MP Policy document			
MP-2	Description: The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	MP-2.3	001005	The organization defines personnel or roles to restrict access to organization-defined types of digital	The organization being inspected/assessed will define and document personnel or roles to restrict access to media	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to restrict access to media to ensure	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media, as defined in DoD regulations, and has developed and documented a Media Protection policy. See MP Policy document			
MP-3	Description: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings	MP-3.1	001010	The organization marks information system media indicating the distribution limitations, handling caveats	The organization being inspected/assessed marks information system media and information system output IAW	The organization conducting the inspection/assessment obtains a sampling of information system media and information system output to verify							
MP-3	Description: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings	MP-3.2	001011	The organization exempts organization-defined types of information system media from marking as lone as the	All information system media must be marked in all areas IAW DoDM 5200.01 Vol. 1-4.	The organization conducting the inspection/assessment examines information system media to ensure it is marked IAW DoDM 5200.01 Vol. 1-4.							
MP-4	Description: The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media]	MP-4.4	001018	The organization protects information system media until the media are destroyed or sanitized using	The organization being inspected/assessed protects information system media IAW DoDM 5200.01 M Vol. 1-4.	The organization conducting the inspection/assessment obtains and examines the list of media and verifies it is being stored and protected IAW DoDM							
MP-5	Description: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of	MP-5.1	001020	The organization protects and controls organization-defined types of information system media during	The organization being inspected/assessed protects and controls information system media during transport outside	The organization conducting the inspection/assessment obtains and examines the organization's records management policy or process to ensure							
MP-5	Description: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of	MP-5.4	001023	The organization maintains accountability for information system media during transport outside of	The organization being inspected/assessed ensures the organization defined security measures IMP-2 includes	The organization conducting the inspection/assessment obtains and examines the list of organization defined security measures IMP-2 to ensure							
MP-5	Description: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of	MP-5.5	001025	The organization documents activities associated with the transport of information system media.	The organization being inspected/assessed documents activities associated with the transport of information system	The organization conducting the inspection/assessment obtains and examines the documented activities to ensure the organization being							
MP-5	Description: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of	MP-5.6	001024	The organization restricts the activities associated with the transport of information system media to authorized	The organization being inspected/assessed ensures the organization defined security measures IMP-2 includes a	The organization conducting the inspection/assessment obtains and examines the list of personnel authorized to transport information system media							
MP-5(4)	Description: The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled	MP-5(4).1	001027	The information system implements cryptographic mechanisms to protect the confidentiality and integrity	The organization being inspected/assessed shall document within their Security Plan, and implement, FIPS 140-2	The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure the organization being inspected has							
MP-6	Description: The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational	MP-6.1	001028	The organization sanitizes organization-defined information system media prior to disposal, release out	The organization being inspected/assessed sanitizes all media prior to disposal, release out of organizational control, or	The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, any other relevant	Compliant	06-Nov-2019	Derek Miller	The organization sanitizes media, as defined in DoD regulations, and records media sanitation activities. See MP Policy document			
MP-6	Description: The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational	MP-6.4	002580	The organization employs sanitization mechanisms with the strength and integrity commensurate with	The organization being inspected/assessed implements sanitization mechanisms with the strength and integrity	The organization conducting the inspection/assessment obtains and examines the audit trail of sanitization actions to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization sanitizes media, as defined in DoD regulations, and records media sanitation activities. See MP Policy document			
MP-7	Description: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information	MP-7.1	002581	The organization defines the types of information system media to restrict or prohibit on organization-defined	The organization being inspected/assessed defines and documents the types of information system media to	The organization conducting the inspection/assessment obtains and examines the documented type of information system media to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media and has developed and documented a Media Protection policy. See MP Policy document			
MP-7	Description: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information	MP-7.2	002582	The organization defines the information systems or system components to restrict or prohibit the use of	The organization being inspected/assessed defines and documents the information systems or system components	The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media and has developed and documented a Media Protection policy. See MP Policy document			
MP-7	Description: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information	MP-7.3	002583	The organization defines the security safeguards to use for restricting or prohibiting the use of organization-defined	The organization being inspected/assessed defines and documents the security safeguards to use for restricting	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media and has developed and documented a Media Protection policy. See MP Policy document			
MP-7	Description: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information	MP-7.4	002584	The organization restricts or prohibits the use of organization-defined types of information system media	The organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7. CCI	The organization conducting the inspection/assessment obtains and examines the documented controls and examines information system procedures	Compliant	06-Nov-2019	Derek Miller	The organization restricts access to media and has developed and documented a Media Protection policy. See MP Policy document			
MP-7(1)	Description: The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	MP-7(1).1	002585	The organization prohibits the use of portable storage devices in organization information systems when	The organization being inspected/assessed does not use portable storage devices in organization information	The organization conducting the inspection/assessment examines a sampling of portable storage devices used in the information system to ensure that	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PE-3	Description: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the	PE-3.11	002922	The organization defines circumstances requiring visitor escorts.	The organization being inspected/assessed defines and documents circumstances requiring visitor escorts. DoD	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Physical and Environmental Protection policy for securing physical access. See PE Policy document			
PE-3	Description: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the	PE-3.13	002924	The organization defines circumstances requiring visitor monitoring.	The organization being inspected/assessed defines and documents circumstances requiring visitor monitorine.	The organization conducting the inspection/assessment obtains and examines the documented circumstances to ensure the organization beine	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Physical and Environmental Protection policy for securing physical access. See PE Policy document			
PE-3(1)	Description: The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical	PE-3(1).1	000928	The organization enforces physical access authorizations to the information system in	The organization being inspected/assessed will provide documentation of additional physical access authorizations	The organization conducting the inspection/assessment obtains and examines the documented list of additional physical access authorizations	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

PE-3(1)	Description: The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical	PE-3(1).2	002926	The organization defines the physical spaces containing one or more components of the information system that	The organization being inspected/assessed defines and documents the physical spaces containing one or more	The organization conducting the inspection/assessment obtains and examines the documented physical spaces to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PE-11	Description: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the	PE-11.1	002955	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the	The organization being inspected/assessed implements an uninterruptible power supply with sufficient capacity to	The organization conducting the inspection/assessment obtains and examines documentation identifying the capacity of the implemented	Not Applicable	06-Nov-2019	Derek Miller	Other; Applicable only to CS that support critical activities (Source: UFC 4-010-06)			
PE-12	Description: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency	PE-12.1	000963	The organization employs and maintains automatic emergency lighting for the information system that	The organization being inspected/assessed must install and maintain automatic emergency lighting for the	The organization conducting the inspection/assessment conducts visual inspections and interviews physical security personnel to validate the	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not need lighting [Enclave] (Source: UFC 4-010-06)			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.1	003049	The organization develops a security plan for the information system.	The organization being inspected/assessed develops and documents a security plan for the information system	The organization conducting the inspection/assessment obtains and examines the documented security plan to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed a System Security Plan. See eMASS record for this system			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.2	003050	The organization's security plan for the information system is consistent with the organization's enterprise	The organization being inspected/assessed defines a security plan for the information system which is consistent with	The organization conducting the inspection/assessment obtains and examines the security plan and the enterprise architecture to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.4	003052	The organization's security plan for the information system describes the operational context of the	The organization being inspected/assessed describes within the security plan the operational context of the	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The approved SSP provides operational context of the control system by describing the system and components, mission, operational and geographic environment, and other attributes as required. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.6	003054	The organization's security plan for the information system describes the operational environment for	The organization being inspected/assessed describes within the security plan the operational environment for the	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.7	003055	The organization's security plan for the information system provides an overview of the security requirements	The organization being inspected/assessed documents within the security plan, an overview of the security	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The approved SSP provides an overview of the security requirements for the system. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.8	003056	The organization's security plan for the information system identifies any relevant overlays, if	The organization being inspected/assessed identifies within the security plan any relevant overlays, if applicable.	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The approved SSP identifies all relevant overlays as applicable. See eMASS record for this system			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.9	003057	The organization's security plan for the information system describes the security controls in place or planned	The organization being inspected/assessed describes within the security plan the security controls in place or	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The approved SSP describes security controls in place or planned for meeting security requirements including rationale for tailoring decisions. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.10	000571	The organization's security plan for the information system is reviewed and approved by the authorizing	The organization being inspected/assessed obtains security plan approval by the authorizing official or designated	The organization conducting the inspection/assessment obtains and examines the security plan approval to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.11	003059	The organization distributes copies of the security plan to [Assignment: organization-defined personnel or roles	The organization being inspected/assessed distributes copies of the security plan to, at a minimum, the ISSO, ISSM and	The organization conducting the inspection/assessment obtains and examines the security plan via the organization's information sharing portal	Compliant	06-Nov-2019	Derek Miller	The System Security Plan (SSP) has been reviewed by stakeholders identified in the SSP, inclusive of the ISSM and SCA. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.13	003061	The organization communicates subsequent changes to the security plan to [Assignment: organization-defined	The organization being inspected/assessed distributes changes to the security plan to, at a minimum, the ISSO, ISSM	The organization conducting the inspection/assessment examines the organization's information sharing portal to ensure at a minimum, the ISSO, ISSM	Compliant	06-Nov-2019	Derek Miller	The System Security Plan (SSP) is managed in eMASS. All changes to the SSP have been communicated to stakeholders identified in the SSP. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.16	000573	The organization reviews the security plan for the information system in accordance with	The information system owner as part of the annual security control review will also review the security plan annually	The organization conducting the inspection/assessment obtains and examines the audit records of security plan reviews to verify the security plan	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.17	000574	The organization updates the plan to address changes to the information system/environment of	The information system owner will update the security plan as necessary to address changes to information	The organization conducting the inspection/assessment obtains and examines the audit records of security plan updates to verify the security plan is	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.18	003063	The organization protects the security plan from unauthorized disclosure.	The organization being inspected/assessed documents and implements a process to protect the security plan from	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2	Description: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture	PL-2.19	003064	The organization protects the security plan from unauthorized modification.	The organization being inspected/assessed documents and implements a process to protect the security plan from	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2(3)	Description: The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting	PL-2(3).1	003065	The organization plans and coordinates security-related activities affecting the information system with	The organization being inspected/assessed defines and documents within the security plan, the planning and	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-2(3)	Description: The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting	PL-2(3).2	003067	The organization defines the individuals or groups with whom security-related activities are planned and	The organization being inspected/assessed defines and documents the individuals or groups with whom security-	The organization conducting the inspection/assessment obtains and examines the documented individuals or groups to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy and obtains System Security Plan approval. See eMASS record for this system and PL Policy document			
PL-4	Description: The organization: a. Establishes and makes readily available to individuals requiring access to the information system. the rules that	PL-4.1	000592	The organization establishes the rules describing the responsibilities and expected behavior, with reward to	The organization being inspected/assessed must develop and document rules that describe information	The organization conducting the inspection/assessment obtains and examines the organization's AUP to ensure the orgnaization has clearly	Compliant	06-Nov-2019	Derek Miller	The organization has developed an Acceptable Use Policy. See AUP			
PL-4	Description: The organization: a. Establishes and makes readily available to individuals requiring access to the information system. the rules that	PL-4.2	001639	The organization makes readily available to individuals requiring access to the information system	The organization being inspected/assessed must disseminate to all information system users. via an information	The organization conducting the inspection/assessment obtains and examines rules that describe information system user responsibilities via the	Compliant	06-Nov-2019	Derek Miller	The organization has developed an Acceptable Use Policy. See AUP			
PL-4	Description: The organization: a. Establishes and makes readily available to individuals requiring access to the information system. the rules that	PL-4.3	000593	The organization receives a signed acknowledgment from individuals requiring access the system.	The organization being inspected/assessed will obtain signed acknowledgment (paper or electronic signature) from	The organization conducting the inspection/assessment obtains a list of individuals with active accounts and validates the existence of signed	Compliant	06-Nov-2019	Derek Miller	The organization has developed an Acceptable Use Policy. See AUP			
PL-4	Description: The organization: a. Establishes and makes readily available to individuals requiring access to the information system. the rules that	PL-4.4	003068	The organization reviews and updates the rules of behavior in accordance with organization-defined	The organization being inspected/assessed reviews and updates the rules of behavior annually. The organization must	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Planning policy. See PL Policy document			
PL-4	Description: The organization: a. Establishes and makes readily available to individuals requiring access to the information system. the rules that	PL-4.6	003070	The organization requires individuals who have signed a previous version of the rules of behavior to read and	The organization being inspected/assessed documents and implements a process to require individuals who have	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed an Acceptable Use Policy. See AUP			
PL-4(1)	Description: The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	PL-4(1).1	000594	The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking	The organization being inspected/assessed includes in the rules of behavior, IAW DoDI 8550.01, explicit restrictions on	The organization conducting the inspection/assessment obtains and examines the rules of behavior to ensure the organization being							
PL-4(1)	Description: The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	PL-4(1).2	000595	The organization includes in the rules of behavior, explicit restrictions on posting organizational information	The organization being inspected/assessed includes in the rules of behavior, IAW DoDI 8550.01, explicit restrictions on	The organization conducting the inspection/assessment obtains and examines the rules of behavior to ensure the organization being							
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.1	003072	The organization develops an information security architecture for the information system.	The organization being inspected/assessed develops and documents an information security architecture for the	The organization conducting the inspection/assessment obtains and examines the documented information security architecture to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.2	003073	The organization's information security architecture for the information system describes	The organization being inspected/assessed describes within the information security architecture for the information	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.3	003074	The organization's information security architecture for the information system describes	The organization being inspected/assessed describes within the information security architecture for the information	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.4	003075	The organization's information security architecture for the information system describes	The organization being inspected/assessed describes within the information security architecture for the information	The organization conducting the inspection/assessment obtains and examines the information security architecture to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.5	003076	The organization reviews and updates the information security architecture in accordance with	The organization being inspected/assessed reviews and updates the information security architecture annually to reflect	The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.7	003078	The organization ensures that planned information security architecture changes are reflected in the security	The organization being inspected/assessed includes planned information security architecture changes in the	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.8	003079	The organization ensures that planned information security architecture changes are reflected in the security	The organization being inspected/assessed includes planned information security architecture changes in the	The organization conducting the inspection/assessment obtains and examines security CONOPS to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8	Description: The organization: a. Develops an information security architecture for the information system that:	PL-8.9	003080	The organization ensures that planned information security architecture changes are reflected in	The organization being inspected/assessed includes planned information security architecture changes in	The organization conducting the inspection/assessment obtains and examines a sampling of procurement materials to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).1	003081	The organization designs its security architecture using a defense-in-depth approach that allocates organization-	The organization being inspected/assessed designs and documents its security architecture using a defense-in-	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the orgnaization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).2	003082	The organization designs its security architecture using a defense-in-depth approach that allocates organization-	The organization being inspected/assessed designs and documents its security architecture using a defense-in-	The organization conducting the inspection/assessment obtains and examines the security architecture to ensure the orgnaization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).3	003083	The organization defines the security safeguards to be allocated to organization-defined locations.	The organization being inspected/assessed defines and documents the security safeguards to be allocated to	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the orgnaization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).4	003084	The organization defines the security safeguards to be allocated to organization-defined architectural layers	The organization being inspected/assessed defines and documents the security safeguards to be allocated to	The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the orgnaization	Compliant	13-Nov-2017	DoD Component	This is a DoD Tier 2 common control. Architectural layers to which it allocates security safeguards are identified at Component level			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).5	003085	The organization defines the locations to which it allocates organization-defined security safeguards	The organization being inspected/assessed defines and documents the locations to which it allocates organization-	The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the orgnaization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).6	003086	The organization defines the architectural layers to which it allocates organization-defined security safeguards	The organization being inspected/assessed defines and documents the architectural layers to which it allocates	The organization conducting the inspection/assessment obtains and examines the documented architectural layers to ensure the orgnaization being	Compliant	13-Nov-2017	DoD Component	This is a DoD Tier 2 common control. Architectural layers to which it allocates security safeguards are identified at Component level			
PL-8(1)	Description: The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security	PL-8(1).7	003087	The organization designs its security architecture using a defense-in-depth approach that ensures that the	The organization being inspected/assessed designs and documents its security architecture using a defense-in-	The organization conducting the inspection/assessment obtains and examines security architecture to ensure the orgnaization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PL-8(2)	Description: The organization requires that [Assignment: organization-defined security safeguards] allocated to [Assignment: organization-defined locations and architectural layers] are	PL-8(2).1	003088	The organization requires that organization-defined security safeguards allocated to organization-defined	The organization being inspected/assessed obtains from different suppliers security safeguards defined in PL-8 (1)	The organization conducting the inspection/assessment obtains and examines procurement records to ensure that different suppliers are used to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
PM-4	Description: The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated	PM-4.5	002993	The organization reviews plans of action and milestones for the security program and associated	The organization being inspected/assessed documents and implements a process to review plans of action and	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a process to review plans of action and milestones for the security program. A POAM is generated on eMASS, and RMF roles and responsibilities are assigned. Reviews and updates of the POAM will follow RMF/eMASS processes			
PM-5	Description: The organization develops and maintains an inventory of its information systems.	PM-5.1	000207	The organization develops and maintains an inventory of its information systems.	DITPR is the inventory for all DoD information systems. The organization being	The organization conducting the							
PM-11	Description: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational	PM-11.2	000236	The organization determines information protection needs arising from the defined mission/business processes	The organization being inspected/assessed determines information protection needs IAW CNSSI 1253 and as	The organization conducting the inspection/assessment obtains and examines the security plan to ensure the security categorization has been							
PM-12	Description: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	PM-12.1	002996	The organization implements an insider threat program that includes a cross-discipline insider threat	The organization being inspected/assessed documents and implements an insider threat program that includes a	The organization conducting the inspection/assessment obtains and examines the documented insider threat program to ensure the organization being							
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.1	002998	The organization implements a process for ensuring that organizational plans for conducting security testing	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the orgnaization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document			
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.2	002999	The organization implements a process for ensuring that organizational plans for conducting security testing	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the orgnaization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document			
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.3	003000	The organization implements a process for ensuring that organizational plans for conducting security training	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the orgnaization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document			
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.4	003001	The organization implements a process for ensuring that organizational plans for conducting security training	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the orgnaization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document			
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.5	003002	The organization implements a process for ensuring that organizational plans for conducting security	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the orgnaization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document			

PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.6	003003	The organization implements a process for ensuring that organizational plans for conducting security	The organization being inspected/assessed documents and implements a process for conducting security monitoring	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document				
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.7	003004	The organization implements a process for ensuring that organizational plans for conducting security testing	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document				
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.8	003005	The organization implements a process for ensuring that organizational plans for conducting security training	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process as well as records of execution to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document				
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.9	003006	The organization implements a process for ensuring that organizational plans for conducting security	The organization being inspected/assessed documents and implements a process for ensuring that organizational	The organization conducting the inspection/assessment obtains and examines the documented process as well as the records of execution to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document				
PM-14	Description: The organization reviews testing plans for consistency with the organizational risk management strategy and	PM-14.10	003007	The organization reviews testing plans for consistency with the organizational risk management strategy and	The organization being inspected/assessed documents and implements a process to review testing plans for	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Organizational risk management strategy and organization-wide priorities for risk response actions associated with testing plans are defined at Component level.				
PM-14	Description: The organization reviews training plans for consistency with the organizational risk management strategy and	PM-14.11	003008	The organization reviews training plans for consistency with the organizational risk management strategy and	The organization being inspected/assessed reviews training plans for consistency with the organizational risk	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Program Management policy. See PM Policy document				
PM-14	Description: The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring	PM-14.12	003009	The organization reviews monitoring plans for consistency with the organizational risk	The organization being inspected/assessed reviews monitoring plans for consistency with the organizational risk	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Organizational risk management strategy and organization-wide priorities for risk response actions associated with monitoring plans are defined at Component level.				
PM-15	Description: The organization establishes and institutionalizes contact with selected groups and associations within the security community:	PM-15.1	003010	The organization establishes and institutionalizes contact with selected groups and associations within the	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Coordination with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel is established at the Component				
PM-15	Description: The organization establishes and institutionalizes contact with selected groups and associations within the security community:	PM-15.2	003011	The organization establishes and institutionalizes contact with selected groups and associations within the	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Coordination with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies is established at the				
PM-15	Description: The organization establishes and institutionalizes contact with selected groups and associations within the security community:	PM-15.3	003012	The organization establishes and institutionalizes contact with selected groups and associations within the	The organization being inspected/assessed establishes and institutionalizes contact with selected groups and	The organization conducting the inspection/assessment obtains and examines artifacts showing contact to ensure the organization being	Compliant	01-Oct-2017	DoD Component	This is a DoD Tier 2 assessment procedure that is automatically compliant. Coordination with selected groups and associations within the security community to share current security-related information including threats, vulnerabilities, and incidents is established at the				
PM-16	Description: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	PM-16.1	003013	The organization implements a threat awareness program that includes a cross-organization information-	The organization being inspected/assessed documents and implements a threat awareness program that	The organization conducting the inspection/assessment obtains and examines the documented threat awareness program to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a threat awareness program and users are required to complete DoD threat awareness training. See PM Policy document				
PS-4(1)	Description: The organization (a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of	PS-4(1).1	003027	The organization notifies terminated individuals of applicable, legally binding post-employment	The organization being inspected/assessed notifies terminated individuals of applicable, legally binding post-	The organization conducting the inspection/assessment obtains and examines the record of notifications of post-employment requirements to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
PS-4(1)	Description: The organization (a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of	PS-4(1).2	003028	The organization requires terminated individuals to sign an acknowledgment of post-employment	The organization being inspected/assessed documents within their personnel security procedures the requirement for	The organization conducting the inspection/assessment obtains and examines the personnel security procedures and a sampling of signed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
PS-6(3)	Description: The organization (a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational	PS-6(3).1	003038	The organization notifies individuals of applicable, legally binding post-employment requirements	The organization being inspected/assessed notifies individuals of applicable, legally binding post-employment	The organization conducting the inspection/assessment obtains and examines the records of notifications of post-employment requirements for	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
PS-6(3)	Description: The organization (a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational	PS-6(3).2	003039	The organization requires individuals to sign an acknowledgment of legally binding post-employment	The organization being inspected/assessed documents and implements a process to require individuals to sign an	The organization conducting the inspection/assessment obtains and examines the documented process and a sampling of signed acknowledgements to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-2	Description: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders,	RA-2.2	001046	The organization documents the security categorization results (including supporting rationale) in the security plan	The organization being inspected/assessed documents the security categorization results (including supporting	The organization conducting the inspection/assessment obtains and examines the documented security categorization results to ensure the	Compliant	06-Nov-2019	Derek Miller	The System Security Plan documents procedure for categorizing information. See RA Policy document				
RA-2	Description: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders,	RA-2.3	001047	The organization ensures the security categorization decision is reviewed and approved by the authorizing	The organization being inspected/assessed documents and implements a process IAW CNSSI 1253 to ensure the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The System Security Plan is reviewed and approved by the authorizing official. See RA Policy document				
RA-3	Description: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use,	RA-3.2	001049	The organization documents risk assessment results in the organization-defined document	The organization being inspected/assessed documents risk assessment results in the risk assessment report. DoD has	The organization conducting the inspection/assessment obtains and examines the risk assessment report to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy. The Risk Assessment Report details the risk of compromise for each applicable NIST control. This report will be completed through the initial, and any subsequent, assessments of the				
RA-3	Description: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use,	RA-3.4	001050	The organization reviews risk assessment results on an organization-defined frequency.	The organization being inspected/assessed reviews risk assessment results upon re-accreditation. The organization	The organization conducting the inspection/assessment obtains and examines the record of reviews to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy. The Risk Assessment Report details the risk of compromise for each applicable NIST control. This report will be completed through the initial, and any subsequent, assessments of the				
RA-3	Description: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use,	RA-3.6	002370	The organization disseminates risk assessment results to organization-defined personnel or roles.	The organization being inspected/assessed documents and implements a process to disseminate risk assessment	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy. See RA Policy document				
RA-3	Description: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use,	RA-3.8	001052	The organization updates the risk assessment on an organization-defined frequency or whenever there	The organization being inspected/assessed updates the risk assessment upon re-accreditation or whenever there	The organization conducting the inspection/assessment obtains and examines historical versions of the risk assessment as well as records of changes	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy. Upon notification from the AO, that the system requires reaccreditation, significant changes to the information system environment, or identification of new threats and vulnerabilities, the				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.1	001054	The organization scans for vulnerabilities in the information system and hosted applications on an	The organization being inspected/assessed will define, document, and implement procedures for vulnerability	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results for the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.3	001056	The organization scans for vulnerabilities in the information system and hosted applications when	The organization being inspected/assessed will conduct vulnerability scans of the information system and hosted	The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results in order	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.5	001643	The organization scans for vulnerabilities in the information system and hosted applications in	The organization being inspected/assessed will conduct random vulnerability scans every 30 days or as directed by an	The organization conducting the inspection/assessment obtains and examines the vulnerability scanning results every	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools	RA-5.6	001057	The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools	The organization being inspected/assessed employs the DoD Enterprise scanning tool.	The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.7	001058	The organization analyzes vulnerability scan reports and results from security control assessments.	The organization being inspected/assessed analyzes vulnerability scan reports and security control assessment	The organization conducting the inspection/assessment will interview organizational personnel with security control assessment and vulnerability	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.8	001059	The organization remediates legitimate vulnerabilities in organization-defined response times in	The organization being inspected/assessed takes corrective actions as appropriate on legitimate vulnerabilities	The organization conducting the inspection/assessment obtains and examines audit records to validate the organization is taking action to remediate	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5	Description: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined	RA-5.10	001061	The organization shares information obtained from the vulnerability scanning process and security control	The organization being inspected/assessed documents and implements a process to share information obtained from	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented a RMF Risk Assessment policy for vulnerability scans. See RA Policy document				
RA-5(1)	Description: The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned	RA-5(1).1	001062	The organization employs vulnerability scanning tools that include the capability to readily update the	The organization being inspected/assessed will employ scanning tools that maintain currency with industry standard	The organization conducting the inspection/assessment will: 1. If the inspected organization is using the DoD provided enterprise scanning	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-5(2)	Description: The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when	RA-5(2).1	001063	The organization updates the information system vulnerabilities scanned on an organization-defined	The organization being inspected/assessed will update the list of information system vulnerabilities scanned for prior	The organization conducting the inspection/assessment obtains and examines the record of scans to ensure the latest most up to date scanning	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-5(4)	Description: The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined	RA-5(4).1	001066	The organization determines what information about the information system is discoverable by adversaries	If the organization being inspected/assessed is conducting vulnerability scans for base control RA-5, they are	The organization conducting the inspection/assessment will review results of validation of base control RA-5, if the inspected organization is compliant with	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-5(4)	Description: The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined	RA-5(4).2	002374	The organization defines the corrective actions when information about the information system is	The organization being inspected/assessed defines and documents the corrective actions when information about	The organization conducting the inspection/assessment obtains and examines the documented corrective actions to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-5(4)	Description: The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined	RA-5(4).3	002375	The organization takes organization-defined corrective actions when information about the	The organization being inspected/assessed documents and implements a process to take the corrective actions	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of actions taken to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
RA-5(5)	Description: The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment:	RA-5(5).3	002906	The organization defines the vulnerability scanning activities in which the information system	The organization being inspected/assessed defines and documents the vulnerability scanning activities in which the	The organization conducting the inspection/assessment obtains and examines the documented vulnerability scanning activities to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-4(7)	Description: The organization: (a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products	SA-4(7).1	000634	The organization limits the use of commercially provided information assurance (IA) and IA-enabled	The organization being inspected/assessed, when using commercially provided IA and IA-enabled IT products uses only	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-4(7)	Description: The organization: (a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products	SA-4(7).2	000635	The organization requires, if no NIAP-approved Protection Profile exists for a specific technology type but a	The organization being inspected/assessed, when using commercially provided IA or IA-enabled IT products for which	The organization conducting the inspection/assessment obtains and examines the hardware and software lists to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-9(1)	Description: The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security	SA-9(1).1	003140	The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated	The organization being inspected/assessed documents and implements a process to conduct an organizational	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services and the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-9(1)	Description: The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services	SA-9(1).2	003141	The organization ensures that the acquisition or outsourcing of dedicated information security services	The organization being inspected/assessed ensures that the acquisition or outsourcing of dedicated information security	The organization conducting the inspection/assessment obtains and examines a list of acquired or outsourced information security services as well as	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-10(1)	Description: The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware	SA-10(1).1	000698	The organization requires the developer of the information system, system component, or information system	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-12	Description: The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined	SA-12.2	000723	The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined	The organization being inspected/assessed must identify and document in the Security Plan whether the system is a	The organization conducting the inspection/assessment obtains and examines the Security Plan for the system to determine whether the system is a	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.1	003233	The organization requires the developer of the information system, system component, or information system	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.2	003234	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.3	003235	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.4	003236	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.5	003237	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.6	003238	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.7	003239	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.8	003240	The documented information system, system component, or information system service development process	The organization being inspected/assessed requires within contracts/agreements that the developer of the	The organization conducting the inspection/assessment obtains and examines the contracts/agreements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.9	003241	The organization reviews the development process in accordance with organization-defined	The organization being inspected/assessed documents and implements a process to review the development process	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.10	003242	The organization reviews the development standards in accordance with organization-defined	The organization being inspected/assessed documents and implements a process to review the development	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.11	003243	The organization reviews the development tools in accordance with organization-defined	The organization being inspected/assessed documents and implements a process to review the development tools	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				

SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.12	003244	The organization reviews the development tool options/configurations in accordance with	The organization being inspected/assessed documents and implements a process to review the development tool	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reviews to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15	Description: The organization: a. Requires the developer of the information system, system component, or information system service to follow a	SA-15.14	003246	The organization defines the security requirements that must be satisfied by conducting a review of the	The organization being inspected/assessed defines and documents the security requirements that must be	The organization conducting the inspection/assessment obtains and examines the documented security requirements to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).1	003283	The organization approves the use of live data in the development environments for the information system,	The organization being inspected/assessed documents and implements a process to approve the use of live data in	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).2	003284	The organization approves the use of live data in test environments for the information system, system	The organization being inspected/assessed documents and implements a process to approve the use of live data in	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of approvals to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).3	003285	The organization documents the use of live data in development environments for the information system,	The organization being inspected/assessed documents the use of live data in development environments for	The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).4	003286	The organization documents the use of live data in test environments for the information system, system	The organization being inspected/assessed documents the use of live data in test environments for the	The organization conducting the inspection/assessment obtains and examines the documented use of live data in test environments to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).5	003287	The organization controls the use of live data in development environments for the information system,	The organization being inspected/assessed documents and implements a process to control the use of live data in	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-15(9)	Description: The organization approves, documents, and controls the use of live data in development and test environments for the information system, system component, or information system	SA-15(9).6	003288	The organization controls the use of live data in test environments for the information system, system	The organization being inspected/assessed documents and implements a process to control the use of live data in	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.1	003356	The organization develops anti-counterfeit policy that include the means to detect counterfeit components	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to prevent and prevent	SA-19.2	003357	The organization develops anti-counterfeit policy that include the means to prevent counterfeit components	The organization being inspected/assessed develops and documents an anti-counterfeit policy that include the means to	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit policy to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.3	003358	The organization develops anti-counterfeit procedures that include the means to detect counterfeit	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.4	003359	The organization develops anti-counterfeit procedures that include the means to prevent counterfeit	The organization being inspected/assessed develops and documents anti-counterfeit procedures that include the	The organization conducting the inspection/assessment obtains and examines the documented anti-counterfeit procedures to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.5	003360	The organization implements anti-counterfeit policy that include the means to detect counterfeit components	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3356 that include the means to	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3356 and any artifacts applicable to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.6	003361	The organization implements anti-counterfeit policy that include the means to prevent counterfeit components	The organization being inspected/assessed implements the policy defined in SA-19, CCIs 3357 that include the means to	The organization conducting the inspection/assessment obtains and examines the policy defined in SA-19, CCIs 3357 and any artifacts applicable to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.7	003362	The organization implements anti-counterfeit procedures that include the means to detect counterfeit	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3358 that include the	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3358 and any artifacts applicable	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.8	003363	The organization implements anti-counterfeit procedures that include the means to prevent counterfeit	The organization being inspected/assessed implements the procedures defined in SA-19, CCIs 3359 that include the	The organization conducting the inspection/assessment obtains and examines the procedures defined in SA-19, CCIs 3359 and any artifacts applicable	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SA-19	Description: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent	SA-19.9	003364	The organization reports counterfeit information system components to source of counterfeit	The organization being inspected/assessed documents and implements a process to report counterfeit information	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of reporting to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	SC-1.1	002378	The organization defines the personnel or roles to be recipients of the system and communications protection	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the system and	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. The organization defined the personnel or roles to be recipients of the system and communications protection policy.			
SC-1	Description: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:	SC-1.2	002380	The organization defines the personnel or roles to be recipients of the procedures to facilitate the	The organization being inspected/assessed defines and documents personnel or roles to be recipients of the procedures	The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to ensure the organization being	Compliant	06-Nov-2019	Derek Miller	The organization has developed and documented RMF purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities. The organization defined the personnel or roles to be recipients of the system and communications protection policy.			
SC-5(1)	Description: The information system restricts the ability of individuals to launch [Assignment: organization-defined denial of service attacks] against other information systems.	SC-5(1).1	001094	The information system restricts the ability of individuals to launch [Assignment: organization-defined denial of service attacks] against other information systems.	The organization being inspected/assessed configures the information system to restrict the ability of individuals	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-5(1)	Description: The information system restricts the ability of individuals to launch [Assignment: organization-defined denial of service attacks] against other information systems.	SC-5(1).2	002387	The organization defines the denial of service attacks against other information systems the information	The organization being inspected/assessed defines and documents the denial of service attacks against other	The organization conducting the inspection/assessment obtains and examines the documented denial of service attacks to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-5(2)	Description: The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.	SC-5(2).1	001095	The information system manages excess capacity, bandwidth, or other redundancy to limit the	The organization being inspected/assessed configures the information system to manage excess capacity.	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
SC-5(3)	Description: The organization: (a) Employs [Assignment: organization-defined monitoring tools] to detect indicators of denial of service attacks against	SC-5(3).1	002388	The organization defines a list of monitoring tools to be employed to detect indicators of denial of service	The organization being inspected/assessed defines and documents a list of monitoring tools to be employed to detect	The organization conducting the inspection/assessment obtains and examines the documented monitoring tools to ensure the organization being							
SC-5(3)	Description: The organization: (a) Employs [Assignment: organization-defined monitoring tools] to detect indicators of denial of service attacks against	SC-5(3).2	002389	The organization employs organization-defined list of monitoring tools to detect indicators of denial of service	The organization being inspected/assessed implements the monitoring tools defined in SC-5 (3). CCI 2388 to detect	The organization conducting the inspection/assessment obtains and examines the list of monitoring tools as defined in SC-5 (3). CCI 2388 and a							
SC-5(3)	Description: The organization: (a) Employs [Assignment: organization-defined monitoring tools] to detect indicators of denial of service attacks against	SC-5(3).3	002390	The organization defines the information system resources to be monitored to determine if sufficient	The organization being inspected/assessed defines and documents the information system resources to be	The organization conducting the inspection/assessment obtains and examines the documented information system resources to ensure the							
SC-5(3)	Description: The organization: (a) Employs [Assignment: organization-defined monitoring tools] to detect indicators of denial of service attacks against	SC-5(3).4	002391	The organization monitors organization-defined information system resources to determine if	The organization being inspected/assessed monitors information system resources defined in SC-5 (3). CCI 2390 to	The organization conducting the inspection/assessment obtains and examines the documented monitoring procedures and any available artifacts							
SC-7	Description: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within	SC-7.2	002395	The information system implements subnetworks for publicly accessible system components that are	The organization being inspected/assessed designs the information system to leverage subnetworks so that publicly	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems are not publicly accessible (Source: UFC 4-010-06)			
SC-7(8)	Description: The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated	SC-7(8).1	001112	The information system routes [Assignment: organization-defined internal communications traffic] to organization-	The organization being inspected/assessed configures the information system to route protocols as designated by	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(9)	Description: The information system: (a) Detects and denies outgoing communications traffic posing a threat to external information systems; and	SC-7(9).1	002398	The information system detects outgoing communications traffic posing a threat to external	The organization being inspected/assessed configures the information system to detect outgoing	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(9)	Description: The information system: (a) Detects and denies outgoing communications traffic posing a threat to external information systems; and	SC-7(9).2	002399	The information system denies outgoing communications traffic posing a threat to external	The organization being inspected/assessed configures the information system to deny outgoing communications traffic	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(9)	Description: The information system: (a) Detects and denies outgoing communications traffic posing a threat to external information systems; and	SC-7(9).3	002400	The information system audits the identity of internal users associated with denied outgoing communications	The organization being inspected/assessed configures the information system to audit the identity of internal users	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(10)	Description: The organization prevents the unauthorized exfiltration of information across managed interfaces.	SC-7(10).1	001116	The organization prevents the unauthorized exfiltration of information across managed interfaces	The organization being inspected/assessed documents and implements mechanisms to prevent the unauthorized	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(11)	Description: The information system only allows incoming communications from [Assignment: organization-defined authorized sources] routed to [Assignment: organization-defined authorized	SC-7(11).1	002401	The organization defines the authorized sources from which the information system will allow incoming	The organization being inspected/assessed defines and documents the authorized sources from which the	The organization conducting the inspection/assessment obtains and examines the documented authorized sources to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(11)	Description: The information system only allows incoming communications from [Assignment: organization-defined authorized sources] routed to [Assignment: organization-defined authorized	SC-7(11).2	002402	The organization defines the authorized destinations for routing inbound communications.	The organization being inspected/assessed defines and documents the authorized destinations for routing inbound	The organization conducting the inspection/assessment obtains and examines the documented authorized destinations to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(11)	Description: The information system only allows incoming communications from [Assignment: organization-defined authorized sources] routed to [Assignment: organization-defined authorized	SC-7(11).3	002403	The information system only allows incoming communications from organization-defined	The organization being inspected/assessed configures the information system to allow incoming communications from	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(12)	Description: The organization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined information system	SC-7(12).3	002406	The organization implements organization-defined host-based boundary protection mechanisms at organization-	The organization being inspected/assessed implements McAfee Host Intrusion Prevention (HIPS) on all	The organization conducting the inspection/assessment examines a sampling of information system components to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(13)	Description: The organization isolates [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal information system	SC-7(13).1	001119	The organization isolates organization-defined information security tools, mechanisms, and support	The organization being inspected/assessed designs the information system to isolate key information security tools.	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-7(14)	Description: The organization protects against unauthorized physical connections at [Assignment: organization-defined managed interfaces].	SC-7(14).1	001121	The organization protects against unauthorized physical connections at organization-defined	The organization being inspected/assessed documents and implements mechanisms to protect against unauthorized	The organization conducting the inspection/assessment obtains and examines the documented mechanisms to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-8(2)	Description: The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	SC-8(2).1	002420	The information system maintains the confidentiality and/or integrity of information during	The organization being inspected/assessed configures the information system to maintain the confidentiality and	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
SC-8(2)	Description: The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	SC-8(2).2	002422	The information system maintains the confidentiality and/or integrity of information during	The organization being inspected/assessed configures the information system to maintain the confidentiality and	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed							
SC-13	Description: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws,	SC-13.2	002450	The information system implements organization-defined cryptographic uses and type of cryptography	The organization being inspected/assessed configures the information system to implement, for, protection of	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Applicable only to CS that have classified information (Source: UFC 4-010-06)			
SC-18(1)	Description: The information system identifies [Assignment: organization-defined unacceptable mobile code] and takes [Assignment: organization-defined corrective actions].	SC-18(1).1	001166	The information system identifies organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to identify unacceptable mobile	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(1)	Description: The information system identifies [Assignment: organization-defined unacceptable mobile code] and takes [Assignment: organization-defined corrective actions].	SC-18(1).2	001662	The information system takes organization-defined corrective action when organization-defined	The organization being inspected/assessed configures the information system to take corrective actions defined in SC-	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(1)	Description: The information system identifies [Assignment: organization-defined unacceptable mobile code] and takes [Assignment: organization-defined corrective actions].	SC-18(1).4	002458	The information system defines what constitutes unacceptable mobile code for its information systems.	The organization being inspected/assessed defines and documents unacceptable mobile code IAW the Protection Profile	The organization conducting the inspection/assessment obtains and examines the documented acceptable and unacceptable mobile code and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(2)	Description: The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code	SC-18(2).1	001167	The organization ensures the development of mobile code to be deployed in information systems meets	The organization being inspected/assessed documents and implements a process to develop mobile code IAW the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(2)	Description: The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code	SC-18(2).2	001168	The organization defines requirements for the acquisition, development, and use of mobile code.	The organization being inspected/assessed defines and documents requirements for the acquisition, development, and	The organization conducting the inspection/assessment obtains and examines the documented requirements to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(2)	Description: The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code	SC-18(2).3	001687	The organization ensures the use of mobile code to be deployed in information systems meets organization-	The organization being inspected/assessed documents and implements a process to use mobile code IAW the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(2)	Description: The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets [Assignment: organization-defined mobile code	SC-18(2).4	001688	The organization ensures the acquisition of mobile code to be deployed in information systems meets organization-	The organization being inspected/assessed documents and implements a process to acoure mobile code IAW the	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(3)	Description: The information system prevents the download and execution of [Assignment: organization-defined unacceptable mobile code].	SC-18(3).1	001169	The information system prevents the download of [Assignment: organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the download of	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(3)	Description: The information system prevents the download and execution of [Assignment: organization-defined unacceptable mobile code].	SC-18(3).2	001695	The information system prevents the execution of organization-defined unacceptable mobile code.	The organization being inspected/assessed configures the information system to prevent the execution of	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(3)	Description: The information system prevents the download and execution of [Assignment: organization-defined unacceptable mobile code].	SC-18(3).3	002459	The organization defines the unacceptable mobile code of which the information system is to prevent	The organization being inspected/assessed defines and documents unacceptable mobile code of which the information	The organization conducting the inspection/assessment obtains and examines the documented unacceptable mobile code to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

SC-18(4)	Description: The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforces [Assignment: organization-defined	SC-18(4).1	001170	The information system prevents the automatic execution of mobile code in [Assignment: organization-defined	The organization being inspected/assessed configures the information system to prevent the automatic execution	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-18(4)	Description: The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforces [Assignment: organization-defined	SC-18(4).4	002460	The information system enforces organization-defined actions prior to executing the code.	The organization being inspected/assessed configures the information system to prompt the user prior to	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-19	Description: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the	SC-19.1	001173	The organization establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies based on	The organization being inspected/assessed establishes and documents usage restrictions for Voice over	The organization conducting the inspection/assessment obtains and examines the documented usage restrictions to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-19	Description: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on	SC-19.3	001175	The organization authorizes the use of VoIP within the information system.	The organization being inspected/assessed authorizes any appropriate usage of VoIP within the information system	The organization conducting the inspection/assessment obtains and examines the documented authorizations and "insert language" to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-19	Description: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on	SC-19.4	001176	The organization monitors the use of VoIP within the information system.	The organization being inspected/assessed documents and implements a process to monitor the use of VoIP within	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of monitoring to	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-19	Description: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on	SC-19.5	001177	The organization controls the use of VoIP within the information system.	The organization being inspected/assessed designs the information system to control the use of VoIP within the	The organization conducting the inspection/assessment obtains and examines network topology diagrams, architecture documentation, or any other	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-20	Description: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in	SC-20.1	001178	The information system provides additional data origin authentication artifacts along with the	The organization being inspected/assessed configures the authoritative name server software for external queries to	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (Source: UFC 4-010-06)			
SC-20	Description: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in	SC-20.2	002462	The information system provides additional integrity verification artifacts along with the authoritative name	The organization being inspected/assessed configures the authoritative name server software for external queries to	The organization conducting the inspection/assessment: 1. inspects the configuration files for the presence of DNSSEC records for each A	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (Source: UFC 4-010-06)			
SC-20	Description: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in	SC-20.3	001179	The information system, when operating as part of a distributed, hierarchical namespace, provides the	The organization being inspected/assessed configures the authoritative name server software to enable DNSSEC and	The organization conducting the inspection/assessment inspect the configuration files for the presence of Delegation Signer (DS) Records for any	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (Source: UFC 4-010-06)			
SC-20	Description: The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in	SC-20.4	001663	The information system, when operating as part of a distributed, hierarchical namespace, provides the	The organization being inspected/assessed installs and utilizes software capable of validating the chain of trust	The organization conducting the inspection/assessment utilizes DNSSEC diagnostic tools, such as dig, and performs queries which will exercise the	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (D/E) (Source: UFC 4-010-06)			
SC-22	Description: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	SC-22.1	001182	The information systems that collectively provide name/address resolution service for an organization	The organization being inspected/assessed implements a name service resolution architecture consisting of	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (Source: UFC 4-010-06)			
SC-22	Description: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	SC-22.2	001183	The information systems that collectively provide name/address resolution service for an organization	The organization being inspected/assessed implements a name service resolution architecture where recursive and	The organization conducting the inspection/assessment reviews the sites implementation documentation of the name resolution servers and verifies	Not Applicable	06-Nov-2019	Derek Miller	Not Applicable to FRCS; Control Systems do not act as DNS server for external clients (Source: UFC 4-010-06)			
SC-23(1)	Description: The information system invalidates session identifiers upon user logout or other session termination.	SC-23(1).1	001185	The information system invalidates session identifiers upon user logout or other session termination.	The organization being inspected/assessed configures the information system to invalidate session identifiers	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-23(3)	Description: The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session	SC-23(3).1	001188	The information system generates unique session identifiers for each session with organization-defined	The organization being inspected/assessed configures the information system to generate unique session	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-23(3)	Description: The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session	SC-23(3).2	001189	The organization defines randomness requirements for generating unique session identifiers.	The organization being inspected/assessed defines and documents randomness requirements for generating	The organization conducting the inspection/assessment obtains and examines the documented randomness requirements to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-23(3)	Description: The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session	SC-23(3).3	001664	The information system recognizes only session identifiers that are system-generated.	The organization being inspected/assessed configures the information system to recognize only session identifiers	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-23(5)	Description: The information system only allows the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.	SC-23(5).2	002470	The information system only allows the use of organization-defined certificate authorities for	The organization being inspected/assessed configures the information system to allow the use of DoD PKI established	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-28(1)	Description: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on	SC-28(1).1	002473	The organization defines the information at rest for which cryptographic mechanisms will be implemented.	The organization being inspected/assessed defines and documents the information at rest that is to be protected by	The organization conducting the inspection/assessment obtains and examines the documented information at rest to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-28(1)	Description: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on	SC-28(1).3	002475	The information system implements cryptographic mechanisms to prevent unauthorized modification of	The organization being inspected/assessed configures the information system to implement cryptographic	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-28(1)	Description: The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on	SC-28(1).4	002476	The information system implements cryptographic mechanisms to prevent unauthorized disclosure of	The organization being inspected/assessed configures the information system to implement cryptographic	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-38	Description: The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.	SC-38.1	002528	The organization defines the operations security safeguards to be employed to protect key organizational	The organization being inspected/assessed defines and documents the operations security safeguards to be	The organization conducting the inspection/assessment obtains and examines the documented operations security safeguards to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SC-38	Description: The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.	SC-38.2	002529	The organization employs organization-defined operations security safeguards to protect key	The organization being inspected/assessed implements operations security safeguards defined in SC-38. CCI 2528 to	The organization conducting the inspection/assessment obtains and examines the audit trail of security safeguard implementation to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-2(1)	Description: The organization centrally manages the flaw remediation process.	SI-2(1).1	001231	The organization centrally manages the flaw remediation process.	The organization being inspected/assessed documents and implements a process to centrally manage the flaw	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-2(3)	Description: The organization: (a) Measures the time between flaw identification and flaw remediation; and	SI-2(3).1	001235	The organization measures the time between flaw identification and flaw remediation.	The organization being inspected/assessed documents and implements a process to measure the time between flaw	The organization conducting the inspection/assessment obtains and examines the documented process as well as the audit trail of flaw	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-2(3)	Description: The organization: (a) Measures the time between flaw identification and flaw remediation; and	SI-2(3).3	002608	The organization establishes organization-defined benchmarks for the time taken to apply corrective	The organization being inspected/assessed implements benchmarks for the time taken to apply corrective actions after	The organization conducting the inspection/assessment obtains and examines records of corrective actions taken to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-2(6)	Description: The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed.	SI-2(6).3	002617	The organization removes organization-defined software components (e.g., previous versions) after	The organization being inspected/assessed configures the information system to remove all upgraded/replaced	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-2(6)	Description: The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed.	SI-2(6).4	002618	The organization removes organization-defined firmware components (e.g., previous versions) after	The organization being inspected/assessed configures the information system to remove all upgraded/replaced	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).1	002634	The organization defines the tools to be employed to analyze the characteristics and behavior of malicious	The organization being inspected/assessed defines and documents the tools to be employed to analyze the	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).2	002635	The organization defines the techniques to be employed to analyze the characteristics and behavior of malicious	The organization being inspected/assessed defines and documents the techniques to be employed to analyze the	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).3	002636	The organization employs organization-defined tools to analyze the characteristics and behavior of malicious	The organization being inspected/assessed documents and implements tools defined in SI-3 (10). CCI 2634 to analyze	The organization conducting the inspection/assessment obtains and examines the documented tools to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).4	002638	The organization employs organization-defined techniques to analyze the characteristics and behavior	The organization being inspected/assessed documents and implements techniques defined in SI-3 (10). CCI 2635 to	The organization conducting the inspection/assessment obtains and examines the documented techniques to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).5	002639	The organization incorporates the results from malicious code analysis into organizational incident	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational	The organization conducting the inspection/assessment obtains and examines the organizational incident response processes to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-3(10)	Description: The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of	SI-3(10).6	002640	The organization incorporates the results from malicious code analysis into organizational flaw	The organization being inspected/assessed incorporates the results from malicious code analysis into organizational flaw	The organization conducting the inspection/assessment obtains and examines the flaw remediation processes to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(1)	Description: The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	SI-4(1).1	002655	The organization connects individual intrusion detection tools into an information system-wide intrusion	The organization being inspected/assessed connects individual intrusion detection tools into an information system	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system architecture and	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(1)	Description: The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.	SI-4(1).2	002656	The organization configures individual intrusion detection tools into an information system-wide intrusion	The organization being inspected/assessed configures individual intrusion detection tools into an information system	The organization conducting the inspection/assessment examines the information system-wide intrusion detection system to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(10)	Description: The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information	SI-4(10).1	002665	The organization defines the encrypted communications traffic that are to be visible to organization-defined	The organization being inspected/assessed defines and documents the encrypted communications traffic that are	The organization conducting the inspection/assessment obtains and examines the documented encrypted traffic to ensure the organization being							
SI-4(10)	Description: The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information	SI-4(10).2	002666	The organization defines the information system monitoring tools that will have visibility into	The organization being inspected/assessed defines and documents the information system monitoring tools that	The organization conducting the inspection/assessment obtains and examines the documented information system monitorine tools to ensure the							
SI-4(10)	Description: The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information	SI-4(10).3	002667	The organization makes provisions so that organization-defined encrypted communications	The organization being inspected/assessed makes provisions so that encrypted communications traffic defined	The organization conducting the inspection/assessment examines the information system architecture to verify that the encrypted communications							
SI-4(11)	Description: The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the	SI-4(11).1	001273	The organization analyzes outbound communications traffic at the external boundary of the information	The organization being inspected/assessed documents and implements a process to analyze outbound	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(11)	Description: The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the	SI-4(11).2	001671	The organization analyzes outbound communications traffic at selected organization-defined interior	The organization being inspected/assessed documents and implements a process to analyze outbound	The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of any discovered	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(11)	Description: The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the	SI-4(11).3	002668	The organization defines the interior points within the information system (e.g., subnetworks, subsystems)	The organization being inspected/assessed defines and documents the interior points within the information system	The organization conducting the inspection/assessment obtains and examines the documented interior points to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(12)	Description: The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-	SI-4(12).1	001274	The organization employs automated mechanisms to alert security personnel of an organization-defined	The organization being inspected/assessed documents and implements automated mechanisms to alert security	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(14)	Description: The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information	SI-4(14).1	001673	The organization employs a wireless intrusion detection system to identify rogue wireless devices and to	The organization being inspected/assessed documents and implements a wireless intrusion detection system to	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified wireless intrusion detection	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(15)	Description: The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	SI-4(15).1	001282	The organization employs an intrusion detection system to monitor wireless communications traffic as	The organization being inspected/assessed documents and implements an intrusion detection system to monitor	The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified intrusion detection system	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(16)	Description: The organization correlates information from monitoring tools employed throughout the information system.	SI-4(16).1	001283	The organization correlates information from monitoring tools employed throughout the information system.	The organization being inspected/assessed documents and implements a process to correlate information from	The organization conducting the inspection/assessment obtains and examines the documented process and the correlated results to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(19)	Description: The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified in [Assignment: organization-defined sources] as	SI-4(19).1	002673	The organization defines the additional monitoring to be implemented for individuals who posine an	The organization being inspected/assessed defines and documents the additional monitoring to be implemented	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(19)	Description: The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified in [Assignment: organization-defined sources] as	SI-4(19).2	002674	The organization defines the sources that may be used to identify individuals who pose an increased level of risk.	The organization being inspected/assessed defines and documents the sources that may be used to identify individuals	The organization conducting the inspection/assessment obtains and examines the documented sources to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(19)	Description: The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified in [Assignment: organization-defined sources] as	SI-4(19).3	002675	The organization implements organization-defined additional monitoring of individuals who have been	The organization being inspected/assessed implements additional monitoring defined in SI-4 (19). CCI 2673 of individuals	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitorine to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(20)	Description: The organization implements [Assignment: organization-defined additional monitoring] of privileged users.	SI-4(20).1	002676	The organization defines additional monitoring to be implemented for privileged users.	The organization being inspected/assessed defines and documents additional monitoring to be implemented	The organization conducting the inspection/assessment obtains and examines the documented additional monitoring to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(20)	Description: The organization implements [Assignment: organization-defined additional monitoring] of privileged users.	SI-4(20).2	002677	The organization implements organization-defined additional monitoring of privileged users.	The organization being inspected/assessed implements additional monitoring defined in SI-4 (20). CCI 2676 of privileged	The organization conducting the inspection/assessment obtains and examines the audit trail of additional monitorine to ensure the organization	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			
SI-4(22)	Description: The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection	SI-4(22).3	002683	The information system detects network services that have not been authorized or approved by the organization	The organization being inspected/assessed documents and implements a process to detect network services that	The organization conducting the inspection/assessment obtains and examines the documented process, and examines the implemented detection	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.			

SI-4(22)	Description: The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection	SI-4(22).4	002684	The information system audits and/or alerts organization-defined personnel when	The organization being inspected/assessed configures the information system to audit and/or alert, at a minimum, the	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SI-4(23)	Description: The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].	SI-4(23).3	002687	The organization implements organization-defined host-based monitoring mechanisms at organization-	The organization being inspected/assessed documents and implements HBSS at all components. DoD has defined	The organization conducting the inspection/assessment obtains and examines documentation of the use of HBSS to ensure the organization being	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SI-7(8)	Description: The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more)	SI-7(8).2	002722	The organization defines other actions that can be taken when the information system detects a potential	The organization being inspected/assessed defines and documents other actions that can be taken when the	The organization conducting the inspection/assessment obtains and examines the documented other actions to ensure the organization being								
SI-7(8)	Description: The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more)	SI-7(8).3	002723	The information system, upon detection of a potential integrity violation, provides the capability to audit the	The organization being inspected/assessed configures the information system to provide the capability to audit	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
SI-7(8)	Description: The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more)	SI-7(8).4	002724	The information system, upon detection of a potential integrity violation, initiates one or more of following	The organization being inspected/assessed configures the information system to initiate one or more of following	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
SI-7(14)	Description: The organization: (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision	SI-7(14).1	002737	The organization prohibits the use of binary or machine-executable code from sources with limited or no	The organization being inspected/assessed prohibits the use of binary or machine-executable code obtained from	The organization conducting the inspection/assessment obtains and examines the software list and examines the information system to ensure the	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SI-7(14)	Description: The organization: (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision	SI-7(14).2	002738	The organization provides exceptions to the source code requirement only for compelling	The organization being inspected/assessed documents and provides exceptions to the source code requirement only	The organization conducting the inspection/assessment obtains and examines the documented exceptions to the source code requirement to ensure	Not Applicable	06-Nov-2019	Derek Miller	Controls N/A for manual removal IAW NIST SP 800-82 rev2, Appendix G and Low system categorization.				
SI-8	Description: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited	SI-8.1	002741	The organization employs spam protection mechanisms at information system entry points to detect	The organization being inspected/assessed implements spam protection mechanisms at information system entry points	The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being								
SI-8	Description: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited	SI-8.2	002742	The organization employs spam protection mechanisms at information system exit points to detect	The organization being inspected/assessed implements spam protection mechanisms at information system exit points	The organization conducting the inspection/assessment obtains and examines the hardware/software list to ensure the organization being								
SI-8	Description: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited	SI-8.3	001306	The organization updates spam protection mechanisms when new releases are available in	The organization being inspected/assessed documents and implements a process to update spam protection	The organization conducting the inspection/assessment obtains and examines the documented process and examines the spam protection								
SI-8(1)	Description: The organization centrally manages spam protection mechanisms.	SI-8(1).1	001307	The organization centrally manages spam protection mechanisms.	The organization being inspected/assessed documents and implements a process to centrally manage spam	The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being								
SI-8(2)	Description: The information system automatically updates spam protection mechanisms.	SI-8(2).1	001308	The information system automatically updates spam protection mechanisms .	The organization being inspected/assessed configures the information system to automatically update spam	The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed								
SI-10(3)	Description: The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	SI-10(3).1	002754	The information system behaves in a predictable and documented manner that reflects organizational and	The organization being inspected/assessed documents proper behavior that reflects organizational and system	The organization conducting the inspection/assessment obtains and examines the documented behavior to ensure the organization being								

FRCS STAKEHOLDERS CONTACTED FOR R-SAT FEEDBACK

POC	Company	Outreach	Notes
Bethany S. Hill, CISSP	Spectrum Solutions, Inc.	Video demo:20- June	Tested R-SAT; Project CRN v 2.0; Validation is delayed
Lindsey Hale, Program Manager	FoxGuard Solutions	Video demo:13-Aug	Willing to evaluate the Tool - Foxguard product is more IT based - Tool may have limited capabilities; Cannot commit to providing feedback by 10.30.2019 due to availability. We plan to use this in the future and will pass along feedback as its available.
Roger Rademacher	FoxGuard Solutions	Video demo:13-Aug	Foxguard product is more IT based - Tool may have limited capabilities
Dave Altman	Raytheon Integrated Defense Systems	None	Aug 21 email contact from Mike Chipley; : Tetreault, Timothy; tabletop exercise
John Butler	Raytheon Integrated Defense Systems	Video demo:6-Sep	proposed use: Otis Air National Guard Base (Cape Cod) microgrid/SCADA system; delay in project start
Patrick Troppe	Chinook Systems	Video demo:21-Aug	Feedback provided
Marco Botzong	Chinook Systems	Video demo:21-Aug	
Matthew Steeves	Chinook Systems	Video demo:21-Aug	
Aleksey Primbetov	Chinook Systems	Video demo:21-Aug	
Wanda Lenkewich	Chinook Systems		
Dave Wolfe	Peregrine (GBPTS)	Video demo:21-Aug	
Alex Gordon	Peregrine (GBPTS)	Video demo:21-Aug	Feedback provided
Mike Chipley	PMC Group	Video demo:5-Apr	Attended Stakeholder Review Meeting; Mike has been very helpful in circulating the Tool in the Cyber community and very supportive
Joe Bush	USACE-ERDC-CERL ; E&C Cybersecurity Lead, HQUSACE	Email R-SAT and User Guide	email - contact from Daryl Haegley
Gerado Trevino	Electric Power Research Institute	Email R-SAT and User Guide	Mike Chipley shared Tool following Energy Exchange Conference (Aug 2019)
Robert Schainker	Electric Power Research Institute	Email R-SAT and User Guide	Mike Chipley shared Tool following Energy Exchange Conference (Aug 2019)
Tara Houlden	USN	None Email R-SAT and User Guide	Mike Chipley shared Tool following Energy Exchange Conference (Aug 2019)
Greg Colley	U.S. Army Installation Management Command	Email R-SAT and User Guide	

Appendix E: Policy and Procedures Templates

Risk Management Framework
Access Control (AC)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name]
System Owner (SO)

Date

_____ _____

[Enter ISSO Name]
Information System Security Officer (ISSO)

Date

_____ _____

[Enter ISSM Name]
Information System Security Manager (ISSM)

Date

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Access Control (AC), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline AC Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
AC-1**	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-7*	Unsuccessful Login Attempts
AC-8*	System Use Notification
AC-14*	Permitted Actions Without Identification or Authentication
AC-17	Remote Access [May be Not Applicable]
AC-18	Wireless Access [May be Not Applicable]
AC-19	Access Control for Mobile Devices [May be Not Applicable]
AC-20*	Use of External Information Systems [May be Not Applicable]
AC-21	Information Sharing [May be Not Applicable]
AC-22	Publicly Accessible Content [May be Not Applicable]
Additional Controls for Security Impact Level: MODERATE	
AC-2(1)*	Account Management (Automated System Account Management)
AC-2(2)*	Account Management (Removal of Temporary/Emergency Accounts)
AC-2(3)*	Account Management (Disable Inactive Accounts)
AC-2(4)*	Account management (Automated Audit Actions)
AC-4*	Information Flow Enforcement
AC-5	Separation of Duties
AC-6*	Least Privilege
AC-6 (1)*	Least Privilege (Authorize Access to Security Functions)
AC-6 (2)*	Least Privilege | Non-Privileged Access for Non-Security Functions
AC-6 (5)*	Least Privilege (Privileged Accounts)
AC-6 (9)*	Least Privilege (Auditing Use of Privileged Functions)
AC-6 (10)*	Least Privilege (Prohibit Non- Privileged Users from Executing Privileged Functions)
AC-11*	Session Lock
AC-11 (1)*	Session Lock (Pattern-Hiding Displays)
AC-12*	Session Termination
AC-17 (1)	Remote Access | Automated Monitoring / Control [May be Not Applicable]
AC-17 (2)	Remote Access | Protection of Confidentiality / Integrity Using Encryption [May be Not Applicable]
AC-17 (3)	Remote Access | Managed Access Control Points [May be Not Applicable]
AC-17 (4)	Remote Access | Privileged Commands / Access [May be Not Applicable]
AC-18 (1)	Wireless Access | Authentication and Encryption [May be Not Applicable]
AC-19(5)	Access Control for Mobile Devices |Full Device/Container Based Encryption [May be Not Applicable]

Control Number (NIST)	Control Name
AC-20 (1)*	Use of External Information Systems | Limits on Authorized Use [May be Not Applicable]
AC-20 (2)*	Use of External Information Systems | Portable Storage Devices [May be Not Applicable]

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.
** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 AC Organizational Policy Controls

Broadly implemented AC policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific AC safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Account Management (AC-2)

Account management for the [FACILITY NAME] includes policies and procedures for privileged users, acceptable use and account tracking. [User accounts established must initially be established on the [FACILITY NAME] Sensitive But Unclassified Network]. The policy and procedures referenced in this document are specific to [FACILITY NAME] accounts.

System configurations for [FACILITY NAME] access control will follow Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Readiness Guides (SRGs) to the extent possible. Exceptions will be noted in the checklists and distributed to the ISSO/ISSM, as well as the Authorizing Official or designee.

The ISSO will serve as the designated Account Managers and will approve the creation, modification, or removal of information system accounts **CCI-002112, CCI-000010, CCI-000011**. The ISSM will notify the Account Manager if an account is no longer required, if a user is terminated or transferred, or if system usage or need-to-know changes **CCI-002121, CCI-002123, CCI-002124 and CCI-002125**. The ISSO will be the account managers for the [FACILITY NAME] control system and will ensure that all system users require access to the system for approved job functions **CCI-002113, CCI-002115**. The assigned system accounts shall be reviewed by the ISSM at least annually for compliance with "need-to-know" requirements **CCI-000012.** Account usage is monitored by the ISSM on a monthly basis by reviewing [audit logs] **CCI-002122**.

The ISSO or designee will maintain a list of authorized users on the Master Authorized User List (Master AUL) [Excel file: LogSheets.xls/Master AUL] **CCI-000008**. Only authorized representatives of the [FACILITY NAME] and company representatives with active contracts with these organizations, who have a mission, administrative, or security function on the [FACILITY NAME] control system, will be authorized to access the system. To obtain an account and appropriate credentials, users will be required to complete all cybersecurity awareness training, along with any required training specific to the assigned job function. The Account Manager will verify training records and user's organization and functional roles prior to approving and authorizing access. Group accounts are not allowed **CCI-002116, CCI-002129**.

3. Access Enforcement (AC-3)

The DoD Standard Notice of Consent and Acceptable Use Policy (AUP) for authorized users are included in Appendix A and B. The [FACILITY NAME] will require authorized users to read and sign the DoD Standard Notice of Consent and AUP and the date is recorded on the Master AUL **CCI-000213**. The AUP and PAUP are also referenced in the [FACILITY NAME] Personnel Security Policy and Procedures document.

AC-5 Separation of Duties for Moderate Level systems:

The ISSO implements processes to maintain separation of job duties for individuals that use the system to ensure that all system users require limited access for approved job functions **CCI-000036, CCI-001380, CCI-002219, CCI-002220.**

AC-6(1) Least Privilege – Authorized Access for Moderate Level systems:

The [ISSO and the SO] allow access to authorize access to functions and information that is not publicly available. Authorized users will be tracked on the Master Authorized User List (Excel file:

LogSheets.xls/Master AUL) and the system will be configured to ensure access for these users **CCI-002222, CCI-002223.**

AC-6(2) Least Privilege – Non-privileged Access to non-security functions for Moderate Level systems:

The [ISSO and the SO] will provide two types of accounts to authorized users: privileges and non-privileged. Users must use privileged account to access privileged security functions/information and use non-privileged accounts when accessing non-security functions/information **CCI-000039.**

AC-6(5) Least Privilege – Privileged accounts for Moderate Level systems:

The [ISSO and the SO] will define and document personnel and roles of privileged account users. Privileged account users will be tracked on the Master Authorized User List (Excel file: LogSheets.xls/Master AUL) and the system will be configured to provide the appropriate access for these users **CCI-002226, CCI-002227.**

4. Permitted Actions without Identification or Authentication (AC-14)

No [FACILITY NAME] systems or user actions are allowed or configured without identification or authentication. The security plan documents the rationale for user actions that do not require identification or authentication **CCI-000232.**

5. Remote Access (AC-17)

The [FACILITY NAME] systems [do not] allow remote access and the system has been configured accordingly**.** The following usage restrictions apply to remote access: [define usage restrictions and methods to allow access, if remote access is allowed] **CCI-000063, CCI-000065, CCI-002310, CCI-002311, CCI-002312.**

AC-17(3) Remote Access-Managed Control Points for Moderate Level systems:

The [FACILITY NAME] systems [do not] allow remote access and the system has been configured accordingly**.** The [FACILITY NAME] system has been designed and configured to control and monitor remote access connections by using managed network access control points through which the information system routes all remote access. These access control points are identified on the network diagram and access is controlled: [define access control] **CCI-000069, CCI-001561, CCI-002315.**

AC-17(4) Remote Access-Privileged Commands for Moderate Level systems:

The [FACILITY NAME] systems [do not] allow remote access and the system has been configured accordingly**.** The following usage restrictions apply to ensure remote access is only allowed for [define organizational needs requiring remote access] **CCI-000070, CCI-002316, CCI-002318.** The security plan documents the rational for remote operational needs requiring remote access **CCI-002319, CCI-002320.**

6. Wireless Access (AC-18)

The [FACILITY NAME] systems [do not] allow wireless access and the system has been configured accordingly. The following usage restrictions apply to wireless access: [define usage restrictions and methods to allow access if wireless access is allowed] **CCI-001438, CCI-001439, CCI-001441, CCI-002323.**

7. Access for Mobile Devices (AC-19)

The [FACILITY NAME] systems [do not] allow mobile access and the system has been configured accordingly. The following usage restrictions and connection requirements apply to mobile access: [define usage restrictions and connection requirements to allow access, if mobile access is allowed] **CCI-000082, CCI-000083, CCI-000084, CCI-002326.**

AC-19(5) Mobile Devices -Full Device/Container based encryption for Moderate Level systems:

The [FACILITY NAME] systems [do not] allow mobile access and the system has been configured accordingly. Authorized mobile devices must employ full-device or container encryption. [List make and model of authorized devices] **CCI-002329, CCI-002330, CCI-002331.**

8. Use of External Information Systems (AC-20)

A [Service Level Agreement (SLA)] will be in place for system validation that establishes terms and conditions external connections to [FACILITY NAME] operations. The SLA establishes trust among the organizations, such that any external systems are consistent with the SSP (i.e. scanning or other IA function) **CCI-000093, CCI-002332.**

AC-20(1) External Information Systems- Limits on Use for Moderate Level systems:

The system will be configured to permit authorized individuals external access to the information system only when the [ISSO] verifies the implementation is consistent with the SSP. The [ISSO] must verify that the external access is authorized to process, store, or transmit system information; that proper approvals have been obtained; and the connection is consistent with established SLAs **CCI-002333, CCI-002334, CCI-002335, CCI-002336, CCI-002337.**

AC-20(2) External Information Systems- Portable Storage Devices for Moderate Level systems:

The [ISSO] must verify the use of portable storage devices on the system, prior to allowing access **CCI-000097.**

9. Information Sharing (AC-21)

The [FACILITY NAME] systems [do not] allow information sharing and the system has been configured accordingly. The following restrictions and considerations apply to information sharing: [define usage restrictions, user discretion guidance and automated methods to allow information sharing] **CCI-000098, CCI-001470, CCI-001471, CCI-001472.**

10. Publicly Accessible Content (AC-22)

The [FACILITY NAME] systems [do not] allow publicly accessible content **CCI-001473, CCI-001474, CCI-001475, CCI-001476, CCI-001478.**

Appendix A - DoD Standard Mandatory Notice and Consent

https://www.arnorth.army.mil/resources/documents/AUP.pdf

Appendix B Acceptable Use Policy/Privileged-Level (AUP)

Example - Army AUP: https://www.arnorth.army.mil/resources/documents/AUP.pdf

Risk Management Framework Security Awareness Training (AT) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name]
System Owner (SO)

Date

_____ _____

[Enter ISSO Name]
Information System Security Officer (ISSO)

Date

_____ _____

[Enter ISSM Name]
Information System Security Manager (ISSM)

Date

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Awareness Training (AT), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline AT Security Controls

Control Number (NIST)	Control Name
Controls for Impact Level: LOW	
AT-1**	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness Training– All aspects of control addressed by DoD Level Policy
AT-3	Role-Based Security Training
AT-4	Security Training Records
Additional Controls for Security Impact Level: MODERATE	
AT-2(2)	Security Awareness | Insider Threat– All aspects of control addressed by DoD Level Policy

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 AT Organizational Policy Controls

Broadly implemented AT policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview* document. The text in the following sections address details regarding the implementation of specific AT safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Role Based Security Training (AT-3)

User account credentials shall be established and administered in accordance with a role-based access. [ORGANIZATION NAME] provides role-based security training to personnel with assigned security roles and responsibilities for each system. The assignment and account management of these roles is described in the system specific [FACILITY NAME] Access Control Policy. Privileged users must take the DoD Cyber Awareness Challenge Training annually or if changes to the system require refresher training. Logging in using a DoD Common Access Card (CAC) and selecting the email certificate will automatically record the course completion in [Training Record Tracking System] **CCI-000109, CCI-000110**.

3. Training Records (AT-4)

All completed security certifications and training shall be uploaded to [Training Record Tracking System]. This will apply to anyone filling the System Administrator role for the [FACILITY NAME] system. All [FACILITY NAME] system users have training (including initial IA Awareness and their specific training for privileged users) tracked in [Training Record Tracking System]. The [FACILITY NAME] ISSM or designee will review the [Training Record Tracking System] profiles of all [FACILITY NAME] administrators to ensure that basic security awareness training and specific information system training is up to date. These training records will be retained on [Training Record Tracking System] **CCI-000113, CCI-000114, CCI-001336.**

Risk Management Framework
Audit & Accountability (AU) Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Audit and Accountability Control (AU), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline AU Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
AU-1**	Audit and Accountability Policy and Procedures
AU-2*	Audit Events
AU-3*	Content of Audit Records
AU-4*	Audit Storage Capacity
AU-4 (1)*	Audit Storage Capacity (Transfer to Alternate Storage)
AU-5*	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting
AU-8*	Time Stamps
AU-9*	Protection of Audit Information
AU-11	Audit Record Retention
AU-12*	Audit Generation
Additional Controls for Security Impact Level: MODERATE	
AU-2 (3)	Audit Events (Reviews and Updates)
AU-3 (1)*	Content of Audit Records (Additional Audit Information)
AU-6 (1)	Audit Review, Analysis, and Reporting (Process Integration)
AU-6 (3)	Audit Review, Analysis, and Reporting (Correlate Audit Repositories)
AU-7*	Audit Reduction and Report Generation
AU-7(1)*	Audit Reduction and Report Generation (Automatic Processing)
AU-8(1)*	Time Stamps (Synchronization with Authoritative Time Source)
AU-9 (4)	Protection of Audit Information (Access by Subset of Privileged Users)

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to

policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 AU Organizational Policy Controls

Broadly implemented AU policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific AU safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Audit Events (AU-2)

The Department of Defense (DoD) has created the list of auditable events which are incorporated into the Operating System (OS) Security Technical Implementation Guides (STIGs) **CCI-000126**. Each system must be capable of auditing the required DoD events **CCI-000123**. A list of auditable events which will be logged per occurrence is listed [list of auditable events]:

These required audit events provide comprehensive information to investigate incidents and effectively determine root cause. Any incidents occurring on a system will trigger a review of the audit logs to effectively determine the best course of action to mitigate against the same threat in the future **CCI-000125**. The System Administrator (SA) will report event findings to the ISSM or ISSO **CCI-000124**.

AU-2 (3) Audit Events Reviews and Updates for Moderate Impact level systems:

The [ISSM or ISSO] will conduct reviews of the list of auditable events annually or more frequently upon changes to situational awareness of threats or vulnerabilities [define] **CCI-000127**. The latest Operating System STIGs will be included in the review process.

3. Content of Audit Records (AU-3)

System audit logs are [configured to comply with applicable STIG/Security Requirements Guide (SRG) guidance, including having enough detail to reconstruct the vulnerability or intrusion event, which is required during a forensics investigation]. The logs provide sufficient information for the incident response team to establish what type of event occurred along with the outcome of the event **CCI-000130, CCI-000131**, **CCI-000132, CCI-000133,CCI-001487, CCI-000134.**

AU-3 (1) Content of Audit Record Additional Information for Moderate Impact level systems:

[ORGANIZATION NAME] defines the additional information to be included in audit records in compliance with the STIG/SRG guidance and ensure this level of detail is provided in the audit record **CCI-000135.** [The additional information must be defined and includes full-text recording of privileged commands or the individual identities of group account users] **CCI-001488**.

4. Audit Storage (AU-4) and Transfer to Alternative Storage (AU-4(1))

The DoD has determined the audit record storage requirements are not appropriate to define at the Enterprise level. [The SO allocates sufficient capacity to store copied audit records to comply with applicable STIGs/SRG guidance **CCI-001848, CCI-001849].** The off-load of records and review of the logs will be done at a minimum, in real-time for interconnected systems and weekly for [FACILITY NAME] systems that are stand-alone **CCI-001851.** These logs will be stored and protected from destruction for a minimum of one year. Audit logs are subject to the [FACILITY NAME] *Media Protection Policy and*

Procedures Document. Audit logs must be stored in a location that meet the requirements of the [FACILITY NAME] Access Control and Physical and Environmental Protection Policy and Procedure Documents.

5. Response to Audit Processing Failures (AU-5)

The DoD has determined the audit processing failure requirements are not appropriate to define at the Enterprise level. [ORGANIZATION NAME] utilizes [list audit software] for system auditing. Defined actions taken by each individual system are determined in accordance with SITG/SRG guidance; these actions include [shut down information system, overwrite oldest audit records, stop generating audit records] **CCI-001490**. At a minimum, audit processing failures or exceeding of log size thresholds found during log reviews will be forwarded to ISSM/ISSO immediately **CCI-000139, CCI-001572.** The ISSO will notify the [DoD Cybersecurity Network Defense Team].

6. Audit Review, Analysis and Reporting (AU-6)

The DoD requires at a minimum a weekly review of audit logs; however, inspections may require more frequent review due to events or anomalies **CCI-000148**. The SA or ISSM will review the audit logs weekly and will store the audit records on a removable media and mark the disk with the hostname and a date. Any significant anomalies, or inappropriate/unusual activities, or other findings will be reported immediately to the ISSO/ISSM (Excel file: LogSheets.xls/Audit Log Template) **CCI- 000149, CCI-001863**. Anomalies to be reviewed should include but are not limited to [List audit anomalies to report] **CCI-001862**:

In the event of inappropriate or unusual activity, the ISSOs will notify the [DoD Cybersecurity Network Defense Team]. [List unusual activity to report from audit logs]

AU-6 (1) Audit Review, Analysis, and Reporting Process Integration for Moderate Impact level systems:

Automated mechanisms are implemented to integrate audit review and analysis [define] **CCI-001864 and CCI-001865**.

AU-6 (3) Audit Review, Analysis, and Reporting Correlate Audit Repositories for Moderate Impact level systems:

[ORGANIZATION NAME] implements a process to analyze and correlate audit records across different repositories to gain organization-side situational awareness [define] **CCI-000153**.

7. AU-7 Audit Reduction and Report Generation

All Audit Reduction and Report Generation requirements apply only to Moderate Impact level system.

AU-7 (1) Audit Reduction and Reporting, Automatic Processing, for Moderate Impact level systems:

The [ORGANIZATION NAME] defines and document the audit fields within audit records to be processed for events of interest [define]. Audit reduction capability must support audit review/analysis and reporting (on-demand and/or after-the-fact) for investigations of security incidents. The [FACILITY NAME] system meets this requirement with a signed and dated audit and accountability policy and by configuring the system to provides audit reduction capability in

accordance with STIG/SRG guidance **CCI-001883**.

8. AU-8 Time Stamps

[ORGANIZATION NAME] configures the information system to generate time stamps for audit records that meet one second granularity of time measurement and that contain time zones or time offsets that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). [FACILITY NAME] system meets this requirement with a signed and dated audit and accountability policy and by [configuring the system to generate time stamps for audit records in accordance with STIG/SRG guidance **CCI-001889].**

AU-8(1) Time Stamp for Moderate Impact Level Systems

[ORGANIZATION NAME] configures the information system to generate time stamps for audit records in accordance with STIG/SRG guidance **CCI-001891.**

9. AU-9 Protection of Audit Information

The audit records and audit tools must be protected from unauthorized access, modification or deletions and the system must comply with applicable STIG/SRG guidance. Access authorizations for the management of audit functionality is documented to ensure only privileged users have access **CCI-001495.**

9 (4) Protection of Audit Information Access by Subset of Privileged Users for Moderate Impact level systems:

[ORGANIZATION NAME] defines and document the subset of privileged users to be authorized access to the management and audit functionality [define] **CCI-001351 and CCI-001894**.

10. Audit Record Retention AU-11

[ORGANIZATION NAME] retains audit records for 5 years for System Acquisition Management Inspection; otherwise for at least 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements **CCI-000167**.

11. Audit Generation AU-12

[ORGANIZATION NAME] configures the information system to ensure that only the ISSM or individuals appointed by the ISSM select auditable events, as defined in Section 2, for specific components. [FACILITY NAME] system meets this requirement with a signed and dated audit and accountability policy and by configuring the system to generate audit records in accordance with Section 2 **CCI-000169, CCI-000171.**

Risk Management Framework
Security Assessment and Authorization (CA) Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Version	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique Security Assessments and Authorization (CA), is provided in Table 2 The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Applicable Baseline CA Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
CA-1**	Security Assessment and Authorization Policy and Procedures
CA-2	Security Assessments
CA-3*	Information System Connections
CA-5	Plan of Action and Milestones
CA-7*	Continuous Monitoring
CA-9*	Internal System Connections
Additional Controls for Security Impact Level: MODERATE	
CA-2 (1)*	Security Assessments -Independent Assessors
CA-3 (5)*	System Connections-Restrictions on External System Connections
CA-7(1)*	Continuous Monitoring - Independent Assessment

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 CA Organizational Policy Controls

Broadly implemented CA policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific CA safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Security Assessments (CA-2)

The [FACILITY NAME] SO will disseminate this CA document which will serve as a security assessment, authorization and monitoring policy that is consistent with Department of Defense (DoD) policy and guidance. Security assessments will follow the DoD guidance provided on the Risk Management Framework Knowledge Service (RMF KS) **CCI-000245, CCI-000246**. The Security assessment plan and security control effectiveness will be documented via the Enterprise Mission Assurance Support System (eMASS) implementation of the System Security Plan (SSP) and the Security Assessment Report (SAR) for each system. The SSP is discussed in detail in the [FACILITY NAME] *Planning Policy and Procedures document*. Supporting information on the [FACILITY NAME] assessment environment will be available on eMASS including, but not limited to system-specific **CCI-000248**:

- Network Diagram
- Data Flow Diagram
- Hardware and Software List
- Ports, Protocols, and Services (PPS) List

[FACILITY NAME] system stakeholders are required to adhere to the security controls listed on the system's SSP. The SO or SO designated representative (SO DR) will complete the self-assessment and Implementation Plan in eMASS, as required by DoD policy. The controls will be assessed and marked as validated by an approved third-party Security Control Assessor-Validator (SCA-V), who will generate the SAR **CCI-002070**. The SO or SO DR will generate the final authorization package via eMASS, which includes the SAR, to be reviewed by the ISSM and ISSO prior to submission to the Authorizing Official (AO) for final approval **CCI-000253, CCI-000254.**

DoD has defined the frequency of assessment as annually for technical controls and annually for a portion of management and operational controls, such that all controls are reviewed in a three-year period. Each control family policy defines the frequency of control assessments required for policy (management and operational) and procedure (technical) controls **CCI-000251**.

CA-2 (1) Security Assessments by Independent Assessors for Moderate Impact level systems for Moderate Impact level systems:

Independent assessors or assessment teams will be employed to conduct a security control assessment of the system. The independent assessment team for the **[**FACILITY NAME**]** system will be selected through [organization defined process]. **CCI-000255 and CCI-002063.**

3. Information System Connections (CA-3)

[Applicable to systems with interconnections.] Interconnection Security Agreements will be established prior to any connections to the system are authorized **CCI-000257**. For each system, the agreement will define the interface characteristics, security and privacy requirements, and the nature of the information communicated **CCI-000258 CCI-000259**. The Interconnection Security Agreements shall be reviewed and updated annually **CCI-002083.**

CA-3 (5) System Interconnections – Restrictions on External Connections for Moderate Impact level systems:

The system is configured to employ either an allow-all/deny-by exception or deny-all/permit by exception policy **CCI- 002080 and CCI- 002082.**

4. Plan of Actions and Milestones (CA-5)

During the process of entering a system's self-assessment into eMASS, any security controls marked as Non-Compliant require the SO or ISSO to add an entry to the Plan of Actions and Milestones (POA&M) maintained in the database. The system's SO/ISSO will document the planned remediation to correct weaknesses or deficiencies prior to package submission for security control validation **CCI-000264**. This POA&M will be reviewed and updated by the SO and ISSO every ninety days, at a minimum, to ensure the information in the POA&M is current. Mitigating efforts for vulnerabilities found will be tracked by the SO/ISSO. During the security control validation process, additional vulnerabilities may be found and will need to be included in the POA&M along with planned mitigations. These will also be reviewed by the SO/ISSO every ninety days at minimum **CCI-000266**.

Due to the [FACILITY NAME] operational requirements, it is possible some security controls may be Non-Compliant and cannot be mitigated to meet the full intent of the control. In these cases, the POA&M will fully explain the reasons why the system will not meet full compliance as well as all mitigations and compensating controls planned or currently in place to most reduce the residual risk. These deviations will require the AO's risk acceptance.

5. Continuous Monitoring (CA-7)

Future DoD-wide Continuous Monitoring (CM) guidance is expected to be published. After DoD CM guidance is published, a security and privacy strategy and continuous monitoring program will be developed **CCI-000274**. The future CM program will define and establish a) metrics for monitoring security status, b) frequencies of continuous monitoring, and c) frequencies for assessments supporting continuous monitoring **CCI-002087, CCI-002088, CCI-002089**. Once metrics and frequencies are established, the organization will implement the continuous monitoring program and an analysis of security related information **CCI-000279, CCI-002090, CCI-002091**. The Organizational ISSM will report the security status of the organization and the information system annually to the [SO] **CCI-000280, CCI-000281, CCI-001581**. The future continuous monitoring program includes response actions for the [ISSM] from the analysis of security-related information **CCI-002092**.

CA-7(1) Continuous Monitoring - Periodic Review for Moderate Impact level systems:

[ORGANIZATION NAME] will employ assessors or assessment teams to monitor the security controls in the information system on an ongoing basis. **CCI-000282, CCI-002085**. Future DoD-wide Continuous Monitoring (CM) guidance will be followed.

Risk Management Framework Configuration Management (CM) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name]
System Owner (SO)

Date

_____ _____

[Enter ISSO Name]
Information System Security Officer (ISSO)

Date

_____ _____

[Enter ISSM Name]

Information System Security Manager (ISSM)

Date

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Configuration Management (CM), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Applicable Baseline CM Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
CM-1**	Configuration Management Policy and Procedures
CM-2*	Baseline Configuration
CM-4*	Security Impact Analysis
CM-6*	Configuration Settings
CM-7*	Least Functionality
CM-7(1)*	Least Functionality (Periodic Review)
CM-8*	Information System Component Inventory
CM-10*	Software Usage Restrictions
CM-11	User-Installed Software
Additional Controls for Security Impact Level: MODERATE	
CM-2 (1)*	Baseline Configuration – Reviews and Updates
CM-2 (3)	Baseline Configuration – Retention of Previous Configuration
CM-2 (7)	Configure Systems, Components or Devices for High-Risk Areas - Not Applicable; Control Systems are not mobile.
CM-3*	Configuration Change Control
CM-3(2)*	Configuration Change Control – Test, Validate and Document Changes
CM-5*	Access Restrictions for Change
CM-7(2)*	Least Functionality – Prevent Program Execution
CM-7(5)*	Least Functionality – Authorized software and whitelisting
CM-8(1)	IS Inventory – Updates during Installation and Removal
CM-8(3)	IS Inventory – Automated unauthorized component detection
CM-8(5)*	IS Inventory – No duplicate accounting of components
CM-9	Configuration Management Plan

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 CM Organizational Policy Controls

Broadly implemented CM policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific CM safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Baseline Configuration (CM-2)

To effectively manage configuration changes, a comprehensive baseline of each control system has been established and will be maintained. Baseline configurations serve as a basis for future builds, releases, and/or changes to the system. Baseline configurations include information about system components, network topology, and the logical placement of those components within the system architecture. The ISSM or SA will manually generate the following baselines, diagrams, and lists and present them to the Configuration Control Board (CCB) for formal review and approval **CCI-000293, CCI-000295**:

- Software list (baseline)
- Hardware list (baseline)
- Ports, Protocols, and Services list (baseline)
- System architecture
- Network topology
- Maintenance tool list
- Spare components list

The goal of the CCB is to promote best practices in maintaining high availability, integrity and confidentiality of the [FACILITY NAME] system. Baselines, diagrams, and lists require a formal CCB approval before the system is installed. [Group Policy Objects (GPOs), registry settings, and secure configurations are applied to [FACILITY NAME] devices based on the devices' build and placement].

CM-2(1) Configuration Change Control – reviews and updates - for Moderate Impact level systems:

The ISSM or SA will manually review and update the baseline configuration of [FACILITY NAME] Moderate Impact level systems (Excel file: LogSheets.xls/Configuration Change Log Template). The organization must document each occurrence of the reviews and update actions. The review must occur annually or when **CCI-000296, CCI-000297 CCI-000298, CCI-000299**:

- significant changes are implemented to the system (e.g., system component or installation)
- system components are upgraded
- system components are removed
- as events occur that dictate configuration changes due to United States Cyber Command tactical orders/directives or cyber-attacks

CM-2(3) Configuration Change Control – retention of previous configurations - for Moderate Impact level systems:

The organization retains previous versions of baseline configurations of [FACILITY NAME]. Moderate Impact level systems to support rollback for a minimum of 3 months **CCI-000304**.

CM-2(7) Configuration Change Control – configure devices for high-risk areas:

The organization defines devices that are located in high-risk areas or locations of concern [list devices and location] **CCI- 001737.** Additional configuration for these devices is implemented [list additional configuration considerations] **CCI- 001738.**

[The organization defines and applies security safeguards to devices that are mobile. For example, devices such as notebook computers that may be mobile require additional hardening, limited applications or safeguards to sanitize hard drives prior to removal.] **CCI- 001739, CCI- 001815, CCI-001816**.

3. Configuration Change Control for Moderate Impact level systems (CM-3)

When baseline configurations must be changed for Moderate Impact level systems, the [FACILITY NAME] system ISSM and/or SA determines the type of changes that must be configuration controlled **CCI-000313**. These actions will be formally presented to the CCB with revised documentation (Excel file: LogSheets.xls/Configuration Change Log Template). Any changes to baselines must be documented and a formal review conducted by the CCB, with explicit consideration for security impact analysis **CCI-000314, CCI-000321, CCI-001740**. The CCB will meet [as needed] to approve changes to the baseline configuration **CCI-000319, CCI-000320, CCI-001741**. The organization implements the configuration changes approved by the CCB **CCI-001819**. The organization must maintain an audit trail of approval/disapproval changes for a period of one-year, as defined in the CCB Charter **CCI-000316, CCI-000318**.

CM-3(2) Configuration Change Control – test, validate and document changes - for Moderate Impact level systems

The [FACILITY NAME] system ISSM and/or SA will examine the CCB approved documentation to ensure the changes have been validated before implementing the change **CCI-000328, CCI-000329**. The changes will be tested, in accordance with the CCB approved testing requirements, prior to implementing the changes on the operational system **CCI-000327**. Any configuration control testing is documented on the Configuration Change Log (Excel file: LogSheets.xls/Configuration Change Log Template).

4. Security Impact Analysis (CM-4)

The CCB will ensure that a structured process is used to consider, evaluate, approve, and monitor proposed changes to any [FACILITY NAME] control system. The ISSO, in conjunction with the [FACILITY NAME] Team [e.g., [NEC] and appropriate vendors], will conduct a security impact analysis of each change request IAW Section 3.3.3 of NIST SP 800-128. The process will include assessing risk, assessing the impact on existing security controls, and planning for safeguards and countermeasures in cases of unacceptable risk. Results will be documented as part of each Change Request **CCI-000333**. The CCB

evaluation and determination is documented on the Configuration Change Log (Excel file: LogSheets.xls/Configuration Change Log Template).

5. Access Restrictions for Change for Moderate Impact level systems (CM-5)

The ISSO, in conjunction with the [FACILITY NAME] Team [e.g., [NEC], [FACILITY NAME IMO] and appropriate vendors], will ensure any physical and logical access restrictions to the information system and/or system enclave are defined when configuration changes for Moderate Impact level systems are proposed to the CCB **CCI-000338, CCI-000339, CCI-000342, CCI-000343.** The CCB will approve configuration changes and access restrictions to the information system/system enclave, based on input from [FACILITY NAME IMO] **CCI-000340, CCI-000344**. The ISSO, in conjunction with the [FACILITY NAME] Team [e.g., [NEC], [FACILITY NAME IMO] and appropriate vendors] will ensure of information access restrictions are enforced and documented **CCI-000341, CCI-000345**.

6. Configuration Settings (CM-6)

The [FACILITY NAME] system components will be configured according to the most current Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirement Guides (SRGs), the [FACILITY NAME] System Configuration Guide, and the [FACILITY NAME] System Security Plan **CCI-000363**. These documents provide the security and operational requirements for secure and functional operation of the [FACILITY NAME] system **CCI-001756**.

STIGs applicable to the [FACILITY NAME] system include but are not limited to:

- [Add Applicable STIGs Here]

Deviations from the STIGs or SRGs will only be authorized after review and approval by the SO and ISSO approval based on analysis of risk to the system, cost to implement, and effect on functionality. Deviations from the NIST 800-82 controls are noted in the Security Plan in enterprise Mission Assurance Support Service (eMASS) **CCI-000369**. A Plan of Action and Milestones (POA&M) will be developed as part of the RMF ATO process. Deviations from STIGs or SRGs are noted in the applicable checklist and are uploaded as eMASS artifacts **CCI-000367, CCI-000368**. STIGs will include but are not limited to:

- STIG or SRG name/number;
- Reason for not fully implementing;
- Current risk-mitigating actions/situations taken.

These deviations will be presented annually, or as needed, to the CCB for formal approval **CCI-001503**. The ISSM or SA will review system configurations annually using the Security Compliance Checker (SCC) tool and manual STIG checklists. This includes review of system and user identifiers. More frequent reviews will occur if determined necessary by the CCB **CCI-001502**.

7. Least Functionality (CM-7)

The [ORGANIZATION NAME] will configure the systems to provide only essential capabilities and will document these configurations in the System Security Plan (SSP) **CCI-000381**. The systems will also be configured to prohibit or restrict the use of functions, ports, protocols, and/or services IAW DoDI 8551.01, and will be documented in the approved ports, protocols, and/or services list **CCI-000382.**

CM-7(1) Least Functionality – Prevent Program Execution

The Ports Protocols and Services (PPS) Document details the ports, protocols, and services required for the system to function, and will be the only authorized PPS in use **CCI-001761**. All other ports, protocols, and services are strictly prohibited for use. The installed applications, capabilities, ports, protocols, and services installed or available on the [FACILITY NAME] system will be reviewed monthly to ensure no capabilities exist outside of what is required for the system to meet the mission **CCI-000384**. The approved hardware list, software list, and PPS will be referenced as part of this activity, and any functions, ports, protocols, and services not approved or deemed to be unnecessary will be removed from the system.

CM-7 (2) Least Functionality – Prevent Program Execution:

All network capable software programs usage on any [FACILITY NAME] system complies with DoDI 8551.01 **CCI-001592, CCI-001763**.

CM-7 (5) Least Functionality – Whitelisting for Moderate Impact level systems:

The Software List required for the system to function, will be the only authorized software in use **CCI-001772, CCI-001773**. [FACILITY NAME] system employs an deny-all/permit-by-exception policy to allow the execution of authorized software programs on the information system **CCI-001774**. The authorized Software List is reviewed and updated monthly **CCI-001777**.

8. Information System Component Inventory (CM-8)

The Hardware List required for the system to function, will be the only authorized components in use and no hardware component will be removed or installed without CCB approval via the Change Request process **CCI-000389, CCI-000392, CCI-000395, CCI-000399**. The authorized Hardware List is reviewed and updated annually **CCI-001780.**

CM-8(1) Information System Component Inventory - Updates during Install/Removal for Moderate Level impact systems

[ORGANIZATION NAME] updates the Hardware List at the time a component is added or removed **CCI-000389, CCI-000408, CCI-000409, CCI-000410**.

CM-8(3) Information System Component Inventory – Automated Unauthorized Component Detection for Moderate Level impact systems

The [ORGANIZATION NAME] uses [automated mechanisms] to detect the presence of unauthorized hardware, software, and firmware components **CCI-000416**. When unauthorized components are detected, the [ORGANIZATION NAME] implements a process to take action by disabling network access, isolating the components, and/or notifying the ISSO and ISSM **CCI-001783, CCI-001784**.

CM-8(5) Information System Component Inventory – No Duplicate Accounting of Components for Moderate Level impact systems

[ORGANIZATION NAME] examines the Hardware List of all systems to ensure components are not duplicated across systems **CCI-000419**. This examination will ensure that all components within the authorization boundary of the [FACILITY NAME] system are not duplicated in other [ORGANIZATION NAME] system inventories.

9. CM-9 Configuration Management Plan for Moderate Impact level systems:

A System Configuration Management Plan will be developed for any **Moderate** Impact level system. This document details:

[roles, responsibilities, and configuration management processes and procedures] for implementing the Configuration Management Plan **CCI-000421, CCI-000423**

[configuration items for the system] **CCI-000424, CCI-000426**

[a process for managing the configuration of the identified configuration items] **CCI-001793, CCI-001795, [**the process for configuring these items throughout the system development life cycle] **CCI-001790, CCI-001792** and [guidelines for implementing configuration management] **CCI-001796, CCI-001798** . The plan is protected from unauthorized disclosure and modification **CCI-001799, CCI-001801.**

10. Software Usage Agreements (CM-10)

System software and software documentation are used in accordance with copyright laws [and/or contract agreements] **CCI-001726, CCI-001727, CCI-001728, CCI-001729**. Software licenses or relevant terms and conditions will be tracked in the software list [and the System Configuration Guide].

11. User-Installed Software (CM-11)

Users may not install software or use software licenses outside of what is allowable in the contracts, copyrights and configuration baselines or approved changes **CCI-001804, CCI-001805, CCI-001806, CCI-001807.** Only Administrative users, as defined in the [FACILITY NAME] *Access Control Policy and Procedures document*, are authorized or are granted permissions to install software, and any software installation is documented, tracked, and maintained per CCB review and approval processes. Monthly Assured Compliance Assessment Solution (ACAS) scans shall include checks for unauthorized software

CCI-001809.

Risk Management Framework
Contingency Planning (CP)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Contingency Planning (CP), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Baseline Controls and Rationale

Control	Control Name
Controls for Security Impact Level: LOW	
CP-1**	Contingency Planning Policy and Procedures
CP-2*	Contingency Plan
CP-3*	Contingency Training
CP-4*	Contingency Plan Testing
CP-9*	Information System Backup
CP-10*	Information System Recovery and Reconstitution
CP-12*	Safe Mode
Added Controls for Security Impact Level: MODERATE	
CP-2 (1)*	Contingency Plan-Coordinate with Related Plans
CP-2 (3)*	Contingency Plan-Resume Essential Mission/Business Function
CP-2 (8)*	Contingency Plan-Identify Critical Assets
CP-4(1)*	Contingency Plan Testing- Coordinate with Related Plans
CP-6*	Alternate Storage Site
CP-6 (1)*	Alternate Storage Site-Separation from Primary Site
CP-6 (3)*	Alternate Storage Site-Accessibility
CP-7*	Alternate Processing Site
CP-7 (1)*	Alternate Processing Site-Separation from Primary Site
CP-7 (2)*	Alternate Processing Site-Accessibility
CP-7 (3)*	Alternate Processing Site-Priority of Service
CP-8*	Telecommunication Services
CP-8 (1)*	Telecommunication Services-Priority of Service
CP-8 (2)*	Telecommunication Services-Single Point of Failure
CP-9 (1)	Information System Backup-Test for Reliability
CP-10 (2)*	Information System Recovery & Reconstitution-Transaction Recovery

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 CP Organizational Policy Controls

Broadly implemented CP policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific CP safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Disaster Recovery and Contingency Plans (CP-2)

The Disaster Recovery Plan (DRP) is a component of this [FACILITY NAME] Contingency Planning Policy & Procedures. The DRP establishes policy and repeatable procedures used by [FACILITY NAME] personnel for the effective and efficient response, service resumption, and recovery of the control system in case of an event that adversely affects the operation of the system **CCI-000448**. This document, [combined with [FACILITY NAME] System Configuration Guide], provides all the necessary information needed for response, resumption, and recovery of system capabilities in the event of a [FACILITY NAME] system failure **CCI-000445.**

[Specific elements of DRP **CCI-000446**]:

[Identify mission critical system and business essential functions and address steps for maintaining these functions during a service disruption, system compromise or system failure.] **CCI-000443, CCI-000444**, **CCI-000450, CCI-000451, 000452, 000453, 000454, 000455.**

Table 3 - Essential Business Functions and Missions

Essential Business Functions	Essential Mission Functions

[Clearly and accurately document recovery objectives for system and identify restoration priorities for essential components] **CCI-000446, CCI-000447.**

Table 4 - Mission Critical Assets and Restoration Priority

System Asset	Description	Restoration Priority

[Identify metrics for addressing system failure and restoration. Recovery plan must address system restoration without allowing deterioration of security safeguards] **CCI-000448, 000456.**

Table 5 - Time to Restore Essential Capabilities

Essential Business or Mission Capability	Time to Restore Minimum Required Operating Capability	Time to Restore Full Operating Capability

[Identify key stakeholders and personnel. Assign key personnel with responsibilities for disaster recovery and include necessary contact information in the DRP. Key stakeholders and personnel must review the DRP.] **CCI-000449, CCI-000457, CCI-000459.**

[Identify coordination with other entities and contact information for key personnel to ensure continuity of operations during various emergencies. The contingency team will coordinate with incident handling personnel to ensure efforts are coordinated in the event of a system compromise] **CCI-000460.**

Table 6 – Disaster Recovery Team

Key Personnel	Name	Contact Information
SO or Representative		
ISSO		
ISSM		

After an emergency is resolved, a synopsis of the problem and the resolution process will be generated in the form of a lessons learned document and disseminated to all concerned (Incident/Event/Failure After Action Report template provided). Modifications to the DRP plan will be made to accommodate the lessons learned to ensure the most efficient response is achieved in the event the DRP must be activated to address a similar issue in the future **CCI-000466**. All modifications to these policies and procedures will be recorded in the Revision History Table in this document **CCI-000462**. The DRP is reviewed and updated every five-years or when changes to the system or organization are implemented **CCI-000463, CCI-000464, CCI-000465**. The DRP is protected from unauthorized disclosure and modification **CCI-002832**. Updates are communicated to all personnel involved in the execution of this plan **CCI-000468**.

CP-2 (1) Contingency Plan – Coordinate with Related Plans for Moderate Impact level systems:

[Documents any applicable agreements with responsible internal or external entities responsible for contingency planning] **CCI-000469.**

CP-2 (3) Contingency Plan – Resume Essential Mission/Business Functions for Moderate Impact level systems:

[Documents procedures for resumption of essential missions/business functions within 1 hour (For systems with High Availability) or 12 hours (For systems with Moderate Availability)] **CCI-000475, CCI-000476.**

CP-2 (8) Contingency Plan – Identify Critical Assets for Moderate Impact level systems:

[Identifies and documents critical system assets supporting essential mission/business systems] **CCI-002828, CCI-002829.**

3. Disaster Recovery and Contingency Plan Training (CP-3)

Personnel who have assumed a significant role or responsibility in managing or implementing the DRP and the contingency team shall be trained in the accomplishment of their responsibility within ten-days of being assigned to such position **CCI-000486, CCI-002834**. The [FACILITY NAME] ISSO shall ensure that the training is completed and any questions regarding activation and implementation of this plan are addressed. Refresher contingency training shall be conducted at least annually **CCI-000487**.

4. Disaster Recovery and Contingency Plan Testing (CP-4)

Exercise and testing the DRP may be necessary to determine the effectiveness of the plan and the organizational readiness to execute the plan **CCI-000492**. Need for contingency testing is determined by the [ORGANIZATION NAME] and documented in the table that follows. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the contingency team on a "per event" basis. DRP will be tested or exercised at least annually **CCI-000494.**

Table 7 – Continency Testing

System	Type of Testing	Key Personnel

The contingency testing must be documented (Incident/Event/Failure After Action Report template provided). The contingency team along with those involved in the test or exercise shall review the results and update this DRP, as required, to improve the effectiveness of the plan **CCI-000496**. Upon completion of testing, the required corrective actions will be documented and tracked within the Plan of Action & Milestones (POA&M) **CCI-000497**.

CP-4 (1) Contingency Plan Testing – Coordinate with Related Plans for Moderate Impact level systems:

[Documents any applicable agreements with responsible internal or external entities responsible for contingency planning testing] **CCI-000498.**

Alternative Storage Site (CP-6) for Moderate Impact level systems:

The alternate storage site for storage and retrieval of system backup information is: [Alternate storage site provides information security safeguards equivalent to that of the primary site] **CCI-**

000505.

Alternative Processing Site (CP-7) for Moderate Impact level systems:

The alternate processing site for the safe transfer and resumption of essential mission/business functions is: [Alternate storage site provides information security safeguards equivalent to that of the primary site] **CCI-000513.** The following essential mission/business functions are permitted to transfer and resume at an alternate processing sites: [Define essential mission/business functions that are permitted to transfer and resume at an alternate processing site] **CCI-002839.**

Alternative Telecommunications Services (CP-8) for Moderate Impact level systems:

The alternate telecommunication services to allow the resumption of essential mission/business functions is: [Define the time period when primary telecommunication capabilities are unavailable at the primary site to permit transfer to the alternative service] **CCI-000524, CCI-000525.** The following essential mission/business functions are to be resumed using the alternative telecommunication services: [Define essential mission/business functions that are permitted to transfer and resume at an alternate processing site] **CCI-002840, CCI-002841.**

5. Information System Backup (CP-9)

The [ORGANIZATION NAME] shall ensure system-level backups are performed on a weekly basis to preserve security configurations. [Specific system backup procedures] **CCI-000535, CCI-000537**. Backup data shall be secured logically or physically as Unclassified, FOUO data in a location separate from the [FACILITY NAME] system **CCI-000540**. Documentation backups shall be generated when created, updated, or as required by system baseline configuration changes **CCI-000539.**

CP-9 (1) System Backup – Testing for Reliability for Moderate Impact level systems:

Backup information is tested at least monthly to verify media reliability and information integrity and the test date is recorded. **CCI-000542.**

6. Information System Recovery and Reconstitution (CP-10)

Recovery and reconstitution of the information system to a known state after a disruption is accomplished following system disruption, compromise or failure. [Specific recovery and reconstitution procedures] **CCI-000550, CCI-000551, CCI-000552**.

7. Safe Mode (CP-12)

The following conditions require the system to enter safe mode of operation: [Define specific conditions]. **CCI-002856.** The following restrictions apply to safe mode of operation: [Define specific operation restrictions]. **CCI-002857**.

Risk Management Framework Identification and Authentication (IA) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date

Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Identification and Authentication (IA), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Applicable Baseline IA Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
IA-1**	Identification and Authentication (I&A) Policy and Procedures
IA-2*	I&A (Organizational Users)
IA-2(1)*	Identification and Authentication | Network Access to Privileged Accounts
IA-2(12)*	I&A (Organizational Users) | Acceptance of PIV Credentials
IA-3*	I&A (Device)
IA-4*	Identifier Management
IA-5*	Authenticator Management
IA-5(1)*	Authenticator Management | Password-Based Authentication
IA-6*	Authenticator Feedback
IA-7*	Cryptographic Module Authentication
IA-8*	I&A (Non-Organizational Users)
IA-8(1)*	I&A (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies
IA-8(2)*	I&A (Non-Organizational Users) | Acceptance of Third-Party Credentials
IA-8(3)*	I&A (Non-Organizational Users) | Use of FICAM-Approved Products
IA-8(4)*	I&A (Non-Organizational Users) | Use of FICAM-Issued Profiles
Controls for Security Impact Level: MODERATE	
IA-2(11)*	I&A (Organizational Users)| Remote Access- Separate Device
IA-2(2)*	I&A (Organizational Users)| Network Access to Non-Privileged Accounts
IA-2(3)*	I&A (Organizational Users)| Local Access to Privileged Accounts
IA-2(8)*	I&A (Organizational Users)| Network Access to Privileged Accounts – Replay Resistance
IA-3(1)*	I&A (Device) | Cryptographic Bidirectional Authentication
IA-3(4)*	I&A (Device) | Device Attestation

IA-5(2)*	Authenticator Management | PKI-Based Authentication
IA-5(3)	Authenticator Management |
IA-5(11)*	Authenticator Management | Hardware Token-Based Authentication

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 IA Organizational Policy Controls

Broadly implemented IA policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific IA safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Organizational Users (IA-2)

Individual accounts, privileged [and non-privileged] users, will each have unique usernames and passwords which allow unique identification and authentication and are closely monitored according to the Access Control Policy & Procedures **CCI-000764**.

3. Organizational Users – Network Access to Privileged Accounts (IA-2(1))

The [FACILITY NAME] system implements multifactor authentication for network access to privileged accounts and will follow applicable STIG/SRG guidance **CCI-000765**.

IA-2 (2) Organizational Users - Network Access to Non-Privileged Accounts for Moderate Impact level systems:

The [FACILITY NAME] system implements multifactor authentication for network access to non-privileged accounts and will follow applicable STIG/SRG guidance **CCI-000766**.

IA-2 (3) Organizational Users - Local Access to Privileged Accounts for Moderate Impact level systems:

The [FACILITY NAME] system implements multifactor authentication for local access to privileged accounts and will follow applicable STIG/SRG guidance **CCI-000767**.

IA-2 (8) Organizational Users - Network Access to Privileged Accounts – Replay Resistance for Moderate Impact level systems:

The [FACILITY NAME] system implements replay-resistant authentication mechanisms for network access to privileged accounts and will follow applicable STIG/SRG guidance **CCI-001941**.

IA-2 (11) Organizational Users - Remote Access to Accounts – Separate Device for Moderate Impact level systems:

The [FACILITY NAME] system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separated from the system gaining access and the device meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval **CCI-001949, CCI-001952**. Configuration will follow applicable STIG/SRG guidance.

4. IA-2 (12) Organizational Users – Acceptance of PIV Credentials

The [FACILITY NAME] system accepts and electronically verifies Personal Identity Verification (PIV) credentials and will follow applicable STIG/SRG guidance **CCI-001954.**

5. Identifier Management (IA-4)

The ISSM will authorize the assignment of individual privileged or non-privileged accounts, groups, roles, and device identifiers. The [FACILITY NAME ISSO or ISSM] manage information system identifiers by selecting an identifier that identifies an individual, group, role, or device **CCI-001971**. [Accounts are described in the *Access Control Policy and Procedures document*, and the Administrator is assigned the duty to monitor and maintain a comprehensive list of account identifiers for all approved groups and users in accordance with the *Configuration Management Policy & Procedures*.] Installation control systems will use the following identifiers for users **CCI-001972**:

- [User accounts type (privileged, non-privileged, group)
- User characteristics
  - Contractor or Government employee
  - Nationality
- Host name
- Member of (groups)
- Internet Protocol (IP) Address]

The process and procedure for assigning and/or altering identifiers for user accounts are [a duty of the Administrator under the supervision of the Change Control Board (CCB)] **CCI-001973**. [The CCB] will review the hardware list or other method that tracks the device identifiers listed above. The Hardware List will include other identifying information for components, such as make and model of equipment. This information is also in the enterprise Mission Assurance Support Service (eMASS) registry. DoD has defined the time period as one-year for reuse of user identifiers and the ISSM monitors and tracks the reuse of identifiers, during the annual review of the System Configuration Information, as detailed in the [FACILITY NAME] *Configuration Management Policy and Procedures document* **CCI-001975**. If applicable for the control system, shared authenticators for group/role accounts will be managed as membership changes **CCI 001990.** DoD has specified the time-period of 35 days of inactivity requires that the identifier (account) be deactivated **CCI-000795**.

6. Authentication Management (IA-5)

The authenticator used for the microgrid control systems are account identifier(s) and password(s). Authentication and password management and protection is also covered in the [FACILITY NAME] *Access Control Policy & Procedures document* (policy) as well as the [FACILITY NAME] *System Configuration Guide* (technical).

All personnel with account access to the control system are required to complete DoD [and ORGANIZATION NAME] mandated training on password usage and protection **CCI-002365**. There is also a requirement to sign the Acceptable Use Policy (AUP). The AUP must be signed before access is granted per the [FACILITY NAME] *Security Planning Policy and Procedures document*. The [FACILITY NAME Account Manager] is responsible for assigning, revoking and monitoring the account(s) and password(s). The [FACILITY NAME Account Manager] will create user accounts only after the ISSM has confirmed that the user has met all of the DoD IA baseline certification prerequisites (i.e. training, background check, etc.). Verification is tracked on the Master Authorized User List (Master AUL List Template provided). **CCI-001980, CCI-001981, CCI-001985, CCI-001990,**

Once the account is created, the [FACILITY NAME Account Manager] will assign a temporary random password to the account and will set the account to require a password change upon first login. Account passwords are not to be shared and will be safeguarded to a level commensurate with the level of the information that the system processes. Temporary passwords will be sent to the users using either an encrypted Common Access Card (CAC) or [Government email]. Factory-set, supplier-set, or default passwords must be changed. The ISSM is responsible for ensuring that all factory-set or vendor/integrator default passwords for the system are changed and meet the criteria above within 30-days of new component or software deployment **CCI-001989**, **CCI-002041, CCI-002042.**

All passwords stored on the system are protected by access control lists, encryption, and are subject to weekly audit reviews. Passwords will never be transmitted in clear text, and passwords on the default vendor accounts have all been changed. As the Administrator, the ISSM maintains a current list of all accounts on the system as well as the individual username(s) for those accounts, as detailed in the [FACILITY NAME] *Access Control Policy and Procedures Document*. This document is sensitive and for official use only and must be stored properly in accordance with the [FACILITY NAME] *Media Protection Policy and Procedures Document*. [A Backup Administrator password must be kept in a sealed envelope in a locked enclosure (e.g., a safe)] **CCI-001982, CCI-000183, CCI-001986.** Accounts that have not been used in 30 days will be deactivated through automation or during the [monthly account audits]. Accounts belonging to personnel who have been terminated will immediately be deactivated as will accounts for personnel who have been transferred **CCI-001984, CCI-001988.**

Factory-set, supplier-set, or default passwords must be changed. The ISSM is responsible for ensuring that all factory-set or vendor/integrator default passwords for the system are changed and meet the criteria above within 30-days of new component or software deployment **CCI-001989**. The [FACILITY NAME Account Manager] will review all accounts monthly and will require Common Access Card (CAC), biometrics and passwords be changed in accordance with DoD requirements **CCI-000182**. All account passwords have a minimum lifetime restriction of 24 hours **CCI-000179.** [For components that cannot meet the password requirements, the strongest password that is technically feasible will be applied.] Authenticators may not be reused **CCI-000181**.

[The organization manages information system authenticators by establishing administrative procedures for damaged authenticators] **CCI-001983, CCI-001987.**

7. Password Based Authentication (IA-5(1))

For components that cannot meet the password requirements, the strongest password that is technically feasible will be applied. Authenticators may not be reused **CCI-000181**. The general rules for password strength can be found in the System Configuration Guide and STIG/SRGs. Additional rules can be found below **CCI-001544, CCI-000200:**

- Cannot use any of the prior 5 passwords
- At least 50% of the minimum password length is changed

All personnel with account access to the microgrid control system are required to complete DoD mandated training on password usage and protection **CCI-002365**. Factory-set, supplier-set, or default passwords must be changed. The ISSM is responsible for ensuring that all factory-set or vendor/integrator default passwords for the system are changed and meet the criteria above within 30-days of new

component or software deployment **CCI-001989**. As the Administrator, the SO or ISSM maintains a current list of all accounts on the system as well as the individual username(s) for those accounts, as detailed in the [FACILITY NAME] *Access Control Policy and Procedures Document*. This document is sensitive and for official use only and must be stored properly on an encrypted hard drive or locked in a safe for paper copies. A Backup Administrator password must be kept in a sealed envelope in a locked enclosure (e.g., a safe) **CCI-000183**. All personnel with account access to the control system are required to complete DoD mandated training on password usage and protection and sign Acceptable Use Policy (AUP). The AUP must be signed before access is granted per the [FACILITY NAME] *Security Planning Policy and Procedures document.*

The [FACILITY NAME Account Manager] will review all accounts monthly and will require Common Access Card (CAC), biometrics and passwords be changed in accordance with DoD requirements **CCI-000182**. All account passwords have a minimum lifetime restriction of 24 hours **CCI-000179.**

Risk Management Framework
Incident Response (IR)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

This document applies to Incident Response (IR). An IR event/incident is any attempted or successful unauthorized access, use, disclosure, modification or destruction of information associated with the [FACILITY NAME] system that is attributable unplanned, but not related to age or defect. A system or application failure due to age or defect may be an emergency event but is not an IR event/incident. System or application failures are addressed in the [FACILITY NAME] *Contingency Planning (CP) Policy and Procedures document*.

An IR event/incident is initially handled by the [FACILITY NAME] Incident Response Team (IRT). The IRT is comprised of individuals who are prepared for and respond to a [FACILITY NAME] system IR event/incident and include all individuals necessary to properly assess cyber incidents and make decisions regarding the proper course of action. The ISSM is responsible for appointing the appropriate team members of the IRT. The IR event/incident is handled and reported in accordance with the CJCSM 6510.01B Cyber Incident Handling Program.

A summary of the organizational policy security controls unique to Incident Response (IR), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Baseline Controls and Rationale

Control	Control Name
Controls for Security Impact Level: LOW	
IR-1**	Incident Response Policy and Procedures
IR-2*	Incident Response Training
IR-4*	Incident Response Handling
IR-5	Incident Monitoring
IR-6*	Incident Reporting
IR-7*	Incident Response Assistance
IR-8*	Incident Response Plan
Controls for Security Impact Level: MODERATE	
IR-3*	Incident Response Testing
IR-3(2)*	Incident Response Testing – Coordinate with Related Plans
IR-4(1)*	Incident Response Handling- Automated
IR-6(1)*	Incident Reporting-Automated
IR-7(1)*	Incident Response Assistance- Automated

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 Organizational Policy Controls

Broadly implemented IR policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific IR safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Incident Response Training (IR-2)

Specific IR training is provided to [ORGANIZATION NAME] users and IRT members consistent with their assigned roles and responsibilities by mandating Annual Awareness Training per DoD Directive 8570.01 compliance. IRT members will complete the [specific training requirements below], within 30 working days of being appointed to the IRT on orders and on an annual basis thereafter **CCI-000813, CCI-000814, CCI-002779**:

- [Complete the Incident Handling Course available on the web on the Enterprise Access Management Service (eMASS) website (https://iatraining.us.army.mil) within 30 days of appointment to the IRT.]
- [Complete eight hours of information assurance or incident response refresher training OR table top exercise annually and record in ATCTS under "other training".]

Incident Response Testing (IR-3) for Moderate Level Systems

[ORGANIZATION NAME] tests the incident response capability for the information system [at least every six months for high availability and] at least annually for systems with Moderate Level Availability **CCI-000818**. The IR Testing plan is as follows: [Briefly describe plan to Test System(s)]. The process to test incident response capability for the information system must be documented (Excel file: LogSheets.xls/Incident_Event_Failure AAR log template) **CCI-001624.**

Incident Response Testing- Coordination with Related Plans (IR-3(2)) for Moderate Level Systems

The [FACILITY NAME] IR testing plan, must document the necessary support and coordination expected from all elements involved in Incident Response **CCI-002780.** Related plans and agency coordination are summarized in the table below:

System	Supporting Agency/Document	Support Provided	Point of Contact
Example	*[FACILITY NAME] Fire Department*	*Fire protection, prevention services.*	*Emergency 911*

3. Incident Handling (IR-4)

The [FACILITY NAME] policy and procedures for handling incidents includes preparation, detection and analysis, containment, eradication, and recovery **CCI-000822**. Proactive detection and initial reporting of potential security incidents is implemented in accordance with the [FACILITY NAME]Audit and Accountability Policy and Procedures. [Proactive detection and incident handling procedures are summarized below]:

Upon noticing anomalous or suspicious activity (incident or reportable event) all [ORGANIZATION NAME] Users will implement the procedures document in the Incident Response Plan Section (Section 7) of this

document. At a minimum, Users will cease all activity on a computer and report the situation immediately to the organizational ISSM, who will immediately notify the ISSO:

Recovery following IR is documented with the [FACILITY NAME] Contingency Planning Policy and Procedures document. [Additional considerations for IR recovery include] **CCI-000823**

- [address critical and mission essential functions/system]
- [address Computer Network Defense Service Providers (CNDSP), as necessary]
- [address connection to the critical networks including: Secret Internet Protocol Router Network (SIPRNet), Non-classified Internet Protocol Router Network (NIPRNet), or any other unclassified network.]

An Incident Response After Action Report will be completed by a member of the IRT to documented IR activities and handling (Excel file: LogSheets.xls/ Incident_Event_Failure AAR log template). The ISSM will review the Incident Response After Action Report and incorporate lessons learned into incident response procedures **CCI-000824, CCI-001625**.

Incident Response Handling-Automated (IR-4(1)) for Moderate Level Systems

[ORGANIZATION NAME] incorporates automated mechanisms into the IR Handling process **CCI-000825. [**A summary of these automated mechanisms is documented as follows:]

4. Incident Monitoring (IR-5)

[FACILITY NAME] security events/incidents are document using an Incident Response After Action Report to ensure proper incident response and follow-up **CCI-000832**. (Excel file: LogSheets.xls/ Incident_Event_Failure AAR log template)

5. Incident Reporting (IR-6)

The Acceptable Usage Policy (AUP) requires [ORGANIZATION NAME] users to report suspected security incidents to the ISSM, ISSO, or IRT, as applicable. Event/incidents are placed into categories to identify the proper response and the allotted timeframe for reporting. The cyber incident handling process will be coordinated to ensure effective coordination and communication through the appropriate channels and implementation of lessons learned to help improve infrastructure protection strategies and the cyber incident handling procedures under DoD CJCSM 6510.01B - Cyber Incident Handling Program. When reporting any incident, it is imperative that attention to detail is exercised, therefore, a Security Incident Report Form is provided in Appendix A. The [ORGANIZATION NAME] reporting chain for security incidents is provided in Appendix B **CCI-000835, CCI-000836**.

Incident Response Reporting-Automated (IR-6(1)) for Moderate Level Systems

[ORGANIZATION NAME] incorporates automated mechanisms into the IR Reporting process **CCI-000837. [**A summary of these automated mechanisms is documented as follows:]

6. Incident Response Assistance (IR-7)

This section addresses specific incident response support within the [ORGANIZATION NAME] that offers

advice and assistance to users of the information system for the handling and reporting of security incidents. **CCI-000839**. Specific IR Assistance is: [An IT help desk is an example of IR Assistance].

Incident Response Assistance-Automated (IR-7(1)) for Moderate Level Systems

The [ORGANIZATION NAME] incorporates automated mechanisms, such as information sharing capability, into the IR Assistance process **CCI-000840. [**A summary of these automated mechanisms is documented as follows:]

7. Incident Response Plan (IR-8)

7.1 OVERVIEW

The [FACILITY NAME] Incident Response Plan (IRP) is summarized in this Section. [The IRP considers the coordination and sharing of information with external organizations involved**.]** The implementation of the IR begins with [ORGANIZATION NAME] User awareness via the AUP and continues with the annual awareness training required by DoD **CCI-002794, CCI-002795**. This *IR Policy and Procedures document* is distributed to personnel that have signed the AUP **CCI-000846** and is reviewed and signed by the SO, ISSO and ISSM **CCI-000844**. This forum also provides an opportunity for users to ask questions and provide feedback relating to the implementation of unique requirements specific to the [FACILITY NAME] **CCI-002796, CCI-002797, CCI-002798.**

7.2 INCIDENT IDENTIFICATION

The [FACILITY NAME] *Audit and Accountability (AU) Policy and Procedures document* defines a list of auditable events to identify event/incidents. Some events/incidents are subtle and require analysis and technical review to ascertain not only the type of event/incident that has occurred. At other times, certain behaviors by computers, servers and devices connected to an information system can indicate an event/incident. [A summary of event/incidents includes] **CCI-002799**:

- [Password activity such as:
  - Changes to a password a System User did not initiate
  - unable to log-in
  - requests to share password
- Browser home page changes or pop-up ads that can't be closed
- New desktop icons appearing at login
- Inability to connect to Internet servers (web- or application-sites)
- Workstation infection from a virus, worm or Trojan, adware, or spyware
- Sudden workstation slowdowns
- File additions, changes, or deletions
- Noticeable decreases in hard drive space
- Sudden increases in hard drive or network activity
- A Ransomware screen on the monitor and systems locked]

7.3 INCIDENT REPORTING

Event/incidents are placed into categories to identify the proper response and the allotted timeframe for reporting. The cyber incident handling process will be coordinated to ensure effective coordination and communication through the appropriate channels and implementation of lessons learned to help improve infrastructure protection strategies and the cyber incident handling procedures under DoD CJCSM 6510.01B - Cyber Incident Handling Program. When reporting any incident, it is imperative that attention to detail is exercised, therefore, an example DoD CJCSM 6510.01B Security Incident Report Form is provided in Appendix A.

Table 3 contains a list of Cyber Incident and Reportable Event Categories and reporting timeline for information systems (IS) based on the Joint Task Force-Global Network Operations (CJCSM 6510.01B) **CCI-002799**.

Table 2 – Cyber Incident and Reportable Event Categories (Source: CJCSM 6510.01B)

Category	Description	Reporting Timeline
0	**Training and Exercises**—Operations performed for training purposes and support to Red Team exercises.	Use reporting timelines outlined for Category 1-7 that exercise or red team activity is replicating
1	**Root Level Intrusion (Incident)**—Unauthorized privileged access to information system (IS). Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS compromised with malicious code that provides remote interactive control, it will be reported in this category.	Ongoing: 1 hour from detection. Existing: 24 hours following validation by ISSM
2	**User Level Intrusion (Incident)**—Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user- level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS compromised with malicious code that provides remote interactive control, it will be reported in this category.	48 hours following validation by ISSM

Category	Description	Reporting Timeline
3	**Unsuccessful Activity Attempt (Event)**—Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. Note the above CAT 3 explanation does not cover the "run-of-the- mill" virus that is defeated/deleted by AV software. "Run-of-the- mill" viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in JIMS.	Ongoing: 10 minutes following start of activity. Event in Progress: Follow up report 1 hour after initial report. Additional reports shall be made on a schedule not to exceed 3 hours. Closeout Report: 48 hours after cessation of DOS.
4	**Denial of Service (Incident)**—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.	48 hours following validation by ISSM
5	**Non-Compliance Activity (Event)**—Activity that potentially exposes ISs to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DoD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.	Major: N/A Minor/Routine: 24 hours following validation by ISSM
6	**Reconnaissance (Event)**—Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.	Major N/A Minor (individual systems infected, no large outbreak): 24 hours following validation by ISSM
7	**Malicious Logic (Incident)**—Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.	Ongoing: 1 hour from detection. Existing: 24 hours following validation by ISSM

Category	Description	Reporting Timeline
8	**Investigating (Event)**—Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.	
9	**Explained Anomaly (Event)**—Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.	

7.4 ROLES AND RESPONSIBILITIES

7.4.1 [FACILITY NAME] USERS

[ORGANIZATION NAME] Users are any employee, vendor, subcontractor or client who has been authorized access to the [FACILITY NAME] system. User responsibilities for IR are **CCI-002801**:

- [ORGANIZATION NAME] Users of the are responsible for identifying and reporting any suspicious activity that may indicate a possible event/incident. [FACILITY NAME] Users will treat every event/incident as an "Event" until a 3rd party investigates (ISSM, CYBERCOM, etc.) and confirms an "Event" is an actual or very likely security incident. Upon confirmation, [FACILITY NAME] Users will activate proceed with notifications.
- At a minimum, cease all activity on a computer and immediately report security incident(s) to the [FACILITY NAME] ISSM.
- If the event/incident involves a password which has been compromised, first CHANGE the password immediately, THEN report the incident, according to the guidelines outlined below in this document.
    - DO NOT continue working. Instead, come to a graceful work stoppage.
    - THEN, close all applications, if possible, and shutdown your computer.
    - DO NOT resume using your computer until it has been cleared by the Information Technology (IT) support personnel, or other members of the IRT.
    - And finally, DO NOT discuss the event/incident with anyone except the IRT, as you may be speaking to someone involved in the event/incident. Also, in an event/ incident, when interviewing individuals, it is better if people recall what happened, as opposed to what they heard someone else describe.
- Take careful notes of all details related to the security incident
- Assist IRT by providing accurate and detailed information, and answer any questions posed as honestly and forthrightly as possible.

- Provide potential means of fixing identified incident response vulnerabilities in correlation with appropriate IR personnel.
- Coordinate with the [FACILITY NAME] ISSM to investigate and resolve incident and security problems.

7.4.2 [FACILITY NAME] ISSM

The ISSM as responsible for the administration and management of [FACILITY NAME] security program and is the focal point for all organizational information systems security concerns. Responsibilities of the ISSM include **CCI-002801**:

- Appoint IRT Members.
- Reviews the [FACILITY NAME] audit logs weekly for anomalies and inappropriate/unusual activities in accordance with the [FACILITY NAME] Audit and Accountability Policy and Procedures.
- Review and update the baseline configuration, diagrams and hardware/software lists, SCAP scans, hardware/software lists, diagrams, PPS, maintenance tools, spare components lists annually. Report significant changes, upgrades and deletions.
- Responsible for the administration and management of [FACILITY NAME] security program and is the focal point for all organizational information systems security concerns.
- Pass incoming incident information to IRT team members [and appropriate levels] in a timely fashion.
- Advise [appropriate levels of leadership] in the event of a serious security incident and coordinating the response with security personnel.
- Implement the overall information system security program.
- Ensure that all information systems security related incidents and violations are immediately reported, properly investigated, and correctly resolved.
- Coordinate all targeted monitoring activity to include appropriate notification to [appropriate levels of leadership] for the system being monitored. During targeted monitoring activities, extreme care must be exercised in conducting targeted monitoring as a response to an incident or suspected incident to ensure that evidence is not destroyed, innocent personnel are not implicated, and the subject does not become aware of a planned monitoring activity.
- Gather data, perform analysis and apply principles, procedures and methodologies to assist the investigating personnel in resolving problems.
- Collect audit records. Review and retain the local security audit trail.

7.4.3 [FACILITY NAME] ISSO

The ISSO serves as the organizational level IT manager. Responsibilities of the ISSO include **CCI-002801:**

- Serves on the IRT.
- Provides guidance and oversight for all security issue resolutions.
- Approves the work plan for remediation of security incidents.
- Performs security audits using approved DoD tools and methods.

- Reviews and approves changes to configuration(s), particularly as they impact existing Authority to Operate (ATO).
- Documents changes or deviations from previously approved security baselines.

7.4.4 Information Assurance Manager (IAM)

The IAM is responsible for the administration and management of the [ORGANIZATION NAME] computer security program and is the focal point for all organizational information systems security concerns. The IAM support members are most likely to be able to spot unusual or suspicious activity and are often the first to recognize a security incident. However, in the case where an incident is first observed by a [ORGANIZATION NAME] User, the IAM Support members' most important role is to listen carefully, and not jump to conclusions. It is imperative to take careful notes and pay attention to detail. The IAM Support members responsibilities are **CCI-002801**:

- Pass incoming incident information from the ISSMs to appropriate network management and service/agency levels in a timely fashion.
- Advise upper leadership in the event of a serious security incident and coordinating the response with security personnel.
- Implement the overall information system security program.
- Ensure that all information systems security related incidents and violations are immediately reported, properly investigated, and correctly resolved.
- Coordinate all targeted monitoring activity to include appropriate notification to [appropriate levels of leadership] for the system being monitored. During targeted monitoring activities, extreme care must be exercised in conducting targeted monitoring as a response to an incident or suspected incident to ensure that evidence is not destroyed, innocent personnel are not implicated, and the subject does not become aware of a planned monitoring activity.
- Gather data, perform analysis and apply principles, procedures and methodologies to assist the investigating personnel in resolving problems.
- Collect audit records from the local Information System components, review and retain the local security audit trail.

7.4.5 Incident Response Team (IRT)

The ISSM manages the response process and is responsible for assembling the IRT. The contact information for the [FACILITY NAME] IRT is provided in Appendix B. The ISSM will ensure the team includes all the individuals necessary to properly assess the incident and make decisions regarding the proper course of action. Training requirements for IRT team members is detailed in Section 2. The IRT meets regularly to review status reports and to authorize specific remedies. In most cases, the IRT will be comprised of **CCI-002801**:

- All members of [ORGANIZATION NAME] IT Support (in-house and contract support)
- [FACILITY NAME] ISSM
- [FACILITY NAME] ISSO
- Security professionals, as designated by vendors or subcontractors for information systems outsourced, as needed

The responsibility of IRT members includes **CCI-002801**:

- The IRT will notify the [FACILITY NAME] ISSO, ISSM or SO of the nature and extent of the incident at the earliest feasible time.
- Serving as the focal point for all communications related to the security incident.
- Develop and implement plans and procedures to address security incidents, in accordance with this document, as well as DoD directives, standards, procedures and guidelines, including CJCSM 6510.01B.

7.5 INCIDENT RESPONSE PLAN REVIEW

Due to changes in technology, it is difficult to create a process that can provide a one size fits all approach to securing information systems. Performing periodic reviews of the IRP is essential. IRT members review the IR Plan on at least an annual basis but may review it more frequently based on direction received from [USCYBERCOM, NETCOM] **CCI-000848**. Updates to the IR Plan will address system/organizational changes or problems encountered during plan implementation, execution, or testing and incorporate lessons learned from past incidents **CCI-000849.** Incident response personnel (identified by name and/or by role in Section 7.4) and organizational elements subject to the AUP will be made aware of incident response plan changes within 30 days via email **CCI-000850.** The incident response plan capabilities shall be evaluated by completing an Incident Response After Action Report for each Incident/Event. (Excel file: LogSheets.xls/Incident_Event_Failure AAR log template) **CCI-002800.** When a review determines that a change is necessary, an IRT member is assigned to draft the necessary change(s) and submit it for peer review to other IRT members. [ORGANIZATION NAME] disseminates SOPs and Policy documents using [SharePoint site or other file sharing resource] and ensures protection from unauthorized disclosure and modification **CCI-002804.**

Appendix A: Security Incident Report Form

Report Classification			
Report No:		**Organization**	
Date:		**Report Type: (initial, Final)**	
Report Prepared by:		Date:	Time:
Title:	Phone:		Email:
Signature:			
SECTION 1 – POC INFORMATION			
Incident Reported by:	Name:	Date:	Time:
	Title:	Phone:	Email:
Signature:			
ISSM Notified:	Name:	Date:	Time:
Method of Notification			
	Phone:	Email:	
Signature:			
CIO Notified:	Name:	Date:	Time:
Method of Notification			
	Phone:	Email:	
Signature:			
(Other) Organization:	Name:	Date:	Time:
Method of Notification			
	Phone:	Email:	
Signature:			
Criminal Investigation Organization Notified:		Date:	Time:
Method of Notification			
	Phone:	Email:	
SECTION 2 – INCIDENT INFORMATION			
Date of Incident:	Time of Incident:		Ongoing: Yes NO
Incident Facility Name:		Incident Facility Location:	
Affected Computer Systems (Hardware and/or Software):			

Classification of Affected Computer Systems:					
Physical Location of Affected Systems:					
Connections of Affected Systems to Other Systems:					
Type of Incident please identify):	Data Destruction Or Corruption	Malicious Code	Data Spill	Privileged User Misuse	
	Security Support Structure Configuration Modification	Destruction/ Corruption/ Disabling	System Contamination	Unauthorized User Access	other

CJCSM 6510.01B Category (Source: Table B-A-1)	Precedence	Category	Description (See CJCSM 6510.01B for full description)
	0	0	Training and Exercises
	1	1	Root Level Intrusion (Incident)
	2	2	User Level Intrusion (Incident)
	3	4	Denial of Service (Incident)
	4	7	Malicious Logic (Incident)
	5	3	Unsuccessful Activity Attempt (Event)
	6	5	Non-Compliance Activity (Event)
	7	6	Reconnaissance (Event)
	8	8	Investigating (Event)
	9	9	Explained Anomaly (Event)

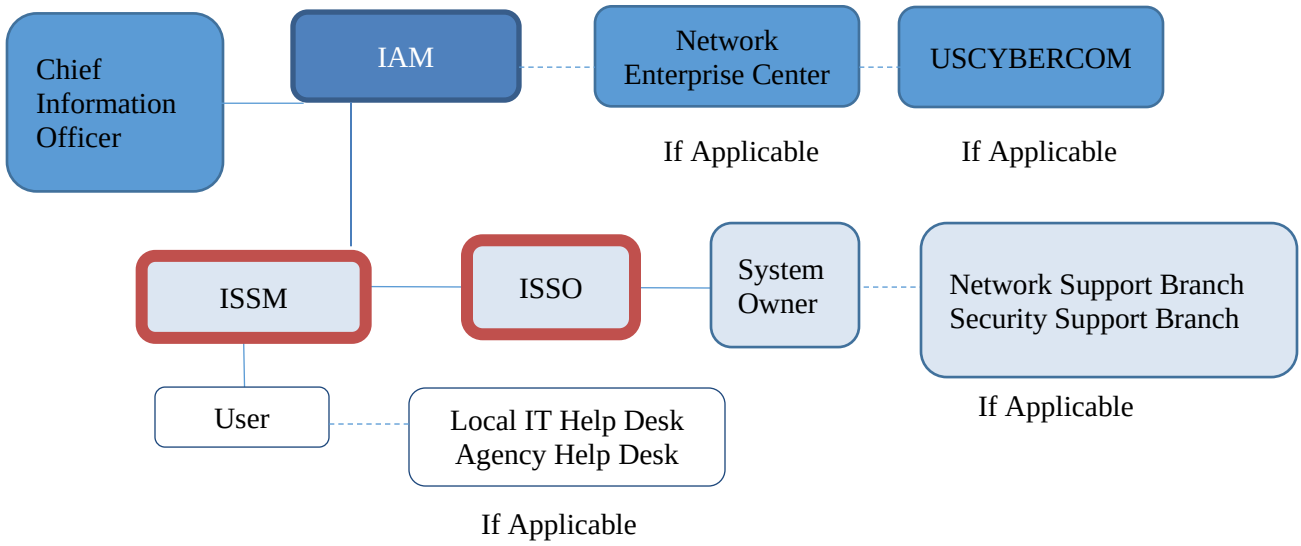
Suspected Method of Intrusion/Attack	
Suspected Perpetrator(s) or Possible Motivation(s)	
Apparent Source (e.g., IP address) of Intrusion/Attack:	
Apparent Target/Goal of Intrusion/Attack:	
Mission Impact	Success/Failure of Intrusion/Attack:

Attach technical details of incident thus far. Include as much as possible about the Detection and Identification, Containment, Eradication, and Recovery – steps taken (with date/time stamps), persons involved, files saved for analysis, etc.
2.1 Functional Impact - Identify the current level of impact on agency functions or services
NO IMPACT – Event has no impact.
NO IMPACT TO SERVICES – Event has no impact to Industrial Control Systems (ICS) services.
MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to non- critical systems and services.
MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.
DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.
NO IMPACT – Event has no impact.
Information Impact - Identify the type of information lost, compromised, or corrupted
NO IMPACT – No known data impact.
SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
PRIVACY DATA BREACH – The confidentiality of personally identifiable information or personal health information was compromised.
PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information[7], such as protected critical infrastructure information, intellectual property, or trade secrets was compromised.
DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record overwrite; have been used against a non-critical system.
CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated.
CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.
Recoverability – Identifies the scope of resources needed to recover from the incident
REGULAR – Time to recovery is predictable with existing sources
SUPPLEMENTED – Time to recovery is predictable with additional resources.
EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
Potential Impact – Identifies the number of systems, records, and users impacted

Minimal	Low	Moderate	High	Severe

Appendix B: Incident Response Team Contact Information

(Contacts and Reporting Chain provided as suggestion)



Title	Phone No	Time Available	Note
ISSM			
ISSM (Alternate)			
ISSO			
System Owner (SO)			
Information Assurance Manager (IAM)			
Chief Information Officer			
Network Enterprise Center			
Local IT Help Desk		24 x 7	
Agency/ Service Help Service Desk		24 x 7	
Network Support Branch			As needed
Security & Planning Branch			As needed

Risk Management Framework Maintenance (MA) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Maintenance (MA), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline MA Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
MA-1**	Maintenance Policy and Procedures
MA-2*	Controlled Maintenance
MA-4*	Nonlocal Maintenance
MA-5*	Maintenance Personnel
Controls for Security Impact Level: Moderate	
MA-3*	Maintenance Tools
MA-3 (1)*	Maintenance Tools (Inspect Tools)
MA-3 (2)*	Maintenance Tools (Inspect Media)
MA-4(2)*	Nonlocal Maintenance (Document Non-Logical Maintenance)
MA-6*	Timely Maintenance

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 MA Organizational Policy Controls

Broadly implemented MA policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific MA safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Controlled Maintenance (MA-2)

The [FACILITY NAME] system maintenance is separated into two general categories: scheduled and unscheduled maintenance. Scheduled maintenance includes routine activities that occur cyclically to keep the system up-to-date and remaining in a secure state.

Scheduled maintenance is performed by [the System Administrator (SA)]. The Configuration Control Board (CCB) is the oversight entity that tracks and monitors all changes made to a system. Vendor specifications will be used to develop a list of the scheduled maintenance anticipated for the coming year and this list will be presented to the CCB 30 days prior to the start of the fiscal year **CCI-002866, CCI-002870** (Excel file: LogSheets.xls/Scheduled Maintenance Template). The CCB will discuss and approve the list of anticipated scheduled maintenance and review the maintenance log from the previous year on an annual basis **CCI-002869, CCI-002873, CCI-000859**.

Unscheduled maintenance can be performed by [the SA] or a properly vetted contractor or vendor. Unscheduled maintenance due to a system malfunction must be processed through the full change request process. However, if it is determined to be an emergency, the SA can implement the changes in accordance with the emergency change management process detailed in the [FACILITY NAME] *Contingency Planning Policy and Procedures document*.

Scheduled and unscheduled maintenance activity will be recorded on a maintenance log **CCI-002867, CCI-002868, CCI-002871, CCI-002872**. Potentially impacted security controls will be tested, after maintenance is finished, to ensure maintenance did not negatively affect security or system functionality **CCI-000862.** The maintenance log will be presented to the CCB annually and will be kept for a minimum of three years. The following information will be recorded on the maintenance log (Excel file: LogSheets.xls/Maintenance Log Template) **CCI-002875, CCI-002876**:

- System component/specific identifier
- Name of personnel implementing maintenance (Name, Organization and title)
- Personnel overseeing maintenance, escort (if applicable)
- Date of maintenance - If maintenance requires more than one (1) day to implement, the date will include the date range from start to completion
- Scheduled/Unscheduled
- Onsite/Off-site
- Personnel removing system, (only applicable to off-site maintenance)
- Summary of maintenance procedure
- Validation of security control functionality following maintenance
- Special comments on procedure

On-site maintenance can be done by the [SA, O&M Support Contractor], or a contractor and/or vendor who has been properly vetted according to the requirements outlined in the Personnel Security Section of this document. Maintenance and diagnostic activities will be monitored/supervised, and potentially

impacted security controls will be reviewed by the ISSO. Any components of the [FACILITY NAME] system that requires off site maintenance will need to be sanitized and all information removed from the associated media prior to removal for off-site repairs and/or maintenance **CCI-000861**. Only [FACILITY NAME] and CCB approved personnel may remove systems for off-site repair **CCI-000860, CCI-002874**.

3. Maintenance Tools (MA-3) for Moderate Impact Level Systems

[FACILITY NAME] maintenance tools must be approved and documented within the Annual Scheduled Maintenance Summary/System Security Plan (SSP) **CCI-000865**. The [ORGANIZATION NAME] will record use of maintenance tools and procedures on the maintenance log **CCI-000866**, **CCI-000867**.

Maintenance Tools/ Inspect Tools (MA 3 (1)) for Moderate Impact level systems:

Maintenance tools must be inspected and verified prior to use. The personnel performing the inspections must be recorded on the maintenance log **CCI-000869**.

Maintenance Tools/ Inspect Media (MA-3(2)) for Moderate Impact level systems:

All media containing diagnostic and test programs will be inspected for malicious code before the media is used in the information system. The personnel performing the inspections must be recorded on the maintenance log **CCI-000870.**

4. Non-local Maintenance (MA-4)

The SSP/Annual Scheduled Maintenance Summary identify the CCB authorized non-local maintenance and diagnostic activities **CCI-000873, CCI-000876.** The [ORGANIZATION NAME] monitors and keeps records of these activities on Maintenance Logs **CCI-000874, CCI-000878**. The system is configured in accordance with applicable STIGs/SRGs to employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions and terminate sessions when maintenance is complete **CCI-000877, CCI-000879**.

Non-local Maintenance/ Document Non-local Maintenance (MA-4(2)) for Moderate Impact level systems:

[ORGANIZATION NAME] will document within the SSP any additional policies and procedures for the establishment and use of non-local maintenance and diagnostic connections **CCI-000881**.

5. Maintenance Personnel (MA-5)

There are two types of maintenance personnel for a [FACILITY NAME] system: organizational and non-

organizational. The [FACILITY NAME] CCB shall review and document maintenance personnel on the Annual Scheduled Maintenance Summary and if necessary will obtain a support contract for maintenance **CCI-000890**. A record of all personnel authorized to perform maintenance on the [FACILITY NAME] system will be recorded on the Master Authorized User Log (Excel file: LogSheets.xls/Master AUL Template) **CCI-000891.**

Organizational personnel are defined as [FACILITY NAME] employees who have been formally appointed by the SO and approved by the CCB to maintain the control system. All organizational maintenance personnel security requirements are detailed in the [FACILITY NAME] *Personnel Security Policy and Procedures document*.

Non-organizational maintenance personnel refer to anyone not employed by the [ORGANIZATION NAME] but with access to the [FACILITY NAME] system for maintenance purposes, e.g. contractor or vendor. The system specific CCB approval process for requesting system access for non-organizational maintenance personnel must be completed prior to the first day of maintenance activities. All non-organizational maintenance personnel security requirements will be completed.

All controlled areas for a [FACILITY NAME] system will have an authorized personnel access list that specifies escort requirements, as described in the [FACILITY NAME] *Physical and Environmental Policy and Procedures document*. Anyone listed as requiring an escort will be escorted by an authorized person while in the area. Organizational personnel will have access authorizations and have a technical competence commensurate with supervising maintenance activities. A record of all personnel supervising maintenance on the [FACILITY NAME] system will be recorded on the Maintenance Log (Excel file: LogSheets.xls/ Maintenance Log Template) **CCI-002894, CCI-002895**.

6. Timely Maintenance (MA-6) for Moderate Impact level systems:

Maintenance support and spare parts must be available within 24-hours. The [ORGANIZATION NAME] ensures any necessary maintenance support contracts are in place and an inventory of spare parts are available for moderate impact level systems **CCI-000903, CCI-002897**.

Risk Management Framework
Media Protection (MP)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Media Protection (MP), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline MP Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
MP-2	Media Access
MP-6	Media Sanitization
MP-7	Media Use
Additional Controls for Security Impact Level: MODERATE	
MP-3	Media Marketing
MP-4	Media Storage
MP-5	Media Transport
MP-5(4)	Cryptographic Protection
MP-7(1)	Media Use | Prohibit Use Without Owner

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 MP Organizational Policy Controls

Broadly implemented MP policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific MP safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Media Access (MP-2)

[FACILITY NAME] System information is not cleared for public release in accordance with Department of Defense Manual (DoDM) 5200.01 and [add additional guidance here]. The ISSO ensures that all system media and information is protected. The Information pertaining the [FACILITY NAME] system is considered [Sensitive]. All other information processed or stored on each [FACILITY NAME] system has been determined not be Sensitive and can be freely shared with the following entities **CCI-001003, CCI-001005:**

- [FACILITY NAME] Change Control Board (CCB) members
- Key Stakeholders
- System users
- [FACILITY NAME] personnel
- Contractors with need-to-know

When access to [FACILITY NAME] sensitive media is necessary for personnel or entities other than those listed above, a written request for release must be issued and submitted directly to the [FACILITY NAME] ISSO. The following information must be included in the written request:

- Name of individual requesting the release
- Date of request
- Sensitive media release date, when it is required
- Recipient of sensitive media
- Reason(s) for release to above recipient

The organization conducting the inspection/assessment obtains and examines the documented personnel or roles and determine if access is allowed IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. The [FACILITY NAME] ISSO will approve or disapprove the request in writing. If the request is not approved, the ISSO will explain the rationale for the denial. If approved, the ISSO will direct all activities necessary for the proper dissemination of the sensitive media as described in this document.

3. Media Marking for Moderate Impact level systems (MP-3)

Information systems media will be marked indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. [ORGANIZATION NAME] will define and exempt types of information systems from marking as long as the media remains within the [FACILITY NAME] defined controlled areas **CCI-001010, CCI-001011**.

4. Media Storage for Moderate Impact level systems (MP-4)

[ORGANIZATION NAME] physically controls and securely stores all digital and/or non-digital media within controlled areas IAW DoDM 5200.01 M Vol. 1-4. [ORGANIZATION NAME] protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures **CCI-001014, CCI-001018**.

5. Media Transport for Moderate Impact level systems (MP-5)

[ORGANIZATION NAME] protects and controls all media during transport outside of controlled areas using security safeguards IAW DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2. [ORGANIZATION NAME] will maintain accountability for information system media during transport outside of controlled areas, document activities associated with the transport of information system media and restrict activities associates with the transport of information system media to authorized personnel **CCI-001020, CCI-001023, CCI-001024, CCI-001025**.

5.1 Media Transport Cryptographic Protection (MP-5(4))

[ORGANIZATION NAME] will ensure the information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas **CCI-001027**.

6. Media Sanitation (MP-6)

Each [FACILITY NAME] system is a compilation of traditional information technology (IT) components and control system (Platform IT (PIT)) components that are Sensitive, Controlled Unclassified, FOUO). [Describe data on system that is classified]

All [FACILITY NAME] media shall be sanitized IAW the [FACILITY NAME] Service Level Agreement, and to the fullest extent possible IAW the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-88 Revision 1, using the specific system categorization defined in the System Security Plan **CCI-001028, CCI-002580**.

The [FACILITY NAME] ISSM will ensure only authorized personnel conduct sanitizations. Verification of the sanitization will be provided to the [FACILITY NAME] ISSM. For any [FACILITY NAME] media to be sanitized, the ISSM will provide the [ORGANIZATION NAME] with, the following information:

- Descriptive title and type of media OR system component name (host name) and type
- Reason for sanitization
- ISSM request and approval of sanitation process

7. Media Use (MP-7)

The use of media on each [FACILITY NAME] system is completely restricted to the system ISSM, SA, other authorized personnel as defined by the system policies and procedures. This media use policy applies to all components within the [FACILITY NAME] authorization boundary. The following polices are in place to restrict and monitor the use of media on control systems:

- [FACILITY NAME] Acceptable Use Policy
- [FACILITY NAME] Maintenance Policy and Procedures
- [FACILITY NAME] Contingency Planning Policy and Procedures

Only CCB approved maintenance tools and media, used for purposes of system maintenance or recovery, are to be used on the system **CCI-002581, CCI-002582, CCI-002583, CCI-002584**. Maintenance tools are documented in the IAW [FACILITY NAME] *Maintenance Policy and Procedures document* and are stored and protected in the IAW [FACILITY NAME] *Contingency Planning Policy and Procedures document*.

7.1 Media Use/ Prohibit Use of Sanitization-Resistant Media for Moderate Impact level systems (MP-7(1))

[ORGANIZATION NAME] will prohibit the use of portable storage devices on [FACILITY NAME] systems **CCI-002585**.

Risk Management Framework
Control System Security Program
Policies and Procedures – Overview

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Version	Date	Name	Description
1.0	08/2019		Initial Release

Approval Page

[provide multiple approval pages for each POC listed in Table 3]

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Purpose

The Security Program Policies & Procedures - Overview provides all [ORGANIZATION NAME] system stakeholders an overview of security policies and procedures (P&Ps) applicable to all Facility Related Control Systems (FRCSs). The P&Ps are organized by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" control families and apply the NIST SP 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security" ICS Overlay. The P&Ps include a policy document for each control family and cover organizational security requirements and organizational aspects of hybrid controls. The P&Ps are tailored to [ORGANIZATION NAME] systems categorized at the "Low" [and "Moderate"] impact level. These do not include security policies or procedures already covered at the DoD level (Tier 1 and Tier2). System-specific security controls and configurations are to be covered separately in system configuration guides and security documentation. Controls that have actions specific to the system are listed in Appendix A (System Specific Security Requirements List). Control Correlation Identifier (CCIs) are referenced within the text of the documents.

The [ORGANIZATION NAME] is fully committed to sustaining the cybersecurity of control systems in their purview through approval and execution of these policies & procedures, and dedicated funding for maintaining the control system components and their security posture. These policies and procedures address purpose, scope, roles, responsibilities, management commitment, compliance and coordination among stakeholders **CCI-000001, CCI-000004, CCI-000117, CCI-000120, CCI-000287 CCI-000290, CCI-000756, CCI-000760, CCI-000852. CCI-000855, CCI-000904, CCI-000908**. All unique Policy and Procedure documents are part of the artifacts included in the Authorizing Official (AO) Approved System Security Plan (SSP), located on the enterprise Mission Support Service (eMASS). Several capabilities are inherited from DoD-level policies **CCI-000100, CCI-000103, CCI-000239, CCI-000242, CCI-000438, CCI-000441, CCI-000805, CCI-000806, CCI-000809, CCI-000810, CCI-000995, CCI-000999, CCI-000563, CCI-000566, CCI-000073, CCI-001680, CCI-001037, CCI-001041, CCI-000602, CCI-000605, CCI-001074, CCI-001078, CCI-001217, CCI-001220**.

2. General Requirements

All P&Ps apply to system owners, information system security managers/officers (ISSMs/ISSOs), operators/users, or other roles who have responsibilities to develop, apply, enforce, or monitor security requirements **CCI-001825**. System-specific configurations and security control implementation guidance shall be provided in System Configuration Guides uploaded to the eMASS record for each system as artifacts. These guides which will include, at minimum, the following:

- Mapping to the NIST security control CCIs

- Hardware & Software Specifications
- Network, System, Authorization Boundary and Data Flow Diagrams
- Baseline Configurations
- Account & Password Management Procedures
- Security Log & Operational Data Download Procedures
- Backup & Recovery Procedures

Deviations to the P&Ps, NIST security controls or applicable Security Technical Implementation Guides (STIGs) or Security Readiness Guides (SRGs) for a given system must be documented as an artifact and approved by the ISSM and SO. Enhancements shall be included in the System Security Plan in eMASS. Any outstanding mitigations or remediation must be noted in a Plan of Action & Milestones (POA&M) in eMASS for each [ORGANIZATION NAME] system.

2.1 APPLICABLE CONTROL SYSTEMS

These RMF Security System Policy and Procedures apply to the [ORGANIZATION NAME] systems listed in Table 2.

Table 2– [ORGANIZATION NAME] Systems

System Name	Security Categorization	eMASS Record Number	Date Applicable
[FACILITY NAME]			

2.2 ROLES & RESPONSIBILITIES

The [ORGANIZATION NAME] has defined personnel who will facilitate the implementation of the P&Ps, including roles and responsibilities of assigned personnel. Table 3 - [ORGANIZATION NAME] Personnel and Roles identifies POCs for key DoD defined cybersecurity roles related to each of the [FACILITY NAME] Systems listed in Table 2.

These roles make up the Configuration Control Board (CCB) for each control system. The CCB is group of stakeholders responsible for evaluating and approving/disapproving proposed changes to control systems. More detailed configuration management (CM) policies and procedures are included in the CM policy artifact **CCI-000290**. Appointment orders for each key role shall be maintained in eMASS as artifacts. A list of high-level responsibilities for each key role is provided below Table.

Table 3 - [ORGANIZATION NAME] Personnel and Roles

Title	Point of Contact	Contact Information
SYSTEM NAME: [FACILITY NAME]		
System Owner (SO)		
System Administration (SA)		
Information System Security Office (ISSO		
Information System Security Manager (ISSM)		
Account Manager		
SYSTEM NAME:		
System Owner (SO)		
System Administration (SA)		
Information System Security Office (ISSO		
Information System Security Manager (ISSM)		
Account Manager		

SYSTEM OWNER

- Chairman of the CCB
- Ensures control systems are compliant with the security posture of the security policies and procedures
- Establishes and standardizes the configuration management tools used across control systems

ISSM

A checklist summarizing on-going actions and ISSM responsibilities for system security and RMF package maintenance is provided in Appendix B (On-going Security Control Checklist). Specific details regarding these actions are summarized in the P&Ps specific to each NIST control family. Additional responsibilities include:

- Assembles CCB and manages baseline configurations
- Supports the Information Assurance Manger to provide additional information on changes of IA regulations
- Maintains the security documentation for the control system
- Performs security audits using approved DoD tools and method
- Documents any changes or deviations from the previously approved security baseline and report to ISSO

ISSO

- Authorizes the establishment of baselines and configuration items, lists, and diagrams
- Authorizes any changes to configuration items or baselines
- Authorizes personnel access to the control system, both organizational and non-organizational
- Represents the interests of all groups who may be affected by changes to the baselines
- Communicates decisions and happenings to all groups who may be affected by changes
- Analyzes and determines security impacts of proposed changes prior to implementation
- Approves, disapproves, or defers proposed system changes
- Sets timelines for enhancements and changes to the baseline

- Determines personnel authorized to implement approved changes
- Ensures implementation of approved changes
- Establishes and maintains system documentation to represent current system configuration status

Account Manager

- Review user accounts monthly to ensure passwords are changed every 60 days
- Review information system accounts at least annually for compliance with account management requirements.
- Review of the privileges assigned to organization-defined roles or classes of users annually

2.3 POLICY DISSEMINATION AND REVIEW

These P&Ps and baseline configurations will be maintained by the SO in coordination with vendors, as needed (**CCI-000117, CCI-000120 CCI-000852, CCI-000855)** and will be disseminated to all personnel accessing, operating or maintaining the system, including the SO, Information System Security Manager (ISSM), Information System Security Officer (ISSO) **CCI-000002, CCI-000005; CCI-001930, CCI-001931, CCI-001832, CCI-001834, CCI-000242, CCI-001825, CCI-000853, CCI-000856, CCI-002378, CCI-002380, CCI-000287.** In addition, personnel responsible for infrastructure management, including disaster recovery and contingency operations of the control system infrastructure, will also receive copies of the applicable P&Ps **CCI-000459**. These documents will also be available to authorized users on the internal Garrison SharePoint site, accessible from a properly configured workstation.

The P&Ps shall be included as artifacts of control system records in eMASS **CCI-000001, CCI-000004, CCI-000287.** These P&Ps will be reviewed at least annually and updated as required by DoD policy **CCI-000003, CCI-000006, CCI-000119, CCI-000122, CCI-001822, CCI-000289, CCI-000292; CCI-000462, CCI-000457, CCI-000466, CCI-000468, CCI-000497, CCI-000463, CCI-000464, CCI-000465, CCI-000854, CCI-000857, CCI-000244.**

Considerations for additional review of the P&Ps include the following:

- System technology or configuration updates/changes
- Organizational/operational environment changes
- Risk level change
- Changes in governance or policies
- Cyberattack, security event

- Tactical orders/directives

Upon completion of any P&Ps review, the documents will be saved as a .pdf file and re-signed by key stakeholders to prevent unauthorized modification **CCI-002832.** If revisions or updates are made to the documents, the revision number, revision date, individual or group responsible for the revision, and revision description and detail of the change must be annotated in Table 1 - Revision History. The updated documents will then be re-distributed to the all personnel accessing or operating [ORGANIZATION NAME] systems upon completion of update.

3. References

The references used throughout these Policy & Procedures are listed below. In addition, a list of acronyms and abbreviations used throughout the documents is provided in Appendix C.

a. CNSSI 1253, “Security Categorization and Control Selection for National Security Systems”, 27 Mar 2014.

b. CJCSM 6510.01B, "Cyber Incident Handling Program," 10 Jul 2012.

c. DoD Directive 8140.01, Cyberspace Workforce Management, 11 Aug 2015.

d. DoD Directive 8570.01-M, “Information Assurance Workforce Improvement Program”, Nov 2015, as amended.

e. DOD Instruction 3020.41 “Operational Contract Support (SCS):, 11 Apr 2017, as amended.

f. DoD Instruction 8510.01, “Risk Management Framework”, 12 Mar 2014.

g. DoD Manual 5200.01, “DoD Information Security Program, 24 Feb 2012.

h. DoD Manual 5200.02, “Procedures for the DoD Personnel Security Program (PSP),” 03 Apr 2017, replacing DoD 5200.2-R “Personnel Security Program,” Jan 1987, authorized by DoD Directive 5200.2, Dec 20, 1979.

i. DoD 5220.22-R, “Industrial Security Regulation”, 04 Dec 1985.

j. DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM),” 28 Feb 2006, as amended.

k. DoD 5500.7-R, “Joint Ethics Regulation (JER),” 17 Nov 2011, as amended.

l. FIPS PUB 200, “Minimum Security Requirement for Federal Information and Information Systems, U.S. Dept. of Commerce, Mar 2006.

m. Information Assurance Support Environment (IASE) website from the Defense Information Systems Agency (DISA) (https://iase.disa.mil/Pages/index.aspx).

n. NIST (SP) 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems”, Feb 2010.

o. NIST (SP) 800-53, “Security Controls and Assessment Procedures for Federal Information Systems and Organizations,” Apr 2013, as amended.

p. NIST (SP) 800-82 revision 2, “Guide to Industrial Control Systems (ICS) Security”, May 2015, as amended.

q. NIST (SP) 800-88, “Guidelines for Media Sanitation”, Sep 2006.

r. NIST (SP) 800-128, “Guide for Security-Focused Configuration Management of Information Systems”, Aug 2011.

s. UFC 4-010-06, “Cybersecurity of Facility-Related Control Systems”, 18 Jan 2017 as amended.

Appendix A: System Specific Security Requirements List

This list summarizes system-specific security controls addressed in separate documents and during the configuration of the system.

System Specific Security Requirements List

Control Number (NIST	CCI-#	Control Name	Documentation/Explanation	Impact Level	Other Supporting Documentation Required
AC-2	CCI-002122 CCI-002126, CCI-002127, CCI-002128	Account Management	Establish rules for access authorization and monitoring accounts and implement automated mechanisms to support management of information based on assigned role(s)	low	Tailor Policy document Applicable STIG/SRG checks
AC-2	CCI-002110, CCI-002117, CCI-002118, CCI-002119	Account Management	Assign user role(s); each role has permissions which allow or restrict user actions based upon the role's intended role or system function required for system operation	low	Applicable STIG/SRG checks
AC-2(1)	CCI-000016		define automated mechanisms to support the management of system account	mod	Applicable STIG/SRG checks
AC-2(2)	CCI-000016, CCI-001682; CCI-001361, CCI-001368	Account Management	Configure system to automatically remove or disable temporary accounts after DoD defined time period of 72-hours. Configure system to never automatically remove or disable emergency accounts.	mod	Applicable STIG/SRG checks
AC-2(3)	CCI-000017, CCI-000217	Account Management	Configure system to automatically disable inactive accounts after DoD defined time period of 35 days.	mod	Applicable STIG/SRG checks
AC-2(4)	CCI-000018, CCI-001403, CCI-001404, CCI-001405, CCI-001683, CCI-001684, CCI-001685, CCI-001686, CCI-002130, CCI-002132	Account Management	Configure system to automatically audits the following account actions: Creation, modification, Disabling, Removal. Configure the system to notify the system administrator and ISSO if these actions occur	mod	Applicable STIG/SRG checks
AC-3	CCI-000213	Access Enforcement	Define Access Control Policies. Develop Standard Mandatory Notice and Consent and Acceptable Use Policy; Obtain signature for authorized users; Configure system to enforce approved authorizations for logical access to system resources in accordance with applicable access control policies.	low	Standard Mandatory Notice and Consent and Acceptable Use Policy (draft provided in AC Appendix A&B) Authorized User List (template Provided)
AC-4	CCI-001368, CCI-001414, CCI-001548, CCI-001549, CCI-001550, CCI-001551	Information Flow Enforcement	Define Information on flow control policies and approve authorization boundaries and controlling the flow of information within the system. Configure system to enforce approved authorizations for controlling the flow of information within the system based on information flow control policy	mod	Applicable STIG/SRG checks Configuration documentation Data Flow diagram
AC-6	CCI-000225	Least Privilege	Configure system to limit access to Users to accomplish assigned tasks in accordance with missions and business functions to ensure that all system users require limited access for approved job functions	mod	Applicable STIG/SRG checks
AC-6(1)	CCI-002221, CCI-002222, CCI-002223, CCI-001558	Least Privilege-authorized access	Configure system to limit access to all security-relevant information not publicly available; This control should be included with features of AC-6(2) and (5)	mod	Applicable STIG/SRG checks
AC-6(2)	CCI-000039, CCI-001419	Least Privilege-non-privileged access	Configure system to provide two types of accounts to authorized users: privileges and non-privileged. Users must use privileged account to access privileged security functions/information and use non-privileged accounts when accessing non-security functions/information	mod	Applicable STIG/SRG checks
AC-6(5)	CCI-002226, CCI-002227	Least Privilege-privileged accounts	[ISSO and the SO] will define and document personnel and roles of privileged account users.	mod	Authorized User List (template Provided)

AC-6(9)	CCI-002234	Least Privilege-auditing	Configure system to audit the execution of privileged functions	mod	Applicable STIG/SRG checks Configuration documentation
AC-6(10)	CCI-002235	Prohibit Non-privileged Users from Executing Privileged Functions	The system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	mod	Applicable STIG/SRG checks Configuration documentation
AC-7	CCI-000043, CCI-000044, CCI-001423, CCI-002236,	System Use Notifications	Configure system to enforce limit of consecutive invalid logon attempts by a user; DoD has defined the maximum number as three. DoD has defined the time period as 15 minutes.	low	Applicable STIG/SRG checks Configuration documentation
AC-7	CCI-002237, CCI-002238	System Use Notifications	Configure system to automatically lock the account or node for defined time period; DoD has defined the delay algorithm as a minimum of 5 seconds. DoD has defined the time period as until released by an administrator.	low	Applicable STIG/SRG checks Configuration documentation
AC-8	CCI-000048; CCI-002243 to CCI-002248	System Use Notifications	Configure system to display the DoD systems – Standard Consent Banner and User Agreement before granting access to the system	low	Applicable STIG/SRG checks Configuration documentation
AC-8	CCI-000050	System Use Notifications	Configure system to retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access	low	Applicable STIG/SRG checks Configuration documentation
AC-11	CCI-000056, CCI-000058, CCI-000059	Session Lock	Configure system to retain the DoD required session lock until the user reestablishes access using established identification and authentication procedures. DoD defined the time period as 15-min	mod	Applicable STIG/SRG checks Configuration documentation
AC-11 (1)	CCI-000060	Session Lock-Pattern Hiding Display	Configure system to conceal, via the session lock, information previously visible on the display with a publicly viewable image.	mod	Applicable STIG/SRG checks Configuration documentation
AC-12	CCI-002360, CCI-002361	Session Termination	Configure system to automatically terminate a user session after [organization-defined conditions or trigger events]	mod	Applicable STIG/SRG checks Configuration documentation
AC-14	CCI-000061, CCI-000232	Permitted Actions without Identification or authentication	Identify actions that can be performed without identification or authentication.	low	Tailor Policy Document Applicable STIG/SRG checks
AC-17	CCI-000063, CCI-000065, CCI-002310, CCI-002311, CCI-002312	Remote Access	Only applicable if remote access is allowed. Define usage restrictions if remote access is allowed. Configure system based on defined restrictions	low	Applicable STIG/SRG checks Tailor Policy document, as needed
AC-17(1)	CCI-000067, CCI-002314	Remote Access-Automated Monitoring/Control	Only applicable if remote access is allowed. Configure the system to control and monitor remote access connections	mod	Applicable STIG/SRG checks
AC-17(2)	CCI-000068, CCI-001453	Remote Access-Protection of Confidentiality	Only applicable if remote access is allowed. Configure the system to implement cryptographic mechanisms to protect the integrity of remote access sessions	mod	Applicable STIG/SRG checks
AC-17(3)	CCI-000069, CCI-001561, CCI	Remote Access-Managed Control Points	Only applicable if remote access is allowed. Configure the system to route all remote accesses through the number of [defined] managed network access control points	mod	Applicable STIG/SRG checks Approved Network diagram
AC-17(4)	CCI-000070, CCI-002316, CCI-002318, CCI-002319, CCI-002320	Remote Access-Privileged Commands	Only applicable if remote access is allowed. The security plan documents the rational for remote operational needs requiring remote access;	mod	System Security Plan Tailor Policy document, as needed

AC-18	CCI-001438, CCI-001439, CCI-001441, CCI-002323	Wireless Access	Only applicable if wireless access is allowed. Define usage restrictions if wireless access is allowed. Configure system based on defined restrictions	low	Applicable STIG/SRG checks Tailor Policy document, as needed
AC-18(1)	CCI-001443, CCI-001444	Wireless Access	Only applicable if wireless access is allowed. Configure the system to protect wireless access to the system using authentication of users and/or devices and using encryption.	mod	Applicable STIG/SRG checks Tailor Policy document, as needed
AC-19	CCI-000082, CCI-000083, CCI-000084, CCI-002326	Mobile Devices	Only applicable if mobile access is allowed. Define usage restrictions and connection requirements if mobile access is allowed. Configure system based on defined restrictions	low	Applicable STIG/SRG checks Tailor Policy document, as needed
AC-19 (5)	CCI-002329, CCI-002330, CCI-002331	Mobile Devices	Only applicable if mobile access is allowed. Ensure authorized mobile devices employ full-device or container encryption	mod	Tailor Policy document, as needed Make and Model of authorized mobile devices
AC-20	CCI-000093, CCI-002332.	External Connections	Only applicable if external connection is allowed. Draft a Service Level Agreement (SLA)] to define terms and conditions for external connections; Configured system to permit external access to the system only when it consistent with the SSP	low	Service Level Agreement or Memorandum of Understanding for External connections
AC-21	CCI-000098, CCI-001470, CCI-001471, CCI-001472	Information Sharing	Only applicable if information sharing is allowed. Define usage restrictions, user discretion guidance and automated methods to allow information sharing.	low	Tailor Policy document, as needed
AC-22	CCI-001474 to 001478	Public Access	Only applicable if public access is allowed.	low	Tailor Policy document, as needed
AU-2	CCI-000123 CCI-000125	Audit Events	The system must be capable of auditing an organization-defined list of auditable events.	low	Sample audit log (000123) Sample of after-action investigations of security event (000125)
AU-3	000130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487	Content of Audit Records	System audit logs will be configured to comply with applicable STIG/SRG guidance; Detailed requirements listed in NIST 800-53	low	Applicable STIG/SRG checks Configuration documentation
AU-3(1)	CCI-000135	Content of Audit Records	System audit logs will be configured to comply with applicable STIG/Security Requirement Guide (SRG) guidance and as defined by organization.	mod	Applicable STIG/SRG checks Configuration documentation
AU-4	CCI-001848, CCI-001849	Audit Storage Capacity	For system components that have applicable STIGs or SRGs, the organization evaluates the components to ensure that the system is configured in compliance with the applicable STIGs and SRGs. Sufficient capacity to store copied audit records must be available.	low	Applicable STIG/SRG checks Configuration documentation Documentation that shows the system provides a warning when allocated audit record storage volume reaches a maximum
AU-4 (1)	CCI-001851	Audit Storage Capacity - Transferee to Alternate Storage	Components will off-load audit records at a minimum, in real-time for interconnected systems and weekly for stand-alone systems onto a different system or media	low	Applicable STIG/SRG checks Configuration documentation
AU-5	CCI-000139, CCI-000140, CCI-001490	Audit Processing Failure	The system must be configured to alert at a minimum, the ISSM/ISSO in the event of an audit processing failure and in accordance with applicable STIGs or SRGs. Detailed requirements listed in NIST 800-53	low	Applicable STIG/SRG checks Configuration documentation
AU-7	CCI-001875 through CCI-001882	Audit Reduction and Report Generation	Provide an audit reduction capability that support a) on-demand audit review/analysis and b) reporting. Detailed requirements of audit records are listed in NIST 800-53. Ensure the audit reduction capabilities do not alter the original content or time ordering of audit records.	mod	Audit reduction capability system logs Applicable STIG/SRG checks Configuration documentation
AU-7(1)	CCI-000158	Audit Reduction and Report Generation	Provide the capability to process audit records for events of interest based on audit fields within audit records	mod	Audit reduction capability system logs Applicable STIG/SRG checks Configuration documentation

AU-8	CCI-000159, CCI-001889, CCI-001890	Time Stamps	Configure system to record time stamps for audit records through use of internal system clock, that meets one second granularity of time measurement. Time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	low	Applicable STIG/SRG checks Configuration documentation
AU-8 (1)	CCI-001891, CCI-002046	Time Stamps	Configure the system to synchronize internal system clocks every 24 hours for networked systems with an authoritative time server which is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DoD network (NIPRNet / SIPRNet) and/or the Global Positioning System (GPS).	mod	Applicable STIG/SRG checks Configuration documentation
AU-9	CCI-000162, CCI-000163, CCI-000164, , CCI-001493, CCI-001494	Protection of Audit Information	The audit records in the system must be protected from unauthorized access, modification or deletions	low	Configure time management system Applicable STIG/SRG checks
AU-12	CCI-000169, CCI-000171, CCI-000172, CCI-001459, CCI-001910	Audit Generation	System must be configured to provide audit record generation capability for all system and network components and allows authorized personnel to specify the audit events.	low	Tailor Policy document List of system components that provide audit record generation capability List of individuals appointed by ISSM that can select/modify audit records (as needed)
CA-2(1)	CCI-000255, CCI-002063	Security Assessment - Independent Assessors	Develop a System Security Plan (SSP) for each system. An independent assessors or assessment teams will be employed to conduct a security control assessment of the system.	mod	System Security Plan (SSP) Independent assessment team designation
CA-3	CCI-000257, CCI-000258 and CCI-000260	system Connections	Interconnection to "other" systems documented on approved design (as needed) 1) Signed and dated MOU, MOA and/or Interconnection Security AgreementsCCI-000257 2) Signed and dated network diagramCCI-000258 andCCI-000260	low	Approved Network Diagram, Interconnection Security Agreements
CA-3 (5)	CCI-000274, CCI-002087	External Connections System Interconnections - Restrictions on External System Connections	1) Configure system to employ a deny-all, permit by exception policy and detail in system configuration guide and/or STIG checklists. CCI-002080 2) Signed and dated SOP/TTP documenting the (reference exception to policy section) configuration of systems to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external systems.	mod	Configuration documentation
CA-7	CCI-000274, CCI-000280, CCI-002087	Continuous Monitoring	Develops a Continuous Monitoring Strategy with metrics CCI-000274 andCCI-002087	low	Tailor Continuous Monitoring Strategy
CA-7(1)	CCI-000282, CCI-002085	Continuous Monitoring	Employ assessors or assessment teams to monitor the security controls in the system on an ongoing basis Define the level of independence the assessors or assessment teams must have to monitor the security controls in the system on an ongoing basis CCI-000282	mod	Tailor Continuous Monitoring Strategy Assign independent assessors
CA-9	CCI-002101 through CCI-002105	Internal System Connections	Internal connections documented on approved design (as needed).	low	Approved Network Diagram Tailor Policy document

CM-2	CCI-000293	Baseline Configuration	Establish baseline configuration for each device and obtain approval from Configuration Control Board Establish Configuration Control Board Charter	low	Software list Hardware list Ports, Protocols, and Services list (baseline) System architecture Network topology Maintenance tool list Spare components list Configuration Control Board Charter?
CM-2(1)	CCI-000298	Baseline Configuration-Review and Update	Review and update the baseline configuration of the information system as an integral part of information system component installation.	mod	Software list Hardware list Ports, Protocols, and Services list (baseline) System architecture Network topology Maintenance tool list Spare components list Configuration Control Board Charter?
CM-2 (7)	CCI-001737, CCI-001738	Baseline Configuration - high risk areas	Identify devices that are located in high-risk areas or locations of concern and additional configuration for these devices.	mod	Approved Hardware List; Tailor Policy document with additional details regarding devices
CM-2 (7)	CCI-001739, CCI-001815, CCI-001816.	Baseline Configuration - mobile devices	Identify devices that are mobile; For example, devices such as notebook computers that may be mobile require additional hardening, limited applications or safeguards to sanitize hard drives prior to removal. Assumed Not Applicable for FRCS	mod	Approved Hardware List; Tailor Policy document with additional details regarding devices
CM-3	CCI-000314, CCI-000319, CCI-000320, CCI-000321, CCI-001740, CCI-001741	Configuration Change Control	When configuration change is needed; provide revised configuration for each device reviewed and approved by CCB	mod	Revised baseline configuration (as needed) Configuration Change Log (template provided)
CM-3(2)	CCI-000327	Configuration Change Control (Test/Validate/Document Changes)	When configuration change is needed; test change prior to implementation and document (as required by CCB)	mod	Configuration Change Request Form/Log
CM-4	CCI-000333	Security Impact Analysis	When configuration change is needed; Security Impact Analysis must be done by CCB	low	Configuration Change Request Form/Log
CM-5	CCI-000338, CCI-000339, CCI-000340, CCI-000341, CCI-000342, CCI-000343, CCI-000344, CCI-000345	Access Restrictions associated with Configuration Change	When configuration change is needed; physical and logical access restrictions to system/enclave are identified and implemented based on IT/Enclave system review	mod	Configuration Change Request Form/Log
CM-6	CCI-000366, CCI-000363, CCI-000367, CCI-000368, CCI-000369	Configuration Settings	Implement the security configuration settings in accordance with applicable STIG/SGRs. Identify and document deviations in POAM	low	Applicable STIG/SRG checks Configuration documentation POAM

CM-7	CCI-000380, CCI-000381, CCI-000382	Least Functionality	Configure system to provide only essential capabilities by prohibit or restrict the use of unused functions, ports, protocols, and/or services. Ensure unnecessary functions, ports, protocols, and services are disabled	low	Approved Ports Protocol Service List Approved Hardware List Approved Software List Applicable STIG/SRG checks
CM-7(1)	CCI-001761, CCI-001762	Least Functionality	Configure system to provide only essential capabilities by prohibit or restrict the use of unused functions, ports, protocols, and/or services. Ensure unnecessary functions, ports, protocols, and services are disabled	low	Approved Ports Protocol Service List Approved Hardware List Approved Software List Applicable STIG/SRG checks
CM-7 (2)	CCI-001592, CCI-001763, CCI-001764	Prevent Program Execution	Configure system to implement rules and restrictions for software program usage Ensure that all network capable software programs are DoDI 8551.01 compliant and that the rules authorizing the use of all other programs are defined	mod	Approved Software List Applicable STIG/SRG checks
CM-7 (5)	CCI-001772, CCI-001773, CCI-001774, CCI-001775	Least Functionality - Whitelisting	Configure the system to prevent the execution of programs not authorized	mod	Approved Software List
CM-8	CCI-000389, CCI-000392, CCI-000395, CCI-000399	system Component Inventory	Document inventory of system components.	low	Approved Hardware List
CM-8(5)	CCI-000419	system Component Inventory	Ensure components are not duplicated across systems	mod	Approved Hardware List
CM-9	CCI-001796, CCI-001798	Configuration Management Plan	Develop a Configuration Management Plan guidelines for implementing configuration management of systems with identified configuration items, throughout the life-cycle of the system	mod	Tailor Configuration Management Plan; Tailor Policy for unique requirements for moderate Level systems
CM-10	CCI-001732, CCI-001733 CCI-001730, CCI-001731	Software Usage Restrictions Peer to peer block	Software documentation and licenses must be tracked by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) Identify peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Examples include: P2P ports being blocked by firewall or restrictions on peer-to-peer file sharing technology.	low	Software license documentation (as needed) Peer to Peer ports blocked (documentation as applicable)
CP-2	CCI-000445, CCI-000446, CCI-000447, CCI-000448, CCI-000449, CCI-000450, CCI-000452, CCI-000454, CCI-000456	Contingency Plan	Develop a Disaster Recovery Plan (DRP) that addresses system restoration without deterioration of the security safeguards originally planned and implemented; Identify essential missions (if applicable); DRP should address recovery objectives, restoration priorities, metrics, coordination with other entities and contact information for key personnel	low	Disaster Recovery Plan; Contingency Plan tailoring
CP-2(1)	CCI-000469	Coordinate with Related Plans	Coordinates contingency plan development with organizational elements responsible for related plans	mod	Memorandum of Understanding with external entities (as needed) Tailor Policy document
CP-2(3)	CCI-000475, CCI-000476	Resume Essential Mission/Business Function	Document the plan to resume of essential missions/business functions within 12 hours (moderate) or 1-hour (high) (if applicable);	mod	Memorandum of Understanding with external entities (as needed) Tailor Policy document
CP-2(8)	CCI-002828	Identify Critical Assets	Identify critical system assets supporting mission/business essential functions (if applicable)	mod	List of critical assets Tailor Policy document

CP-3	CCI-000486	Contingency Training	List of contingency personnel and provide initial contingency training, within 10 working days of assuming a contingency role or responsibility.	low	ISSO provide and document initial training of key personnel Tailor Policy document to list key personnel
CP-4	CCI-000492	Contingency Plan Testing	Define contingency plan tests to be conducted	low	List of assets that require contingency testing; Tailor Policy document
CP-4(1)	CCI-000498	Coordinate with Related Plans	Coordinate contingency plan tests with organizational elements	mod	Memorandum of Understanding with external entities (as needed)
CP-6	CCI-000505, CCI-002836	Alternate Storage Site	Establishes an alternate storage site to permit the storage and retrieval of system backup information; alternate storage site provides information security safeguards equivalent to that of the primary site; including necessary agreements to implement	mod	Signed agreement(s) with alternate storage site
CP-6(1)	CCI-000507	Alternate Storage Site-Separation from Primary Site	Alternate storage site must be separate from primary system site to ensure alternate site not susceptible to the same threats that exist at the primary site	mod	Tailor Contingency Plan
CP-6(3)	CCI-000509, CCI-001604	Alternate Storage Site-Accessibility	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	mod	Tailor Contingency Plan
CP-7	CCI-000513, CCI-000514, CCI-000515, CCI-000521, CCI-002839	Alternate Processing Site	Establish an alternate processing site to permit the transfer and resumption of necessary system operations for essential mission/business function; alternate processing site requirements are listed in NIST 800-53	mod	Signed agreement(s) with alternate processing site
CP-7(1)	CCI-000516	Alternate Processing Site-Separation from Primary Site	Alternate processing site must be separate from primary system site to ensure alternate site not susceptible to the same threats that exist at the primary site	mod	Tailor Contingency Plan
CP-7 (2)	CCI-000517, CCI-001606	Alternate Processing Site-Accessibility	Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.	mod	Tailor Contingency Plan
CP-7 (3)	CCI-000518	Alternate Processing Site-Priority of Service	Develop priority-of-service provisions with alternate processing site	mod	Signed agreement(s) with alternate processing site Tailor Contingency Plan
CP-8	CCI-000524, CCI-000525, CCI-002840, CCI-002841	Telecommunication Services	Establishes an alternate telecommunication services; Define the time period when primary telecommunication capabilities are unavailable at the primary site to permit transfer to the alternative service	mod	Signed agreement(s) with alternate telecommunication services
CP-8(1)	CCI-000527, CCI-000528, CCI-000529	Telecommunication Services-Priority of Service	Develops alternate telecommunications service agreements that contain priority-of-service provisions	mod	Signed agreement(s) with telecom service Tailor Contingency Plan
CP-8(2)	CCI-000530	Telecommunication Services-Single Point of Failure	Alternate telecommunications services must reduce the likelihood of sharing a single point of failure with primary telecommunications services	mod	Tailor Contingency Plan
CP-9	CCI-000535, CCI-000537	System Backup	Specific system backup procedures will be documented in System Configuration Guides	low	Applicable STIG/SRG checks Configuration documentations

CP-10	CCI-000550, CCI-000551, CCI-000552	System Recovery and Reconstitution	Specific recovery and reconstitution procedures to a known state after a compromise or failure are documented in System Configuration Guides	low	System Configuration - Recovery procedures
CP-10(2)	CCI-000553	System Recovery & Reconstitution-Transaction Recovery	Implement transaction recovery for systems that are transaction-based	mod	System Configuration - Transaction based recovery procedures
CP-12	CCI-002855, CCI-002856, CCI-002857	Safe mode	Define conditions to enters a safe mode of operation; Define process to enter safe mode of operation and configure system Define restrictions on safe mode of operation;	low	System Configuration - Safe mode
IA-2	CCI-000764	I&A (Organizational Users)	configure the system to uniquely identify and authenticate organizational users	low	Applicable STIG/SRG checks
IA-2(1)	CCI-000765	Network Access to Privileged Accounts	Configure the system to implement multifactor authentication for network access to privileged accounts.	low	Applicable STIG/SRG checks
IA-2(2)	CCI-000766	Network Access to Non-Privileged Accounts	Configure the system to implement multifactor authentication for network access to non-privileged accounts.	mod	Applicable STIG/SRG checks
IA-2(3)	CCI-000767	Local Access to Privileged Accounts	Configure the system to implement multifactor authentication for local access to privileged accounts.	mod	Applicable STIG/SRG checks
IA-2(8)	CCI-001941	Network Access to Privileged Accounts – Replay Resistance	Configure the system to implement replay-resistant authentication mechanisms for network access to privileged accounts.	mod	Applicable STIG/SRG checks
IA-2(11)	CCI-001948, CCI-001949, CCI-001951, CCI-001952	Remote Access-Separate Device	Configure the system to implementation of multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separated from the system gaining access and the device meets Federal standards for authentication such as FIPS 140-2, NIAP Certification, or NSA approval	mod	Applicable STIG/SRG checks
IA-2(12)	CCI-001953, CCI-001954	Acceptance of PIV Credentials	Configure the system to accepts and electronically verifies Personal Identity Verification (PIV) credentials	low	Applicable STIG/SRG checks
IA-3	CCI-000777, CCI-000778, CCI-001958	I&A (Device)	Defined list of specific and/or types of devices to allow local, remote, or network connection; DoD has defined the types of devices as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs).	low	System Configuration STIG/SRG List of mobile devices and network connected endpoint devices Tailor Policy document
IA-3(1)	CCI-001967	Cryptographic Bidirectional Authentication	Configure the system to authenticates defined devices before establishing a local, remote and/or network connection using bidirectional authentication that is cryptographically based.	mod	Applicable STIG/SRG checks
IA-3(4)	CCI-001965, CCI-001966, CCI-001968, CCI-001969	Device Attestation	Configure the system to ensure device authentication based on attestation	mod	System Configuration

IA-4	CCI-000795	Identifier Management	Configuration system to ensure that identifiers are disabled after 35 days of inactivity	low	Applicable STIG/SRG checks
IA-4	CCI-001971	Identifier Management	The [ISSO or ISSM] manage system identifiers by selecting an identifier that identifies an individual, group, role and preventing reuse of identifiers for one year	low	System Configuration
IA-5	various	Authentication Management	Assigning, revoking and monitoring the account(s) and password(s).	low	Tailor Policy document Master AUL List Template
IA-5	various	Authentication Management	ISSM will confirm that the user has met all of the DoD IA baseline certification prerequisites (i.e. training, background check, etc.) and will notify Account Manager that password must be assigned.	low	Tailor Policy document Master AUL List Template
IA-5	CCI-000176, CCI-001544, CCI-001982, CCI-001989, CCI-002366	Authentication Management	Configure system to ensure that authenticators have 1) sufficient strength authenticators, 2) are changing/refreshing in accordance in accordance with DoD policy 3)authenticators by changing default content of authenticators, 4) changed after initial login and 5) not disclosed by system	low	Applicable STIG/SRG checks Configuration Settings for PW management
IA-5(1)	CCI-000192 to CCI-000200 CCI-000205, CCI-002041 CCI-001611 to CCI-001619	Password-Based Authentication	Configure system to enforce DoD required password complexity (upper case, lower case, numeric, special characters, length); password restrictions; cryptographic protection; password reuse; establish temporary password for initial logon that requires immediate change to permanent password	low	Applicable STIG/SRG checks
IA-5(2)	CCI-000185, CCI-000186, CCI-000187, CCI-001991	PKI-Based Authentication	Configure the system to validates PKI-based authentication in accordance with RFC 5280 and DD-2842 (more detail in NIST 800-53)	mod	Applicable STIG/SRG checks
IA-5(3)	CCI-001992 through CCI-001995	In-Person or Trusted Third-Party Registration	Identify In-Person or Trusted Third-Party Registration; DoD PKI RA–LRA CPS defines the nomination process for DoD PKI RAs	mod	Tailor Policy document
IA-5(11)	CCI-002003	Hardware Token-Based Authentication	Configure the system to accept only DoD-approved PKI credentials IAW DoDI 8520.02 and DoDI 8520.03; token-based authentication, employs mechanisms that satisfy organization-defined token quality requirements.	low	Applicable STIG/SRG checks
IA-6	CCI-000206	Authenticator Feedback	Configure the system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	low	Applicable STIG/SRG checks
IA-7	CCI-000803	Authenticator Feedback	Configure the system to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	low	Applicable STIG/SRG checks
IA-8	CCI-000804	Cryptographic Module Authentication	Configure the system to uniquely identifies and authenticates non-organizational users (if applicable)	low	Applicable STIG/SRG checks
IA-8(1)	CCI-002009, CCI-002010	I&A (Non-Organizational Users)	Configure the system to validate DoD-approved external PKI PIV credentials to authenticate federal agency users in accordance with RFC 5280. (if applicable)	low	Applicable STIG/SRG checks
IA-8(2)	CCI-002011	Acceptance of PIV Credentials from Other Agencies	Configure the system to accept Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. (if applicable)	low	Applicable STIG/SRG checks

IA-8(3)	CCI-002012	Acceptance of Third-Party Credentials	Configure the system to employ only Federal Identity, Credential, and Access Management (FICAM)-approved system components (if applicable).	low	Applicable STIG/SRG checks
IA-8(4)	CCI-002013	Use of FICAM-Issued Profiles	Configure the system to conform to Federal Identity, Credential, and Access Management (FICAM)-issued profiles.	low	Applicable STIG/SRG checks
IR-2	CCI-000813	Incident Response Training	Complete the Incident Response training requirements for and Incident Response Team members within 30 working days of being appointed to the IRT.	low	Training documentation
IR-3	CCI-000818	Incident Response Testing	Develop an Incident Response Plan to test the incident response capability for the system on an annually basis for moderate level systems (bi-annual basis for high level systems).	mod	Incident Response Test Plan Tailor Policy document
IR-3(2)	CCI-002780	Incident Response Testing - Coordination	Develop an Incident Response Plan to test the incident response capability for the system. IR Test plan must document the necessary support and coordination expected from all elements involved in Incident Response.	mod	Incident Response Test Plan Tailor Policy document
IR-4	CCI-000822	Incident Response Handling	Develop an Incident Response Handling Process. Consider critical and mission essential systems and networks in the process.	low	Tailor Policy document
IR-4(1)	CCI-000824	Incident Response Handling - Automated Process	Incorporate automated mechanisms to support the incident handling process	mod	Automated IR Handling documentation
IR-6	CCI-000835, CCI-000836	Incident Response Reporting	Develop an Incident Response Reporting Process. Include important contact information	low	Tailor Policy document
IR-6(1)	CCI-000837	Incident Response Reporting - Automated Process	Incorporate automated mechanisms to support the incident reporting process	mod	Automated IR Reporting documentation
IR-7	CCI-000839	Incident Response Reporting	Develop an Incident Response Assistance Program, such as an IT Help Desk. Include important contact information	low	Incident Response agreement Tailor Policy document
IR-7(1)	CCI-000840	Incident Response Reporting - Automated Process	Incorporate automated mechanisms in the IR Response Assistance process to support the automated sharing capability	mod	Incident Response agreement documentation (Automated) Tailor Policy document
IR-8	CCI-002799	Incident Response Plan	Develop a list of parameters to identify event/incidents. Develop a list of metrics to evaluate event/incidents response. ISSM Appoints Incident Response Team	low	Tailor Policy document
MA-2	CCI-002866 CCI-002870 CCI-002874	System Maintenance	Develop a list of the scheduled maintenance/repairs in accordance with manufacturer or vendor specifications (Also a component of SSA) Define maintenance personnel and schedules maintenance on system components in accordance with manufacturer or vendor specifications	low	Annual Scheduled Maintenance Summary (template provided)

MA-2	CCI-000862, CCI-002867, CCI-002868, CCI-002871, CCI-002872, CCI-002875, CCI-002876	System Maintenance	Develop a method to record the maintenance-related information on maintenance logs	low	Maintenance Log (template provided)
MA-3	CCI-000865	System Maintenance	Develop a list of approved system maintenance tools/firmware	mod	Vendor Documentation Annual Scheduled Maintenance Summary
MA 3(1), 3(2)	CCI-00869, CCI-00870	System Maintenance	Develop a method to control and check maintenance tools, including media containing diagnostic and test programs for malicious code before the media are used in the system.	mod	Vendor Documentation Maintenance Log (template provided)
MA-4	CCI-000877, CCI-000879 CCI-000873, CCI-000874, CCI-000876,000878	Nonlocal Maintenance	Develop a list of the non-local maintenance/repairs in accordance with manufacturer or vendor specifications (Also a component of SSA)CCI-000876 Configure system to employs strong authenticators in the establishment of non-local maintenance (via STIG/SGR)CCI-000877 Configure system to terminates sessions and network connections when nonlocal maintenance is completed (via STIG/SGR)CCI-000879	low	Annual Scheduled Maintenance Summary and Maintenance Log, pertaining to non-local maintenance requirements (template provided) Applicable STIG/SRG checks Configuration documentation
MA-4(2)	CCI-000881	Document Non-Local Maintenance	Additional procedures for remote maintenance and digital connections	mod	Annual Scheduled Maintenance Summary and Maintenance Log, pertaining to non-local maintenance requirements (template provided) Applicable STIG/SRG checks Configuration documentation
MA-5	CCI-000891, CCI-002894, CCI-002895	Maintenance Personnel	Identify authorized maintenance organizations or personnel. Develop a method to maintain a current list of authorized maintenance organizations or personnel. Ensure maintenance personnel will be escorted by an authorized person, as required	low	Authorized User Log (template provided) Annual Scheduled Maintenance Summary (template provided) Maintenance Log (template provided) Tailor Policy documents
MA-6	CCI-000903, CCI-002897	Timely Maintenance	Develop a method to ensure maintenance support and spare parts must be available within 24-hours. Ensure any necessary maintenance support contracts are in place and an inventory of spare parts are available.	mod	System Data Sheet(s) Spare parts inventory (as needed) Maintenance support contract (as needed) Tailor Policy documents
PE-2	CCI-000912, CCI-000913, CCI-002910, CCI-002911	Personnel Access Roster	Develop and approve a list of individuals with authorized access to the facility and issues credentials accordingly	low	Physical Access Roster (template provided) Tailor Policy documents
PE-3	CCI-002915, CCI-002916, CCI-002917, CCI-002918, CCI-002924 CCI-002919, CCI-002920, CCI-002921, CCI-002923	Physical Access Log	Define and document the entry/exit points to the FACILITY where the system resides. Define and document entry/exit points and security at these points (badge swipe, etc.) Develop a log to track physical access to these points	low	Design documents showing physical access points Optional Physical Access Inventory Template for open facility (template provided) Physical Access Log Template (template provided) Tailor Policy documents
PE-4	CCI-002930, CCI-002931	Access Control for Transmission Medium	Define system distribution and transmission lines and safeguards to controls physical access to these lines	mod	Design documents showing distribution and transmission lines

PE-5	CCI-000937	Access Control for Output devices	Define output devices and safeguards to controls physical access to these devices. (i.e. Stickers/signs indicating highest classification of output from device on printers, copiers, fax, etc.)	mod	Output devices and safeguards Tailor Policy document
PE-6(1)	CCI-000942	Monitoring Physical Access - Alarms and Surveillance	Actively monitor physical intrusion alarms and surveillance equipment	mod	Document active alarm/surveillance equipment Tailor Policy document
PE-6(4)	CCI-002950, CCI-002951	Monitoring Physical Access - Access to systems	Define and document the entry/exit points to the components where the system resides. Define and document entry/exit points and security at these points (badge swipe, etc.) Develop a log to track physical access to these points	mod	Design documents showing physical access points Optional Physical Access Inventory Template for open facility (template provided) Physical Access Log Template (template provided)
PE-8	CCI-000947, CCI-000948	Visitor Access Records	Develop a method to maintain visitor access records to the facility	low	Personnel Access Roster (template provided)
PE-9	CCI-000952	Power Equipment and Cabling	List of protective measures to prevent damage to the power equipment and power cabling for the system	mod	Design documents showing power supply and cables and protection measures Tailor Policy documents
PE-9(1)	CCI-000953, CCI-002953, CCI-002954	Power Equipment and Cabling - Redundant Cabling	Employ redundant and parallel power cabling paths that are physically separate from primary cables by [organizational defined] distance.	mod	Design documents showing redundant power cables
PE-10	CCI-000956, CCI-000957, CCI-000959	Emergency Shutoff	Provide the capability of shutting off power to the system or individual system components in emergency situations.	mod	Evidence of a protected emergency power shutoff capability
PE-11	CCI-002955	Emergency Power	Applicable only to systems that support critical activities: Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the system and/or transition of the system to long-term alternate power in the event of a primary power source loss	low	Documentation of uninterruptible power supply
PE-11 (1)	CCI-000961	Emergency Power - long term	Applicable only to systems that support critical activities: Provides a long-term alternate power supply for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source	low	List of physical IT assets within boundary of system that require long term alternative power supply Tailor Policy document
PE-12	CCI-000963	Emergency Lighting	May not be Not Applicable for FRCSs Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility	low	Evidence of automatic emergency lighting
PE-13	CCI-000965	Fire Protection	Install and maintains fire suppression and detection devices/systems for the system that are supported by an independent energy source.	low	Evidence of fire suppression and detection devices/systems for the system that are supported by an independent energy source.
PE-13 (3)	CCI-000968	Fire Protection - Automatic	Install an automatic fire suppression capability for the system when the facility is not staffed on a continuous basis.	mod	Evidence of fire suppression and detection devices/systems for the system that is automated

PE-14	CCI-000973	Temperature and Humidity Control	May not be Not Applicable for all systems Install temperature and humidity levels within the facility where the system resides at organization-defined acceptable levels	low	Evidence of Temperature and Humidity Control for the system
PE-15	CCI-000977, CCI-000978, CCI-000979	Water Damage Protection	Master shutoff valves must be accessible to protect the system from damage resulting from water leakage	low	Plan showing accessible master shutoff valves
PE-17	CCI-000988	Alternate Work Site	For system moved to alternate work site, provides a means for employees to communicate with information security personnel in case of security incidents or problems.	mod	Contact list for appropriate security personnel Tailor Policy document
PL-2	CCI-003053	System Security Plan	Define within the security plan the security categorization of the information system including supporting rationale.	low	System Security Plan
PL-8	CCI-003072, CCI-003075	Information System Architecture	The externally and internally facing security architecture will be documented and will support the enterprise architecture. Assumptions about and dependencies on external services are documented on network diagrams	low	System Security Plan (security architecture) Network Diagram
PM-5	CCI-000207	DITPR System Inventory	Develop and maintain an inventory of its systems in DITPR.	low	DITPR registration
PM-11	CCI-000236	Mission Process Definition	Determine information protection needs arising from the defined mission processes and revises the processes as necessary, until an achievable set of protection needs are obtained.	low	System Security Plan Tailor Policy document to document Impact Level
PM-12	CCI-002996	Insider Threat Program	Establish contact with selected groups and associations (i.e. Network Enterprise Center] to facilitate insider threat awareness and monitoring.	low	Service Level Agreement/Contract for security support
PS-7	CCI-001540, CCI-001541	Third-Party Security	Establish agreements with third-party provider that documents personnel security requirements for employees that access the system. (i.e. Security Background Checks)	low	Service Level Agreement/Contract for security support language
RA-3	CCI-001048	Risk Assessment	Conduct an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction.	low	System Security Plan (section pertaining to Risk Assessment Implementation)
RA-5	CCI-001054, CCI-001056, CCI-001057, CCI-001641	Vulnerability Scanning	Define the process for conducting random vulnerability scans on each individual system at DoD defined frequency (DoD has defined the frequency as every 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs))	low	Tailor Policy document Scanning with DISA approved tools
RA-5(1)	CCI-001062	Vulnerability Scanning	Use of scanning tools that maintain currency with industry standard information system vulnerabilities to ensure that scanning activities are conducted with the most up to date list of known vulnerabilities to include USCYBERCOM issued IAVMs.	low	Documentation that scanning tool being used can be updated
RA-5(5)	CCI-001067, CCI-001645	Vulnerability Scanning (Privileged Access)	Configure the system to implement privileged access authorization to all systems and infrastructure components for vulnerability scanning activities. Configuration must comply with applicable STIGs/SRGs.	mod	Applicable STIG/SRG checks Configuration documentation
SA-4(2)	CCI-003101 to CCI-003106	Acquisition Process -Design/ Implementation Information	The organization requires the developer of the system, system component, or system service to provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics and/or organization-defined design/information at organization-defined level of detail.	mod	External system interfaces Approved Hardware diagram and schematics Design related documents

SA-4(2)	CCI-003103, CCI-003104, CCI-003105, CCI-003106	Acquisition Process -Design/ Implementation Information	Define the design and implementation information (including level of detail) that the developer is required to provide for the security controls to be employed.	mod	Tailor Policy document to define design information to be provided by system developer
SA-4(9)	CCI-003114	Acquisition Process - Function/PPS in use	The organization requires the developer of the system, system component, or system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	mod	System security plan (SSP) must document Ports Protocol Service use
SA-4(10)	CCI-003116	Acquisition Process -Use of Approved PIV Products	The organization employs only information technology products on the FIPS PUB 201-2-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	low	System security plan (SSP) must document Personal Identify Verification (PIV) capability
SA-5	CCI-003124 through CCI-003131	System Design	The organization obtains, manages and documentations secure configuration, installation and operation of the system; effective use and maintenance of security functions/mechanisms (including user responsibilities); known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.	low	Design requirements must ensure secure configuration Tailor Policy document (as needed)
SA-9	CCI-000669, CCI-000670, CCI-000671, CCI-000672, CCI-000673, CCI-000674	External system Services	Establish contractual agreements to ensure external system services providers comply with security requirements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance	low	Contracts, Memorandum of Agreement, Service Level Agreement (as needed)
SA-9(2)	CCI-003143,	Identification of Functions/PPS	External system services must identify the functions, ports, protocols, and other services required for the use of such services.	mod	Approved Ports Protocol and Services List Port identification on drawings
SA-10	CCI-003155 through CCI-003163 CCI-000692, CCI-000694	Developer Configuration Management	The organization requires the developer of the system to: perform configuration management during system design, development, implementation and/or operation; document approved changes to the system, component, or service; document the integrity of changes; manage the integrity of changes under configuration management; control the integrity of changes; document the potential security impacts of approved changes All configuration changes will be approved and documented	mod	System development life cycle (SDLC) documentation Tailor Policy document (as needed)
SA-10	CCI-003160. CCI-003161, CCI-003162, CCI-003163	Developer Configuration Management	The organization requires the developer of the system service to identify, report and track security flaws and flaw resolution within the system to organization-defined personnel.	mod	System development life cycle (SDLC) documentation Tailor Policy document (as needed)
SA-11	CCI-003171 through CCI-003178	Developer Security Testing and Evaluation	Security Testing/Evaluation	mod	System security plan (SSP) System development life cycle (SDLC) documentation Tailor Policy document (as needed)
SC-2	CCI-001082	Application Partitioning	Configure system to separate user functionality (including user interface services) from system management functionality.	mod	Data flow diagram. Applicable STIG/SRG checks

SC-4	CCI-001090	Information in Shared Resources	Configure the system to prevent unauthorized and unintended information transfer via shared system resources	mod	Data flow diagram Applicable STIG/SRG checks
SC-5	CCI-001093, CCI-002385, CCI-002386	Denial of Service Protection	Define the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the system.	low	Define Denial of Service types of Attacks Tailor Policy document Applicable STIG/SRG checks
SC-7	CCI-002395, CCI-001097, CCI-001098	Boundary Protection	Implement external boundary defense and if needed internal boundaries to protect the system; monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. If applicable, publicly accessible systems require subnetwork	low	Approved Network Diagram Approved Topology Diagram
SC-7(3)	CCI-001101	Access Points	Implement access control mechanisms	mod	Approved Network Diagram Approved Topology Diagram
SC-7(4)	CCI-001102, CCI-001103, CCI-001105, CCI-002396	External Telecommunications Services	Implement managed interface for each telecommunication service, if applicable, to protect confidentiality and integrity of information being transmitted across each interface for each external telecommunication service	mod	Approved Network Diagram Approved Topology Diagram
SC-7(5)	CCI-001109	Deny by Default/Allow by Exception	The system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	mod	Approved Network Diagram Approved Topology Diagram
SC-7(7)	CCI-002397	Prevent Split Tunneling for Remote Devices	Configure system to prevent the remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks, in conjunction with a remote device	mod	Approved Network Diagram Applicable STIG/SRG checks
SC-7(18)	CCI-001126	Fail Secure	Configure system to fail securely in the event of an operational failure of a boundary protection device.	mod	Approved Network diagram Applicable firewall rule set. Applicable firewall logs.
SC-8	CCI-002418	Transmission Confidentiality and Integrity	The system protects the confidentiality and/or integrity of transmitted information.	mod	Approved Network diagram Applicable STIG/SRG checks
SC-8(1)	CCI-002419, CCI-002421	Cryptographic or Alternate Physical Protection	Configure system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.	mod	Approved Network diagram Applicable STIG/SRG checks
SC-10	CCI-001133	Network Disconnect	Configure System to terminate the network connection associated with a communications session after 10 minutes in band management and 15 minutes for user sessions.	mod	Applicable STIG/SRG checks
SC-12	CCI-002433, CCI-002434, CCI-002435, CCI-002436, CCI-002437, CCI-002438, CCI-002439, CCI-002440, CCI-002441, CCI-002442	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys for required cryptography employed within the system in for key generation, distribution, storage, access, and destruction as defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for systems."	low	Encryption related checks

SC-13	CCI-002449, CCI-002450	Cryptographic Protection	Applicable only to systems with classified information; Configure system to implement cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. DoD has defined the cryptographic uses and type of cryptography required for each use as protection of classified information: NSA-approved cryptography; provision of digital signatures and hashing: FIPS-validated cryptography.	low	Applicable STIG/SRG checks
SC-15	CCI-001150, CCI-001152	Collaborative Computing Devices	Configure the system to prohibit remote activation of collaborative computing devices. DoD has defined the exceptions as dedicated VTC suites located in approved VTC locations that are centrally managed.	low	Applicable STIG/SRG checks
SC-17	CCI-001159	Public Key Infrastructure Certificates	Configure the system to issue public key certificates under DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" or obtains public key certificates from an approved service provider.	mod	Applicable STIG/SRG checks
SC-18	CCI-001160 through CCI001165	Mobile Code	Define acceptable and unacceptable mobile code and mobile code technologies IAW the Protection Profile for Web Browsers and Application SRG. Establishes usage restrictions and authorizations for the use of mobile code. Monitor and control the use of mobile code within the system.	mod	Applicable STIG/SRG checks
SC-20	various	Secure Name/Address Resolution Service (authoritative source)	Applicable only to systems that act as DNS server for external clients; Configure the authoritative name server software for external queries to enable DNSSEC and creates resource records with digital signatures (RRSig) for each A record.	low	Applicable STIG/SRG checks
SC-21	various	Secure Name/Address Resolution Service (recursive or cashing resolver)	Configure system to request and perform 1) data origin authentication and 2) data integrity verification on the name/address resolution responses the system receives from authoritative sources.	low	DNS logs, if applicable Applicable STIG/SRG checks that determine the name server software configuration files
SC-22	CCI-001182, CCI-001184	Architecture and Provisioning for Name/Address Resolution	Applicable only to systems that act as DNS server for external clients; Verify primary and alternate services are available for resolution servers; configure system accordingly	low	DNS logs, if applicable Applicable STIG/SRG checks that determine the name server software configuration files
SC-23	CCI-001184	Session Authenticity	Configure system to protect the authenticity of communications sessions.	mod	Applicable STIG/SRG checks
SC-24	CCI-001190 to CCI-001193 CCI-001665	Fail in Known State	Configure system to fail to an [organization-defined] known-state and preserves [organization-defined] system state information in the event of a system failure.	mod	Tailor Disaster recovery plan and/or Contingency Planning Applicable STIGS/SRG checks
SC-28	CCI-001199, CCI-002472	Protection of Information at Rest	Define the information at rest that is to be protected (PII and classified information at a minimum) and protects the confidentiality and/or integrity of organization-defined information at rest.	mod	Applicable STIG/SRG checks Tailor Policy documents
SC-39	CCI-002530	Process Isolation	Maintain a separate execution domain for each executing process.	low	Applicable STIG/SRG checks

SC-41	CCI-002544, CCI-002545, CCI-002546	Port and I/O Device Access	Physically disable or remove unneeded ports or input/output devices on [organization-defined] systems or system components. Configure system to protect against or limits the effects of [organization-defined] types of denial of service attacks by employing security safeguards.	low	Ports Protocol and Services List
SI-2	CCI-001225, CCI-001230	Flaw Remediation	Establish a system to identify flaws in system and install security-related software and firmware updates to vulnerable systems will be completed as soon as possible or within 30-days of release. (USCYBERCOM or ICS CERT)	low	Software Update procedures Tailor Policy documents
SI-2(2)	CCI-001233	Automated Flaw Remediation Status	Establish an **automated** system to identify flaws in system	mod	Software Update procedures Tailor Policy documents
SI-3	CCI-001241	Malicious Code Protection	Configure system to provide malicious code protection mechanisms to perform periodic scans of the system every 7 days	low	Applicable STIG/SRG checks
SI-3(1)	CCI-001246	Central Management	Malicious code protection mechanisms must be centrally managed	mod	Approved Network Diagram
SI-3(2)	CCI-001247	Automatic Updates	Malicious code protection mechanisms must be automatically updated	mod	Applicable STIG/SRG checks
SI-4	CCI-001253, CCI-002645	System Monitoring	Define the techniques and methods to be used to identify unauthorized use of the system. DoD has defined the monitoring objectives as sensor placement and monitoring requirements within CJCSI 6510.01F.	low	Tailor Policy documents
SI-4(2)	CCI-001260	Automated Tools for Real-Time Analysis	Identify techniques and methods to be used to identify unauthorized use of the system must support near real-time analysis of events	mod	Tailor Policy documents
SI-4(4)	CCI-001261, CCI-001262	Inbound and Outbound Communication Traffic	Identify techniques and methods to be used to identify unauthorized use of the system must monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions	mod	Tailor Policy documents
SI-4(5)	CCI-001264	system Monitoring - System-Generated Alerts	Identify techniques and methods to be used to identify unauthorized use of the system must use real time intrusion detection to notify ISSM	mod	Tailor Policy documents
SI-7	CCI-002703, CCI-002704	Software, Firmware, and Information Integrity	Define the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes and define the tools used to provide integrity checks.	mod	list of software, firmware, and information tools requiring integrity checks.
SI-7(1)	CCI-002705 through CCI-002708, CCI-002710 through CCI-002712	Software, Firmware, and Information Integrity – Integrity Checks	Define the software, firmware, and information on which integrity checks will be performed. Integrity checks are performed at annually	mod	Tailor Policy documents
SI-7(7)	CCI-002719, CCI-002720	Software, Firmware, and Information Integrity – Integration of Detection and Response	Identify security relevant changes that must be incorporated in the Incident Response procedures and capabilities	mod	Tailor Policy documents

SI-10	CCI-001310	Information Input Validation	The system checks the validity of organization-defined inputs.	mod	Applicable STIG/SRG checks
SI-10	CCI-002744	Information Input Validation	Define the inputs the system is to conduct validity checks.	mod	Tailor Policy documents
SI-11	CCI-001312, CCI-001314	Error Handling	Configure system to generate an error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. software configuration documentation only transmits error message alerts to ISSM	mod	Applicable STIG/SRG checks
SI-16	CCI-002823, CCI-002824	Memory Protection	Configure system to implements security safeguards to protect the system's memory from unauthorized code execution	mod	Applicable STIG/SRG checks
SI-17	CCI-002773, CCI-002774, CCI-002775	Fail Safe Procedures	Define failure conditions that result in fail-safe implementation; Identify procedures to implement when failure of system occurs; configure system to implement fail-safe procedures (See CP-12 for safe mode entry configuration details)	low	Applicable STIG/SRG checks; Contingency Plan/Disaster Recovery Documentation Tailor Policy documents

Appendix B: Ongoing Security Control Checklist

This list summarizes on-going security control requirements. The list includes DoD policy level requirements - These CCIs are listed with (r) behind the CCI identification number.

On-going Security Control Checklist

LOW Impact Level Controls

Includes DoD policy requirements that are removed IAW NIST SP 800-82 rev2, Appendix G and **Low-Low-Low** system categorization. These CCIs are listed with (r) behind the CCI identification number.

As-Needed

Action	*Source*	*CCI(s)*	*Comments*
Third-party personnel security - change of status	PS-7	**CCI-003041, CCI-003042, CCI-003043**	Contractors or vendors will immediately notify the ISSO of any transfer or termination of contractor/vendor personnel who possess credentials and/or badges or who have control system privileges.
Retain Training Records	AT-4	**CCI-001337(r)**	Retain individual security training records at least 5 years or 5 years after completion of a specific training program.
Retain Audit Records	AU-11	**CCI-000167 CCI-000168(r)**	Retain audit records to provide support for after-the-fact investigations of security incidents for a minimum of 5-years for SAMI; otherwise for at least 1 year.
Audit generation - change of review frequency	AU-12	**CCI-001459 CCI-000169, CCI-001910, CCI-000172**	In the event of a notification for increased auditing and monitoring, the ISSM will notify the SO within 24 hours via email or phone of the events to audit for increased activity.
Enforce minimum password lifetime restrictions of 24-hr	IA-5(1)	**CCI-000179, CCI-000198, CCI-001616**	All account passwords have a minimum lifetime restriction of 24 hours.
Security Authorization	CA-6	**CCI-000271 CCI-000272**	SO will request an ATO prior to placing in operational status and then every three years or when significant system changes have occurred
Baseline Configuration	CM-2	**CCI-000293**	The ISSM or SA will generate documents for the baseline configuration and present them to the Configuration Control Board (CCB) for formal review and approval
Baseline Configuration - modifications	CM-4	**CCI-000333**	The ISSO will conduct a security impact analysis of each configuration change request. Revised configuration documents will be presented to the Configuration Control Board (CCB) for formal review and approval (Configuration Change Log Template provided)
System Configuration STIG and SRG	CM-6	**CCI-000363 CCI-000367 CCI-000368**	**Configure system according to the most current** Security Technical Implementation Guides (STIGs) and Security Requirement Guides (SRGs) system component inventory. Review is presented to the CCB. Deviations from STIGs or SRGs are noted and the applicable checklist and are uploaded as eMASS artifacts
System Configuration Least Functionality	CM-7	**CCI-000381, CCI-000382**	Configure system configures the information system to provide only essential capabilities (restrict the use of ports, protocols, and/or services).
System Configuration Least Functionality	CM-7(1)	**CCI-001762**	Disable unnecessary ports, protocols, and/or services.

Contingency Plan	CP-2	**CCI-000457**	ISSM and ISSO examines the audit trail to ensure the contingency plan has been reviewed
Contingency Training	DoD Policy CP-3	**CCI-000486 CCI-002833(r)**	Organization provides contingency training to information system users consistent with assigned roles and responsibilities within 10-days of appointment.
Contingency Testing	CP-4	**CCI-000494**	Tests the contingency plan for the information system. [This time period is defined by the organization]
Identifier Management	IA-4	**CCI-000794(r) CCI-000795**	Configures the information system to disable identifiers after 35 days of inactivity
Authenticator Management	IA-5	**CCI-000180 CCI-001610(r)**	Manages information system authenticators by changing/refreshing authenticators. DoD requires authenticators to be changed or refreshed in the following time periods: CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years. DoD has defined the time period as CAC - every 3 years, or 1 year from term of contract Password: 60 days Biometrics: every 3 years
Incident Response Training (initial appointment)	DoD Policy IR-2	**CCI-002778(r) CCI-000813**	All personnel with privileged-level access to any information system or network device must have completed all required training and certifications IAW DoD 8570.01M and Army BBP 05-PR-M-0002 within 30-days of appointment.
Incident Response Handling	IR-4	**CCI-000824, CCI-001625**	The ISSM will review IR activities associated with each incident and incorporate lessons learned into incident response procedures. (Incident Response After-Action Log Template provided)
Incident Response (reporting)	IR-6	**CCI-000835**	personnel to report suspected security incidents within the timeframes specified by CJCSM 6510.01B (Table C-A-1)
Incident Response (After Action Review)	IR-8	**CCI-002800**	The incident response plan capabilities shall be evaluated by completing an After Action Report for each Incident/Event.
Update System Maintenance Policy	MA-1 PA-1	**CCI-000851(r) CCI-001628(r)**	review and update the current system maintenance policy, security planning policy
Physical Access Roster (develop)	PE-2	**CCI-000912, CCI-001635**	Develop Access Roster and list individuals with authorized access to each system. Personnel who no longer require access will be removed from the authorized access roster and their credentials revoked within 24 hours of notification of access change or on the last date of employment. (Personnel Access Roster Template provided)
Physical Access Inventory (develop)	PE-3	**CCI-002919**	Develop Access Inventory and document entry/exit points to facility (or where components reside for open access facility). (Physical Access Inventory Template provided)
Physical Access Log (develop)	PE-3	**CCI-002917, CCI-000920, CCI-000921**	Develop physical access logs for personnel and visitors and verifying that personnel have proper security access control (Physical Access Log Template provided)

Physical Access (Monitor)	PE-8	**CCI-000947**	Visitors accessing the systems are recorded on the Physical Access Log (template provided). Authorization of visitor is checked using Personnel Access Roster (template provided).
Physical Delivery and Removal	PE-16	**CCI-000982**	Monitors any information system components entering and exiting the facility and ensure changes are approved by CCB.
Plan of Action and Milestones Process	PM-4	**CCI-002993**	Implements a process to review plans of action and milestones for the security program and associated organization information systems for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
Information System Inventory	PM-5	**CCI-000207**	Register the information systems in DITPR.
Program Management; Testing, Training, and Monitoring	PM-14	**CCI-003004** **CCI-003009**	Implements a process for ensuring that organizational plans for conducting security testing associated with organizational information systems continue to be executed **in a timely manner**.
Rescreen employees	PS-3 AU-2	**CCI-001517**	Rescreening of employees will be completed and documented by the SO or ISSO [**based on organizational defined frequency**]. Retain rescreening actions for a minimum of three (3) years as an audit trail.
Personnel Termination	PS-4 AU-2	**CCI-001522**	ISSO terminates information system access immediately for terminated employees. Retain an audit trail of account termination actions.
Personnel Termination	PS-4 AU-2	**CCI-003016** **CCI-003022(r)**	ISSO revokes credentials immediately or within 24 hours upon termination of individual employment
Access Agreements	PS-7	**CCI-003036,** **CCI-003041** **CCI-003043(r)**	ISSO is responsible for ensuring individuals re-sign access agreements when access agreements have been updated or when there is a change to the user's level of access.
Personnel Sanctions	PS-8	**CCI-003044** **CCI-003046(r)**	Managers initiate a formal sanctions process for individuals failing to comply with established information security policies and procedures. ISSO is notified immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction
Risk Assessment	RA-3	**CCI-001050,** **CCI-001051(r)** **CCI-001053(r)** **CCI-002370**	Review Risk Assessment results upon re-accreditation and disseminates risk assessment results to the ISSM, ISSO, AO, and PM
External Information System Services	SA-9	**CCI-003138**	Monitor security control compliance by external service providers on an ongoing basis and document records of monitoring.
ICS-CERT alerts/bulletins Flaw Remediation & related software updates	SI-2	**CCI-001227,** **CCI-002604(r)** **CCI-002606(r)** **CCI-002622**	ISSM will ensure All security-related software and firmware updates to vulnerable systems will be completed as soon as possible or within 30 days of release.

Information system component scans for flaw remediation	DoD policy SI-2(2)	**CCI-001233 CCI-001234(r)**	DoD has defined the frequency as continuously with HBSS; 30 days for any additional internal network scans not covered by HBSS; annually for external scans by Computer Network Defense Service Provider (CNDSP).
Malicious Code Protection	SI-3	**CCI-001242, CCI-002624**	configures malicious code protection mechanisms to perform **real-time scans of files** from external sources at endpoints as the files are downloaded, opened, or executed
Information System Monitoring	SI-4	**CCI-002650, CCI-002652**	Monitor information system; [organizational defined information] and [organizational defined frequency]
Security Alert Monitoring	SI-5	**CCI-002692, CCI-001285**	ISSO will subscribing to security alerts and advisories from authorized sources to remain up to date security matters.
Document scheduled and unscheduled maintenance	MA-2	**CCI-002875, CCI-002876**	Records maintenance activity on a maintenance logs (see draft Maintenance Log for required information)
Document non-local maintenance	MA-4	**CCI-000874, CCI-000878**	Records non-local maintenance on a maintenance logs (see draft Maintenance Log for required information)
Record authorized maintenance personnel on Master Authorized User Log	MA-5	**CCI-000891**	Record of all personnel authorized to perform maintenance on the USAG-KA DPW microgrid system will be recorded on the Master Authorized User Log (see draft Master AUL Template for required information)
Media Access	MP-2	**DoD Policy CCI-001003, CCI-001005**	ISSO ensures that all system media and information is protected. Access is restricted IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001
Media Sanitation	MP-6	**DoD Policy CCI-001028, CCI-002580**	ISSO ensures that all system media and information is sanitized IAW the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-88 Revision 1 and all Service Level Agreements
Media Use	MP=7	**CCI-002581, CCI-002582, CCI-002583, CCI-002584**	Only CCB approved maintenance tools and media, used for purposes of system maintenance or recovery, are to be used on the system.

Weekly

***Action* - Weekly**	***Source***	***CCI(s)***	***Comments***
Configuration scans per STIGS and update vendor provided new security updates	DoD SI-3	**CCI-002621, CCI-002622, CCI-002623, CCI-001241, CCI-000366**	Set malicious code protection mechanisms to perform periodic scans of the information system on a weekly basis. Configure system to comply with STIG/SRG guidance
User-level and System-Level Information Backups	CP-9	**CCI-000534 CCI-000535 CCI-000536 CCI-000537 CCI-000538(r)**	System backups are performed weekly. This includes, data download from the GUI – operational data and audit logs. Document backups and store in a location separate from the system (as noted in Configuration Plan).
Off-load and Review audit logs	DoD Policy AU-4 AU-4(1) AU-6	**CCI-001850(r) CCI-001851 CCI-000148 CCI-000151(r)**	Off-load audit records; Look for anomalies and indications of activity defined in Section AU-6 of the AU Policy at least weekly or more frequently if required by alarm. Maintain an audit trail of the reviews and store as noted and Configuration Plan. Any significant anomalies, or inappropriate/unusual activities, or other findings will be reported immediately to the ISSO/ISSM.

Monthly

Quarterly

***Action* – Quarterly**	***Source***	***CCI(s)***	***Comments***
Update AV software	SI-3	**CCI-001240**	Update antivirus software and signatures quarterly. DoD Patch Repository>Antivirus>McAfee Software>VirusScan Enterprise.
Review Access roster	PE-2	**CCI-002914 CCI-000915(r)**	Review system access roster (template: Personnel Access Roster Template)
Review and Update POA&M	CA-5	**CCI-000265(r) CCI-000266**	SO/ISSO Review and update POA&M milestones and edit so it's current. Do this regardless of activation status of system. Note status in review in eMASS.
Review Incident Response Training Records	IR-2	**DoD CCI-002779**	Army Training & Certification Tracking System (ATCTS) at the web site, https://atc.us.army.mil, and reviewed on a quarterly basis
Review publicly accessible information system	DoD Policy AC-22	**CCI-001477(r)**	DoD has defined the frequency to review the content on the publicly accessible information system for nonpublic information.
Review information system privileges	DoD Policy	**CCI-001827(r) CCI-001828(r) CCI-001829(r) CCI-001830(r)**	DoD has defined the frequency to review information system privileges as every 90 days.

Semi-Annual

***Action* - Semi-Annual**	***Source***	***CCI(s)***	***Comments***
Review network topology	Network Infrastructure STIG		Verify external connections are as documented (if applicable).
Review traffic flow policy	DoD Policy SC-7(4)	CCI-001106 CCI-001107(r) CCI-001108	Traffic flow policies for each external telecommunication service are reviewed semi-annually. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need

Annual

***Action* – Annual**	***Source***	***CCI(s)***	***Comments***
Review RMF Policies and Procedures Documents	Overview	DoD Policy Various NIST Controls Families	RMF Policies and Procedures will be reviewed annually and updated as needed but at a minimum every 10-years. Revision description must be annotated in the "Revision History" Section of document.
Review configuration baselines	DoD Policy CM-2(1)	CCI-000296(r) CCI-001585(r) CCI-001497(r)	DoD requires the ISSM or SA will manually review and update the baseline configuration, diagrams and hardware/software lists based on any changes. Include: SCAP scans, hardware/software lists, diagrams, PPS, maintenance tools, spare components list. The organization must document each occurrence of the reviews and update actions as an audit trail.
Review System Configuration STIG and SRG	CM-6	CCI-001503	**ISSM or SA,** will review system configurations and deviations from Security Technical Implementation Guides (STIGs) and Security Requirement Guides (SRGs) annually, or as needed using the Security Compliance Checker (SCC) tool and manual STIG checklists. This review includes the information system component inventory. Review is presented to the CCB.
Review System Hardware Inventory	CM-8	CCI-001780	**ISSM or SA,** review and update the information system component inventory (Hardware List)
Contingency Plan	CP-2	CCI-000457, CCI-000461(r) CCI-000462	**ISSM or ISSO** reviews the Contingency Plan annually. Create an audit trail to ensure the contingency plan has been reviewed. Update Contingency Plan as needed.
Review security controls	CA-2 DoD	CCI-000251, CCI-000252	Technical controls will be reviewed annually. A portion of the management control and operational controls will be reviewed annual, such that all controls are reviewed at least once in a three (3) year period.
Review SLA	CA-3	CCI-002083, CCI-002084(r)	Service Level Agreement will be reviewed and updated, at a minimum annually by both parties.
Continuous Monitoring – Report Security Status	CA-7	CCI-000281, CCI-001581	Future DoD-wide CM guidance to be published; ISSM will report the security status of the organization and the information system annually [to the SO].
Review SSP	PL-2	CCI-000572(r) CCI-000573, CCI-003076(r) CCI-003077(r)	System Security Plan will be reviewed and updated by the ISO and ISSO, at a minimum annually. DoD requires annual updates to the information security architecture.
Review Incident Response Plan	DoD Policy IR-8	CCI-000847 CCI-000848	Incident Response Plan will be reviewed and updated, at a minimum annually. Updates are communicated to

***Action* – Annual**	***Source***	***CCI(s)***	***Comments***
		CCI-000850 **CCI-002803(r)**	stakeholders within 30-days.
Review Physical Access Inventory	PE-3	**CCI-000924** **CCI-000925(r)**	Keys or other physical access devices shall be physically secured and inventoried. Inventories shall be reviewed annually.
Security Awareness and Training Procedures	AT-1	**CCI-001564** **CCI-000105**	DoD has defined the frequency as reviewed annually - updated as appropriate but at least within 10 years of date of issuance.
Training – Security Awareness	DoD Policy AT-2 AT-3	**CCI-001480(r)** **CCI-000111(r)**	Annual refresher security awareness training to all information system users (including managers, senior executives, and contractors).
Training - Disaster Recovery and Contingency Plan	CP-3	**CCI-000485(r),** **CCI- 000487**	ISSO shall ensure that Disaster Recovery and Contingency Plan refresher training is completed and any questions regarding activation and implementation of this plan are addressed at least annually.
Testing - Disaster Recovery and Contingency Plan	CP-4	**CCI- 000490**	Disaster Recovery and Contingency Plan will be tested or exercised at a minimum annually.
Training - Incident Response	IR-2 IR-9(2)	**CCI-000814** **CCI-000815(r)** **CCI-002816(r)** **CCI-002817(r)**	All personnel with privileged-level access to any information system or network device must have completed all annual refresher training IAW DoD 8570.01M and Army BBP 05-PR-M-0002. DoD requires documentation of the training records.
Incident Response Team Orders	IR-2	**CCI-002779**	Incident Response Team on orders signed by the RNEC Director. These orders must be uploaded to ATCTS and validated annually.
Testing - Incident Response	DoD Policy IR-3	**CCI-000818(r)** **CCI-000819(r)** **CCI-000820(r)**	The Incident Response Policy and Procedures will be tested or exercised at a minimum of annually for systems with Moderate Level Availability. DoD has defined the frequency as at least **every six months for systems with High Level Availability.**
Review employee training records	DoD Policy AT-3(2)	**CCI-001566(r)** **CCI-001567(r)** **CCI-001568(r)**	Identify personnel or roles that require refresher training in the employment and operation of physical security controls and ensure training is received.
Review and Re-sign Acceptable Use Policy (AUP)	PS-6 PL-4	**CCI-001532** **CCI-001533(r)** **CCI-003037** **CCI-003068** **CCI-003069(r)**	The AUP will be reviewed, updated, and signed by all users annually or when any change in access level occurs. This includes a review of the rules of behavior.
Review Information System Accounts	AC-2	**CCI-000012** **CCI-002226(r)** **CCI-002228(r)** **CCI-002230(r)**	**Account Manager**: The information system accounts shall be reviewed at least annually for compliance with account management requirements. DoD policy also requires an annual review of the privileges assigned to organization-defined roles or classes of users.
Retain Audit Records	AU-11	**CCI-000168(r)**	Retain audit records to provide support for after-the-fact investigations of security incidents for a minimum of 5-years for SAMI; otherwise for at least 1 year.
Review auditing system	AU-12	**CCI-000171** **CCI-000127(r)** **CCI-001486(r)**	ISSM will review annually the auditing system to ensure that the proper management of the system will support event and incident forensics investigations. DoD also requires organization to conduct an annual review of the auditable

***Action* – Annual**	***Source***	***CCI(s)***	***Comments***
			events to ensure applicability.
Retain Audit logs	AU-4	**CCI-001848, CCI-001849**	The DHCP audit and event logs must include hostnames and MAC addresses of all clients will be stored for at least one-year.
Incident Response Training (refresher)	IR-2	**DoD CCI-000814**	Provide incident response training to information system users, other than general users, consistent with assigned roles and responsibilities annually. (requirement based on DoDD 8570.01)
Maintenance log (review)	MA-2	**CCI-002873**	Previous year maintenance Logs will be presented to and approved by the CCB annually and will be kept for a minimum of three (3) years.
Schedule Maintenance (present)	MA-2	**CCI-002869**	Anticipated Scheduled Maintenance for the upcoming year will be presented to and approved by the CCB annually. Complete the Annual Scheduled Maintenance Summary and System Security Plan (SSP) prior to end of fiscal year. (see Scheduled Maintenance Log Template)
Scheduled non-local maintenance (Present)	*MA-4*	**CCI-000873, CCI-000876**	Non-local must be approved and documented by the CCB annually. Complete the Annual Scheduled Maintenance Summary and System Security Plan (SSP) prior to end of fiscal year. (see Scheduled Maintenance Log Template)
Retain Visitor Records	PE-8	**CCI-000947, CCI-000948.**	Visitor records will be reviewed at least every 30 days and will be maintained for at least one year.
Review Risk Management Strategy	PM-9	**CCI-002995**	Reviews and updates the risk management strategy annually, in accordance with DoD Risk Management Framework. Updated as appropriate but at least within 10 years of date of issuance (DoDI 8510.01).
Review Risk designation	PS-2	**CCI-001514, CCI-001515**	SO, ISSO, Base Ops COR review the risk designation and appointments for control system positions annually against all applicable DoD and Army guidance (in accordance with DoD 5200.2-R CCI- 001513). Records of these reviews must be maintained as an audit trail.
Review Development Standards	DoD Policy	**CCI-003241(r) CCI-003242(r) CCI-003243(r) CCI-003244(r)**	DoD policy requires an annual review of the development tools to determine if the development tools selected and employed can satisfy organization-defined security requirements.
Administrator Password management			Passwords for the built-in administrator account and any emergency administrator accounts must be changed at least annually or when any member of the administrative team leaves the organization. The site will have a policy that application account passwords are changed at least annually or when a system administrator with knowledge of the password leaves the organization.

On-going Security Control Checklist

MODERATE Impact Level Controls

This list is in addition to the LOW Impact Level Control ISSM Checklist. Includes DoD policy requirements that are removed IAW NIST SP 800-82 rev2, Appendix G and **Moderate- Moderate - Moderate** system categorization. These CCIs are listed with (r) behind the CCI identification number.

As-Needed

Action	***Source***	***CCI(s)***	***Comments***
Disable inactive accounts	AC-2(3)	**CCI-000017**	Configure the system to disable inactive accounts after 35 days.
Disable temporary accounts	AC-2(2)	**CCI-000016 CCI-001361(r)**	Configure the system to disable temporary accounts after 72 hours.
Contingency Plan -	CP-2(3)	**CCI-000473(r) CCI-000473(r) CCI-000475, CCI-000476**	As needed, develop procedures for resumption of essential mission functions within 1 hour (Availability High) 12 hours (Availability Moderate).
System Recovery and Reconstitution	CP-10(2)	**CCI-000553**	Document transaction recovery results as part of contingency plan testing.
Record maintenance tools on Maintenance Log (record)	MA-3 (1) (2)	**CCI-000866**, **CCI-000867 CCI-000869 CCI-000870**	Records maintenance tools on a maintenance logs (see draft Maintenance Log for required information). Maintenance tools and media must be inspected and verified prior to use
Ability to obtain maintenance support and/or spare parts	*MA-6*	**CCI-000903 CCI-002897(r)**	Maintenance support for information system components will be provided within 24 hours (Low and Moderate Availability) or immediately upon failure for (High Availability)
Media Marking	MP-3	**CCI-001010, CCI-001011**	All information systems media will be marked indicating the distribution limitations, handling caveats, and applicable security markings (if applicable)
Media Storage	MP-4	**DoD Policy CCI-001014, CCI-001018**	All information systems media will be stored within controlled areas IAW DoDM 5200.01 M Vol. 1-4.
Media Transport	MP-5	*DoD* **CCI-001020, CCI-001023, CCI-001024, CCI-001025**	Protects and controls all media during transport outside of controlled areas using security safeguards IAW DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2
Vulnerability Scanning	RA-5(1)	**CCI-001062**	DISA tools readily update vulnerabilities identified during scan

Install Scan Tool update	RA-5(2)	**CCI-001063 CCI- CCI-001064(r)**	Review DISA for scan tool updates prior to completing scan
Configuration baselines - changes	DoD Policy CM-3	**CCI-000314, CCI-000321, CCI-001740 CCI-000319, CCI-000320, CCI-001741**	Changes to baseline configuration must be documented and a formal review conducted by the CCB, with explicit consideration for security impact analysis (Configuration Change Log Template provided)
Configuration baselines – testing of changes	CM-3 (2)	**CCI-000327**	changes will be tested, in accordance with the CCB approved testing requirements, prior to implementing the changes on the operational system
Configuration baselines – access restrictions for changes	CM-5	**CCI-000338, CCI-000339, CCI-000342, CCI-000343**	The ISSO, in conjunction with the [DPW] Team [e.g., [NEC], [DPW IMO] and appropriate vendors], will ensure any physical and logical access restrictions to the information system and/or system enclave are defined when configuration changes
Review System Hardware Inventory	CM-8(1)	**CCI-000389, CCI-000408, CCI-000409, CCI-000410**	**ISSM or SA,** update the information system component inventory (Hardware List) any time a component is added or removed
Automated monitoring of system	*CM-8(3)*	**CCI-000416**	Implements automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system continuously
Configuration Management Plan	CM-9	**CCI-000421, CCI-000423, CCI-000424, CCI-001790, CCI-001792, CCI-001793, CCI-001795**	Develop a Configuration Management Plan guidelines for implementing configuration management of systems with identified configuration items, throughout the life-cycle of the system (Configuration Change Log Template provided)
Physical Access – Alarms and Surveillance (monitor)	PE-6 (1)	**CCI-000942**	actively monitor physical intrusion alarms and surveillance equipment
Physical Access Inventory – Moderate Level Information Systems (develop)	PE-6 (4)	**CCI-002950, CCI-002951**	Develop Access Inventory and document entry/exit points for each individual system with Moderate Level Impact (Physical Access Inventory Template provided)
Alternate Work Site	PE-17	**CCI-000988**	ISSM must disseminate current the contact information of appropriate security personnel to employees at alternate work sites (as needed)
Information System Monitoring	SI-4(4)	**CCI-002660(r) CCI-002661**	Continuously monitor outbound communications traffic

Monthly

Action	*Source*	*CCI(s)*	*Comments*
Least Functionality	CM-7 (1)	DoD Policy **CCI-001760**	ISSM: Review the system annually to identify unnecessary and/or nonsecure functions, ports, protocols and services and will disable these organization defined functions that are deemed to be unnecessary and/or nonsecure
Review Configurations	DoD Policy CM-7(5)	**CCI-001777**	ISSM: Check systems and review ACAS scans for any unauthorized hardware, software, PPS, or software. DoD also requires review and update of authorized software installed on the system. The organization must maintain audit trails of the review.
Review Security Functions	SI-6	**CCI-002697** **CCI-002699**	Inspected/assessed configures the information system to perform verification of the correct operations every 30 days (Applicable STIG/SRG checks apply)
System Backup	CP-9(1)	**CCI-000541(r)** **CCI-000542**	Test and logs backup information monthly to verify media reliability and information integrity.
Vulnerabilities Scanning – Update Tool prior to Scan	DoD Policy RA-5(2)	**CCI-001063**	Prior to Vulnerability Scanning, exam the record of scans to ensure the latest most up to date scanning policies are present.

Quarterly

Action	*Source*	*CCI(s)*	*Comments*
Retain Previous Configurations	CM-2(3)	**CCI-000304** **CCI-001736(r)**	Retain previous versions of configurations for 3-months

Annually

Action	*Source*	*CCI(s)*	*Comments*
Audit Events Reviews and Updates	AU-2(3)	**CCI-000127**	Conduct reviews of the list of auditable events annually or more frequently upon changes to situational awareness of threats or vulnerabilities
Continuous Monitoring – Independent Assessment	CA-7(1)	**CCI-000282,** **CCI-002085**	Independence the assessors or assessment teams will monitor the security controls in the system annually or in accordance with future DoD wide CM guidance
Review configuration baselines and updates	DoD Policy CM-2(1)	**CCI-000296** **CCI-000299** **CCI-001585(r)** **CCI-001497(r)**	DoD requires the ISSM or SA will manually review and update and upgrades the baseline configuration, diagrams and hardware/software lists based on any changes. Include: SCAP scans, hardware/software lists, diagrams, PPS, maintenance tools, spare components list. The organization must document each occurrence of the reviews and update actions as an audit trail.
Least Functionality	CM-7 (1)	CCI-001760 **DoD**	ISSM: Review the system annually to identify unnecessary and/or nonsecure functions, ports, protocols and services and will disable these organization defined functions that are deemed to be unnecessary and/or nonsecure

Incident Response Testing	IR-3	**CCI-000813** **CCI-001624**	tests the incident response capability for the information system at least annually for low/med availability [and at least every six months for high availability]. IR Testing must be documented. (Incident Response Testing Template provided)
Scheduled Maintenance tools (present)	MA-3	**CCI-000865**	Maintenance tools must be approved and documented by the CCB annually. Complete the Annual Scheduled Maintenance Summary and System Security Plan (SSP) prior to end of fiscal year. (see Scheduled Maintenance Log Template)
Review Information System Architecture	DoD Policy PL-8	**CCI-003077 (r)**	DoD policy requires an annual review and update of the information system architecture.
Software, Firmware, and Information Integrity	SI-7(1)	**CCI-002709(r)** **CCI-002711**	Configures the information system to perform an integrity check of firmware on start-up. The Configuration must be reviewed annually

Appendix C: Acronyms and Abbreviations

Acronym	Description
AC	Access Control – NIST Control Family
ACAS	Assured Compliance Assessment Solution
APMS	Army Portfolio Management System
AT	Awareness and Training – NIST Control Family
ATO	Authorization to Operate
ATCTS	Army Training and Certification Tracking System
AU	Audit and Accountability – NIST Control Family
AUP	Acceptable Use Policy
CA	Security Assessment and Authorization – NIST Control Family
CAC	Common Access Card
CCB	Configuration Control Board
CCI	Control Correlation Identifier
CD	Compact Disc
CM	Configuration Management – NIST Control Family
CERT	Cyber Emergency Response Team
CJCSI	Chairman of the Joint Chief of Staff Instruction
CID	U.S Criminal Investigation Command
CM	Configuration Management
CND-SP	Computer Network Defense Service Provider
CNSSI	Committee on National Security Systems Instruction
CP	Contingency Planning – NIST Control Family
CYBERCOM	US-Cyber Command
CRN	Closed Restricted Network
DISA	Defense Information Systems Agency
DoD	Department of Defense
DITPR	DoD Information Technology Portfolio Registration
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DRP	Disaster Recovery Plan
DTIC	Defense Technical Information Center
DVD	Digital Versatile Disc
eMASS	Enterprise Mission Assurance Support Service

Acronym	Description
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FRCS	Facility Related Control System
GMT	Greenwich Mean Time
GPO	Group Policy Object
GPS	Global Positioning System
IA	Identification and Authentication – NIST Control Family
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
ICS	Industrial Control System
IP	Internet Protocol
IR	Incident Response – NIST Control Family
IRT	Incident Response Team
IS	Information System
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
MFR	Memorandum For Record
MA	Maintenance – NIST Control Family
MP	Media Protection – NIST Control Family
NACLC	National Agency Check with Law and Credit
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute for Standards and Technology
OS	Operating System
OSHA	Occupational Safety and Health Administration
PAUP	Privileged Acceptable Use Policy
PE	Physical & Environment – NIST Control Family
PIT	Platform Information Technology
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning – NIST Control Family
PM	Program Management – NIST Control Family
POA&M	Plan of Actions & Milestones

Acronym	Description
P&Ps	Policies & Procedures
PPBE	Planning, Programming, Budget, and Execution Process
PS	Personnel Security – NIST Control Family
PPS	Ports, Protocols, and Services
RA	Risk Assessment – NIST Control Family
RAR	Risk Assessment Report or Rapid Action Revision (AUP document)
RMF	Risk Management Framework
RMF KS	Risk Management Framework Knowledge Service
SA	System Administrator
SA	System Service and Acquisition – NIST Control Family
SAR	Security Assessment Report
SDLC	System Development Life Cycle
SC	System and Communication Protection – NIST Control Family
SCAP	Security Content Automation Protocol
SCA-V	Security Control Assessor - Validator
SCC	Security Compliance Checker
SI	System and Information Integrity – NIST Control Family
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SO	System Owner
SP	Special Publication
SSP	System Security Plan
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus
US CERT	United States Computer Emergency Readiness Team
UTC	Coordinated Universal Time

Risk Management Framework Physical & Environmental (PE) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Physical and Environmental (PE), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline PE Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
PE-1**	Physical and Environmental Policy and Procedures
PE-2*	Physical Authorizations
PE-3*	Physical Access Control
PE-6	Monitoring Physical Access
PE-8*	Visitor Access Records
PE-11*	Emergency Power
PE-11(1)*	Emergency Power | Long-Term Alternate Power Supply – Self-Contained
PE-12*	Emergency Lighting
PE-13*	Fire Protection
PE-14*	Temperature and Humidity Controls
PE-15*	Water Damage Protection
PE-16	Delivery and Removal
Additional Controls for Security Impact Level: MODERATE	
PE-4*	Access Control for Transmission Medium
PE-5*	Access Control for Output Devices
PE-6(1)*	Monitoring Physical Access [Intrusion Alarms / Surveillance Equipment]
PE-6(4)*	Monitoring Physical Access [Monitoring Physical Access to Information Systems]
PE-9*	Power Equipment and Cabling
PE-9 (1)*	Power Equipment and Cabling - Redundant
PE-10*	Emergency Shutoff
PE-13(3)*	Fire Protection
PE-17*	Alternate Work Site

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 PE Organizational Policy Controls

Broadly implemented PE policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific PE safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Physical Authorizations (PE-2)

An access roster is available which lists all individuals with authorized access to each system log (Excel file: LogSheets.xls/Personnel Access Roster Template) **CCI-000912**. The [FACILITY NAME] SO will develop and maintain this list and the ISSO will formally approve it **CCI-002911, CCI-002910**. Employees of [FACILITY NAME] and support personnel on an active contract will obtain [Common Access Card (CAC) credentials badge] to access controlled areas **CCI-000913**.

The access roster will be reviewed and updated as changes occur or every 90 days at minimum **CCI-002914**. Personnel who no longer require access will be removed from the authorized access roster and their credentials revoked within 24 hours of notification of access change or on the last date of employment. All updates, reviews, and approval actions will be documented for audit purposes and maintained by the ISSO or SO **CCI-001635**.

3. Physical Access Control (PE-3)

Physical access the facility shall be documented and controlled at all entry/exit points where any [FACILITY NAME] components reside (Optional Excel file: LogSheets.xls/Physical Access Inventory Template). No [FACILITY NAME] components shall be located in publicly accessible areas and access to [FACILITY NAME] components are controlled by the organization owning the building where the components are deployed **CCI-002919**. Physical access shall be documented and controlled at all entry/exit points where any [FACILITY NAME] components reside (Excel file: LogSheets.xls/Physical Access Log Template). Visitor escorts are required for anyone not on the approved access roster users to access [FACILITY NAME] components **CCI-002922**. Organizations are responsible for logging physical access logs for personnel and visitors and verifying that personnel have proper security access control (Excel file: LogSheets.xls/Visitor Access Log Template) **CCI-002917, CCI-000920, CCI-000921.**

Keys, access badges or other physical access devices to [FACILITY NAME] components shall be physically secured and inventoried annually, at minimum **CCI-000924**. Access badges and keys will be changed after a security relevant event (i.e. when keys are lost, combinations are compromised, or individuals are transferred or terminated) and documented **CCI-000923, CCI-000926**.

Access Control for Transmission Medium (PE-4) (for Moderate Level control systems if applicable)

Information system distribution and transmission lines are documented on Network Diagrams (Excel file: LogSheets.xls/Physical Access Inventory Template) **CCI-002930**. No [FACILITY NAME] system distribution and transmission shall be located in publicly accessible areas and access to [FACILITY NAME] system distribution and transmission is controlled by the organization owning the Information system distribution and transmission lines **CCI-000937, CCI-002931**.

Access Control for Output Devices (PE-5) (for Moderate Level control systems if applicable)

Physical access to information system output devices shall be reviewed by [FACILITY NAME] SO and

any additional access controls required for output devices will be implemented. This includes, but is not limited to, tickers and/or signs indicating highest classification of output from device on printers, copiers and fax machines. Media protection policy is documented in the [FACILITY NAME] Media Policy and Procedures, DoD 5200.08-R and DoD 5200.01-M **CCI-000937**.

4. Monitoring Physical Access (PE-6)

For facilities containing [FACILITY NAME] components, Physical Access logs shall be reviewed by the ISSM at least every 30-days, or when an indication of a physical event exists **CCI-000939, CCI-000941**. Documentation of the review will be recorded on the Physical Access Log (Excel file: LogSheets.xls/Physical Access Log). A summary of and investigation findings resulting from a of physical security incidents will be recorded on the Physical Assess Inventory and coordinated with the appropriate [Cyber Incident Reporting Chains] **CCI-002939, CCI-002940** (Excel file: LogSheets.xls/Physical Access Inventory Template). Indicators of physical security incidents include, but are not limited to **CCI-002941:**

- Forced physical entry into areas where [FACILITY NAME] components reside
- Tampering or intentional damage done to any [FACILITY NAME] component
- Access outside of normal work hours
- Repeated access to areas not normally accessed
- Access for unusual lengths of time
- Out-of-sequence accesses

Monitoring Physical Access – Intrusion Alarms and Surveillance (PE-6(1)) (for Moderate Level control systems if applicable)

The [ORGANIZATION NAME security monitoring service] will actively monitor physical intrusion alarms and surveillance equipment and will document the process to monitor **CCI-000942**.

Monitoring Physical Access – Access to Information Systems (PE-6(4)) (for Moderate Level control systems if applicable)

The location of all Moderate Level information system(s) is documented. Physical access shall be documented and controlled at all entry/exit points where any [FACILITY NAME] Moderate Level information systems reside (Excel file: LogSheets.xls/Physical Access Inventory Template) **CCI-002950, CCI-002951**.

5. Visitor Access Records (PE-8)

All visitors accessing the [FACILITY NAME] systems are recorded on the Physical Access Log **CCI-000947**. Access Control is described in the [FACILITY NAME] Access Control Policy and Procedures documents [Visitors must complete a visitor access request, through to the [FACILITY NAME] security office.] All visitors to the [FACILITY NAME] facilities who are not on the Personnel Access Roster (Excel file: LogSheets.xls/Personnel Access Log), Master Authorized User List (Excel file: LogSheets.xls/Master Authorized User Log) or other physical access authorization lists must be escorted. Escorts will monitor visitor activities. Physical Access Logs will be reviewed at least every 30 days and will be maintained for at least one-year **CCI-000948**.

6. Delivery and Removal (PE-16)

The NVESD-ESM SO, O&M Contractors, and ISSO maintain access control of the [FACILITY NAME] entry/exit points including components. Authorized components are listed in the hardware list and network diagram artifacts. Changes to these components are made through the Configuration Control Board (CCB) process. Controls for the removal of any information and/or [FACILITY NAME] component is detailed in the [FACILITY NAME] Media Protection Policy and Procedures and Maintenance Policy and Procedures documents **CCI-000981, CCI-000982, CCI-000983, CCI-000984**.

Alternate Work Site (PE-17) for Moderate Level control systems

The policy for off-site system maintenance is described in the Maintenance Policy and Procedures document. Physical access to an alternate work sites shall be documented and controlled **CCI-000985**. The ISSM defines security controls to employ at alternate work sites and assesses as feasibility and effectiveness of these security controls **CCI-000987, CCI-002975**. The ISSM must disseminate current the contact information of appropriate [FACILITY NAME] security personnel to employees at alternate work sites to open to ensure a means of communication in case of security incidents or problem **CCI-000988**. Current contact information is documented in the [FACILITY NAME] Overview Policy and Procedures document.

Risk Management Framework
Security Planning (PL)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Security Planning (PL), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline PL Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
PL-2	System Security Plan
PL-2(3)	System Security Plan (Plan/ Coordinate with Other Organizational Entities)
PL-4	Rules of Behavior
Additional Controls for Security Impact Level: MODERATE	
PL-4 (1)	Rules of Behavior (Social Media and Networking Restrictions)
PL-7	Security Concept of Operations
PL-8	Information Security Architecture

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 PL Organizational Policy Controls

Broadly implemented PL policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific PL safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. System Security Planning (PL-2)

The System Security Plan (SSP) is the foundational document that directs and supports system risk management activity. The SSP is developed for each [FACILITY NAME] system using the Enterprise Mission Assurance Support Service (eMASS) and is submitted to the Authorizing Official (AO) for signature of approval **CCI-003049, CCI-000571**. By using eMASS as the tool for generating the SSP for each [FACILITY NAME] system, all the specified requirements in this security control are completed during registration of the system.

The [FACILITY NAME] SSP will also include policy and procedure documents that are standard across the control system portfolio. These documents will be delineated by security control families and will explain how security controls are applied on all [FACILITY NAME] systems. These are uploaded as artifacts to eMASS.

The key stakeholders for each system will be placed in the appropriate role to be able to update, review, edit, and approve as needed. These roles are: The Information System Owner (SO); Information System Security Officer (ISSO), or Information System Security Manager (ISSM), the Security Controls Assessor (SCA) team and the AO. Through eMASS, each of these key roles will have access to the SSP and will be notified of any changes to the system **CCI-003059, CCI-003061**.

[Each eMASS SSP contains the following information]:

- Clearly defined logical, physical, and authorization boundaries (architecture diagram) **CCI-003051**
- Description of the system and components, mission, operational and geographic environment, and other information that may assist in defining the context of the system (system description field in eMASS) **CCI-003052**
- Security categorization (confidentiality, integrity, availability impact levels) and rationale **CCI-003053**. Security categorization is performed IAW the CNSSI 1253, *Security Categorization and Control Selection for National Security Systems,* March 2014
- Formally appointed [FACILITY NAME] personnel (eMASS assignments and appointment orders)
- Description of the operational environment for the control system and relationships with or connections to other information systems (architecture diagram, interconnection field in eMASS) **CCI-003054**
- Overview of [FACILITY NAME] security requirements including applicable overlays (e.g., Appendix G., NIST 800-82) and the security control baseline with tailoring rationale **CCI-003055, CCI-003056,CCI-003057**
- Proof of consistency with the enterprise architecture (e.g., UFC 4-010-06 *Cybersecurity of Facility Related Control Systems*) through architecture diagrams **CCI-003050**

The ISO and ISSO will review and update each SSP annually, at a minimum **CCI-000573**. Changes to the information system/environment or problems identified during plan implementation or security control assessments will require analysis and updates to the SSP **CCI-000574**. Access to eMASS is restricted to authorized users placed in the proper roles for each system, which protects the SSP from unauthorized

disclosure and modification **CCI-003063, CCI-003064**.

PL-2(3) Planning - Coordination With Other Organizations:

The responsibility for establishing and maintaining coordinated relationships between the [ORGNAIZATION NAME] and other entities, whether organizational or external, is solely the responsibility of the [FACILITY NAME] ISSM **CCI-003065**. [FACILITY NAME] personnel are responsible for establishing coordinated relationships with the following organizations/entities **CCI-003067**: [Enter Organizations with shared responsibility]

3. Rules of Behavior (PL-4)

The full policy for user behavior on the [FACILITY NAME] control system is detailed in the *Access Control Policy and Procedures document*. The Acceptable Use Policy (AUP) Memorandum for Record (MFR) for non-privileged users and the Privileged Acceptable Use Policy (PAUP) MFR for privileged users is included in Appendix B of *the Access Control Policy and Procedures document* **CCI-000592, CCI-000593**. Any user requiring non-privileged access to the [FACILITY NAME] system (e.g., operators) will read and sign an AUP prior to gaining access to the system. Any user requiring privileged access (e.g., ISSM, SA, vendor or contractor) will read and sign a PAUP prior to gaining access to the control system **CCI-001639**. The ISSM will review and update the AUP and PAUP annually **CCI-003068**. If changes occur, the ISSM will distribute the updated versions to all system ISSMs. The system ISSM will ensure all system users reread and resign the updated AUP or PAUP **CCI-003070**.

PL-4 (1) Social Media and Networking Restrictions for Moderate Impact level systems:

The [ORGNAIZATION NAME] will include the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites **CCI-000594, CCI-000595**.

4. Security Concept of Operations (PL-7) for Moderate Impact level systems:

The security Concept of Operations (CONOPS) for each control system must be developed and contain, at a minimum, how the organization intends to operate the system from the perspective of information security. This is documented in eMass as part of the [FACILITY NAME] System Security Categorization **CCI-000944.**

5. Information Security Architecture (PL-8) for Moderate Impact level systems

Information security architecture including information security implementation and safeguards, [both externally and internally facing security architecture will be documented and will support the enterprise architecture] **CCI-003072**. [Assumptions about and dependencies on external services are documented on [FACILITY NAME] network diagrams] **CCI-003074, CCI-003075**. The information

security architecture, documented in the [FACILITY NAME] System Security Plan, will include the overall philosophy, requirements, and approach to protect the confidentiality, integrity, and availability of organizational information **CCI-003073**. Audit records of the security plan updates will include changes to the information system architecture and all changes will be included in the [FACILITY NAME] System Security Plan, the security Concept of Operations (CONOPS), and in [ORGANIZATION NAME] procurements/acquisitions **CCI-003076, CCI-003078, CCI-003079, CCI-003080**.

Risk Management Framework Program Management (PM) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Program Management (PM), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline PM Security Controls

Control Number (NIST)	Control Name
PM-1**	Program Management Policy and Procedures
PM-4	Plan of Action and Milestones Process
PM-5*	Information System Inventory
PM-11*	Mission / Business Process Definition
PM-12*	Insider Threat Program
PM-14	Testing, Training, and Monitoring
PM-16	Threat Awareness Program

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 PM Organizational Policy Controls

Broadly implemented PM policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific PM safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Plan of Action and Milestone (POA&M) Process (PM-4)

The [ORGANIZATION NAME] utilizes enterprise Mission Assurance Support Service (eMASS) for POA&M records and processing. The POA&M is reviewed, completed actions are tracked, and updates to milestones are performed through the eMASS interface **CCI-002993**.

3. Information System Inventory (PM-5)

The [FACILITY NAME] system has been registered in the DoD IT Portfolio Registration (DITPR) via the Army Portfolio Management System (APMS). The [FACILITY NAME] component inventory is contained within the Hardware and Software lists. The system baseline is maintained by the ISSM **CCI-000207**.

System Name	DITPR ID Number
[Add System Name]	[Add DITPR ID Number]

4. Mission/Business Process Definition (PM-11)

Mission/business process definitions and associated information protection requirements are documented in accordance with organizational policy and procedures. The [FACILITY NAME] system categorization contains the information protection requirements and impacts for [ORGANIZATION NAME]. A clear understanding of the level of adverse impact that could result if a compromise of information occurs is included in defining the [ORGANIZATION NAME] information protection needs. The security categorization process is used to make such potential impact determinations and the POA&M review process further refines information protection needs via Risk Assessments and measures their effectiveness using periodic assessments. The [FACILITY NAME] system has been categorized as: [C-I-A Impact Level] **CCI-000236**.

System Name	CIA Impact Level for Risk Determination
[Add System Name]	[Add CIA Impact Level]

5. Insider Threat Program (PM-12)

[Applicable organization] will manage incident response for the system. The [applicable organization] is responsible to establish a cross-discipline insider threat handling team, or to identify and leverage existing incident handling teams already in place. [See the applicable Service Level Agreement (SLA)] **CCI-002996**.

6. Testing, Training, and Monitoring (PM-14)

The [FACILITY NAME] system continuous monitoring strategy will implement the process for the required security testing, training, and monitoring activities when defined by DoD. The [ORGANIZATION NAME], will coordinate with [applicable organization] to ensure that the continuous monitoring strategy plans for security testing, training and monitoring are developed and maintained, and that all activities (testing, training, and monitoring) are executed in a timely manner. The [ORGANIZATION NAME] [,in conjunction

with the applicable organization,] will also review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The [ORGANIZATION NAME] [and applicable organization] will maintain records of all testing, training, and monitoring activities, as well as of periodic reviews **CCI-002998, CCI-002999, CCI-003000, CCI-003001, CCI-003002, CCI-003003, CCI-003004, CCI-003005, CCI-003006, CCI-003007, CCI-003008, CCI-003009.**

7. Threat Awareness Program (PM-16)

The threat awareness program for the [FACILITY NAME] system is inherited from [ORGANIZATION NAME] [and applicable organization]. In addition, the annual DoD Cyber Awareness Challenge Training module [website] and proof of completion is a requirement per the Acceptable Use Policy. All system users will participate in training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and nonstandard threats such as social engineering) before receiving system access **CCI-003013.**

Risk Management Framework
Personnel Security (PS)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Personnel Security (PS), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline PS Security Controls

Control Number (NIST)	Control Name
PS-1**	Personnel Security Policy and Procedures
PS-2	Position Risk Designation
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7*	Third-Party Personnel Security
PS-8	Personnel Sanctions

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 PS Organizational Policy Controls

Broadly implemented PS policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of PS safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact as well as moderate-impact systems.

2. Position Risk Designations (PS-2)

Risk designations for Information Technology (IT) positions in the [FACILITY NAME] system is in accordance with DoD 8570.01-M, Department of Defense Directive (DoDD) 8140.01, and Army Regulation (AR) 25-2 and [other memorandums] **CCI-001512**. The [ORGANIZATION NAME Civilian Personnel Advisory Center (CPAC)] and [ORGANIZATION NAME] are responsible for hiring actions and the ISSM will screen IT positions responsible for [FACILITY NAME] systems in accordance with DoD 5200.2-R. The SO and ISSM review the risk designation and appointments for [FACILITY NAME] IT positions annually against all applicable DoD and Army guidance **CCI-001514**.

3. Personnel Screening (PS-3)

Only personnel employed by the [ORGANIZATION NAME], or [a contractor with an active contract with the FACILITY NAME] are authorized to access this system. Personnel are screened as part of the hiring processes and allowed access in accordance with the [FACILITY NAME] *Access Control Policy and Procedures document*. The SO and ISSM are all screened by their respective organizations prior to appointment to their assigned position. The [ORGANIZATION NAME Human Resource Branch] and the [ORGANIZATION NAME Security Office] will screen all contractors prior to granting access **CCI-001516**.

There are multiple instance requiring the SO or ISSM to rescreen appointed personnel to include but not limited to **CCI-001518**: Cyber incident involving insider threat, Employee position change, Changes in published DoD or Army regulations or rescreening of the three-year reauthorization cycle for the [FACILITY NAME] system **CCI-001519**. Rescreening of employees will be documented by the SO or ISSM and retained for a minimum of three-years **CCI-001517.**

4. Personnel Termination (PS-4)

Many of the personnel actions and policies for the [FACILITY NAME] system are mandated by the [Civilian Personnel Advisory Center (CPAC)]. These polices are not within the [ORGANIZATION NAME] community's power for change. Personnel Terminations require special documentation and steps to ensure security is not compromised. Access control to the [FACILITY NAME] system is detailed in the [FACILITY NAME] *Access Control Policy and Procedures document* **CCI-001522, CCI-003023**. Exit interviews are handled by the [Civilian Personnel Advisory Center (CPAC)] **CCI-003024, CCI- 001523**. The ISSM is responsible for ensuring that all [FACILITY NAME] proprietary information and property is retrieved from the terminated employee before the employee's last day **CCI-001524**, **CCI-001525**. If the terminated employee held the ISSM position, the SO must ensure that all access to the [FACILITY NAME] system that the ISSM maintained, e.g. account lists, passwords, etc., is in the possession of the SO prior to the ISSM's last day **CCI-001526**. Termination records will be maintained by the SO for each employee and the ISSM will be notified within 24 hours upon termination **CCI-003016**.

The SO will ensure a written notification is given to terminated employees of applicable and legally binding post-employment requirements for the protection of the [FACILITY NAME] system. These requirements are established by the [ORGANIZATION NAME Civilian Personnel Advisory Center (CPAC)]. Terminated individuals will sign an acknowledgement of receiving post-employment requirements which will be maintained by the SO or ISSM.

5. Personnel Actions (PS-5)

Personnel Transfer or any change in authorized personnel level access to the [FACILITY NAME] system, either physical or logical, must occur in accordance with the Access Control Policy & Procedures document. The ISSM will be notified within 24-hours when individuals are transferred or reassigned **CCI-001527, CCI-001528, CCI-003031, CCI-003032.**

6. Access Agreements (PS-6)

Access agreements for the [FACILITY NAME] systems are covered in the Acceptable Use Policy (AUP), included as an Appendix in the [FACILITY NAME] *Access Control Policy and Procedures document* **CCI-003035, CCI-001531**. Authorized Users are tracked using a Master Authorized User List. The AUP will be reviewed, updated, and signed by all [FACILITY NAME] users annually or when any change in access level occurs **CCI-001532, CCI-003036.**

7. Third-Party Personnel Security (PS-7)

The [FACILITY NAME] systems may use third-party providers for installation and maintenance on the system, typically via means of a contractor or vendor. Contractor or vendor personnel must acquire the security background check commensurate to the system access level they need to complete their tasks in accordance with DoD 5220.22-M, DoD 5220.22-R, DoD 5200.2-R, DoDI 3020.41, DoD 8570.01-M and AR 25-2 **CCI-003040, CCI-001540**. For example, if a contractor needs root access to the operating system, that level of access is equivalent to an Information Assurance Technical (IAT) II or Information Assurance Manager (IAM) I in DoD 8570.01-M or IT II in AR 25-2. These roles require a Tier III, National Agency Check with Law and Credit (NACLC), background check. The contractor is required to show proof of favorable adjudication prior to gaining access to the system.

Contractors or vendors will immediately notify the ISSM of any transfer or termination of contractor/vendor personnel who possess credentials and/or badges or who have [FACILITY NAME] system privileges within 24 hours of the change **CCI-003041**. The contractor/vendor is required to provide proof of favorable adjudication at the appropriate level for any newly appointed personnel to the ISSM for approval prior to that personnel having access to the system. Monitoring of personnel security requirements for third-party provider will be documented to ensure compliance with applicable policy and procedures **CCI-001541**.

8. Personnel Sanctions (PS-8)

A formal personnel sanctions process is established and documented by [ORGANIZATION NAME] for personnel failing to comply with security policies and procedures **CCI-001542**. The ISSM will be notified immediately when a formal sanctions process is initiated identifying the individual sanctioned and the reason for the sanction **CCI-003044**.

Risk Management Framework
Risk Assessment (RA)
Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to Risk Assessment (RA), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline RA Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
RA-2	Security Categorization
RA-3	Risk Assessment
RA-5*	Vulnerability Scanning
Additional Controls for Security Impact Level: MODERATE	
RA-5(1)	Vulnerability Scanning – Update Tool Capability
RA-5(2)	Vulnerability Scanning –Update by Frequency, Prior to Scan and When Identified
RA-5(5)*	Vulnerability Scanning –Privileged Access

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 RA Organizational Policy Controls

Broadly implemented RA policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific RA safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Security Categorization (RA-2)

The System Security Categorization will be documented in a System Security Plan (SSP), unique to each [FACILITY NAME] system, based upon CNSSI 1253 and FIPS PUB 200. The SSP and each unique record number are located on the Enterprise Mission Assurance Support Service (eMASS) **CCI-001045, CCI-001046, CCI-001047**.

3. Risk Assessment (RA-3)

The Risk Assessment Report (RAR) for each [FACILITY NAME] system details the risk of compromise for each applicable NIST control. [This report will be completed] through the initial and any subsequent assessments of each system then uploaded to eMASS, which maintains an audit trail of previous risk assessments **CCI-001048, CCI-001049, CCI-001050**. Results of the RAR(s) will be available to the SO, ISSO, ISSM and AO. The Security Controls Assessor - Validator (SCA-V) will upload the report to eMASS upon completion of their analysis **CCI-002370**. Upon notification from the AO that a system requires reaccreditation, significant changes to the information system environment, or identification of new threats and vulnerabilities, the risk assessment process will be re-initiated **CCI-001052**.

4. Vulnerability Scanning (RA-5)

Vulnerability scans occur monthly IAW the Service Level Agreement (SLA) using [DISA-approved tools (ACAS Nessus, SCAP Compliance Checker (SCC), and applicable STIGs/IAVMs)] on all applicable assets within the accreditation boundary **CCI-001054, CCI-001056, CCI-001057**. The vulnerability scans are documented as an audit trail for future reference. Any vulnerabilities found in these scans shall be mitigated according to the [FACILITY NAME] *Configuration Management Policy and Procedures document*. Upon analysis of found vulnerabilities, corrective action is to be taken within 30-days and mitigation is to be reported to the Configuration Control Board, SO, ISSO, ISSM, and AO via eMASS **CCI-001058, CCI-001059, CCI-001061**. Any vulnerabilities which cannot be mitigated within 30-days will be mapped to the appropriate security control and added to the [FACILITY NAME] POA&M in eMASS. Random scanning or additional scans are initiated when vulnerabilities, potentially affecting the system/applications, are identified and reported via any authoritative sources **CCI-001641, CCI-001643.**

RA-5(1) Vulnerability Scanning requirements for Moderate Impact Level Systems (Update Tool Capability):

[FACILITY NAME] systems employ [DISA-approved tools] for vulnerability scanning that include the capability to readily update the information system vulnerabilities to be scanned **CCI-001062**.

RA-5(2) Vulnerability Scanning requirements for Moderate Impact Level Systems (Update by Frequency):

Records of previous scans and a review of DISA site for tool updates will be conducted prior to scans to ensure the latest most up to date scanning policies are used **CCI-001063**.

RA-5 (5) Vulnerability Scanning requirements for Moderate Impact Level Systems (Privileged Access):

Components within the [FACILITY NAME] system which require privileged access to allow vulnerability scanning activities are configured to comply with the STIG/SRG guidance **CCI-002906.** [Define vulnerability scanning].

Risk Management Framework System Service and Acquisition (SA) Policy and Procedures

[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date

Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to System Service and Acquisition (SA), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline SA Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
SA-1**	System Service and Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	System Development Life Cycle
SA-4	Acquisition Process
SA-4 (10)*	Acquisition Process | Use of Approved PIV Products
SA-5*	Information System Documentation
SA-9*	External Information System Services
Controls for Security Impact Level: MODERATE	
SA-4 (2)*	Acquisition Process | Design/ Implementation Information
SA-4 (9)*	Acquisition Process | Function/PPS in use
SA-8	Security Engineering Principles
SA-9(2)*	External Information System Services | Identification of Functions/PPS
SA-10*	Developer Configuration Management
SA-11*	Developer Security Testing and Evaluation

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 SA Organizational Policy Controls

Broadly implemented SA policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific SA safeguards and countermeasures applicable to related

[FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Allocation of Resources (SA-2)

The SO is responsible for managing the mission/business process within [FACILITY NAME] system and is responsible for capital planning and investment, allocation of resources, budgeting, and security **CCI-003091, CCI-000610, CCI-000611.** The resources will be allocated for the security requirements to protect the information system as part of the Planning, Programming, Budget and Execution process (PPBE) **CCI-000612, CCI-000613, and CCI-000614.**

3. System Development Life Cycle (SA-3)

The [FACILITY NAME] system development life cycle is a cradle to grave process consisting of six phases: acquisition, development, production, fielding, sustainment, and disposal; all systems go through this process **CCI-003092**. The current state of any system can be in any phase of the life cycle, and information security is a critical component during each of the life cycle phases. During the acquisition, development, production, and fielding phases, the security engineer defines, refines, and implements the information security requirements for the system using the Risk Management Framework (RMF). This process is detailed in the [FACILITY NAME] *Planning Policy and Procedures document*. During the sustainment and disposal phases, the SO, ISSM and SA are responsible for the operations and maintenance of the system **CCI-000615, CCI-000616, CCI-000618**. These information system security roles are fully explained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. The system development lifecycle process includes the organizational information security risk management process in its activities **CCI-003093.**

4. Acquisition Process (SA-4)

The acquisition process is used for all new projects, existing projects, the upgrade or retrofit of a project, operations and maintenance of a project, and disposal of a project. All acquisition practices of the [FACILITY NAME] system will follow all current Federal Government, Department of Defense (DoD) regulations. [FACILITY NAME] systems that contain Personal Identity Verification (PIV) capabilities will ensure tokens are implemented for identity verification **CCI-003116**.

Acquisition involving work that will be accomplished by external entities requires a contract between the SO and the contractor/developer conducting the work. The contract language will include at a minimum:

- Scope of to be accomplished
- Operational requirements
- Cybersecurity requirements
- Timeframe for accomplishing the work
- Monetary value of the contract, including bonuses and penalties
- Acceptance and failure criteria for contract completion

The contract language may also include references for applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business requirements. However, the contract language will exclude telling the company how to do the work **CCI-003094, CCI-**

003100. The cybersecurity requirements language in the contract will describe the cybersecurity functional requirements, strength requirements, and assurance requirements **CCI-003095, CCI-003096, CCI-003097**.

The following sections are an example of contracting language for cybersecurity requirements for the General Settings of a system:

> The Supplier shall provide documentation of software/firmware that supports the procured product, including scripts and/or macros, run time configuration files and interpreters, databases and tables, and all other included software (identifying versions, revisions, and/or patch levels, as delivered). The listing shall include all ports and authorized services required for normal operation, emergency operation, or troubleshooting.
>
> The Supplier shall remove and/or disable, through software, physical disconnection, or engineered barriers, all services and/or ports in the procured product not required for normal operation, emergency operations, or troubleshooting. This shall include communications ports and physical input/output ports [e.g. Universal Serial Bus (USB) docking ports, compact disc/digital versatile disc (CD/DVD drives), video ports, and serial ports]. The Supplier shall provide documentation of disabled ports, connectors, and interfaces **CCI-003098**.
>
> The Supplier shall configure the procured product to allow the Acquirer the ability to re-enable ports and/or services if they are disabled by software.
>
> The Supplier shall disclose the existence of all known methods for bypassing computer authentication in the procured product, often referred to as backdoors, and provide written documentation that all such backdoors created by the Supplier have been permanently deleted from the system.
>
> The Supplier shall provide summary documentation of the procured product's cybersecurity features and security-focused instructions on product maintenance, support, and reconfiguration of default settings **CCI-003099.**

Acquisition Process | Design/ Implementation Information - for Moderate Impact level systems SA-4(2)

Design information for [modifications to] the [FACILITY NAME] system will include security-relevant external system interfaces, high-level design, low-level design, source code, hardware schematics. This information required will be defined in contracts/agreements and will be examined by the [FACILITY NAME] SO **CCI-003101, CCI-003102, CCI-003103, CCI-003104, CCI-003105, CCI-003106.**

Acquisition Process | Function and PPS in Use - for Moderate Impact level systems SA-4(9)

Design information for [modifications to] the [FACILITY NAME] system will include the functions, ports, protocols, and services intended for organizational use. This information required will be defined in contracts/agreements and will be examined by the [FACILITY NAME] SO **CCI-003114.**

5. Security Documentation (SA-5)

The [FACILITY NAME] System Configuration Guides describes the secure configuration, installation, operation, use and maintenance of the [FACILITY NAME] system. The System Security Plan (SSP) (in eMASS), the supplier's System Configuration Guide, and the applicable Security Technical Implementation Guides (STIGs) provide additional details of the technical security requirement implementations. These documents address the protections in place for the [FACILITY NAME] system against known vulnerabilities (e.g., privileged use, shared credentials, etc.). Users and administrators can refer to these documents to use [FACILITY NAME] security functions effectively and operate the system in a secure manner **CCI-003124, CCI-003125, CCI-003126, CCI-003127, CCI-003128, CCI-003129, CCI-003130, CCI-003131.** [Other system-specific artifacts for the RMF process include]:

- Security Assessment Report (SAR)
- Plan of Actions and Milestones (POA&M)
- Risk Assessment Report (RAR)
- Security Authorization Decision document

The SO or ISSM will ensure that the system documentation is protected, but available and disseminated to authorized users, personnel operating or managing the system, and Security Control Assessors (SCA) **CCI-003134, CCI-003135**. For missing documentation, the SO, ISSM, or SA will reconstruct the documents to be included as artifacts **CCI-000642, CCI-003132, CCI-003133.**

Security Engineering Principles (SA-8) - for Moderate Impact level systems:

The [FACILITY NAME] system was designed using system security engineering principles. **CCI-000664, CCI-000665, CCI-000666, CCI-000667.** The SO and Configuration Control Board will apply and documents system security engineering principles when modifications are made. **CCI-000668.** NIST SP 800-160 - Systems Security Engineering, currently in draft form, will be used as the primary source of general and DoD-specific guidance regarding system security engineering principles.

6. SA-9 External Information System Services - for Moderate Impact level systems:

External information system services providers are: [List external information system services] External information system services providers will comply with security requirements [as stated in contractual agreements, Memorandum of Understanding or other agreements] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. **CCI-000669, CCI-000670, CCI-000671, CCI-000672, CCI-000673, CCI-000674.** [Defines processes, methods, and techniques to employ to monitor security control compliance by external service providers on an ongoing basis] **CCI-003138, CCI-003139.**

External Information System Services | Identification of Functions/PPS (SA-9(2)- for Moderate Impact level systems:

The functions, ports, protocols and services used by external information system services are: [List] **CCI-003143.**

Developer Configuration Management (SA-10) - for Moderate Impact level systems:

The [FACILITY NAME] SO will ensure that contracts/agreements are written to ensure that the developer of the system will implement only organization-approved changes to the [FACILITY NAME] system and that all changes are documented, managed and controlled **CCI-000692, CCI-000694.** [This includes]:

- Impacts to system configuration – Changes to the system made during the configuration management process or integrity of changes to configuration items and system components **CCI-000694, CCI-003155, CCI-003156, CCI-003157, CCI-003158, CCI-003159.** This include: Documentation developed or used in the lifecycle, including requirements and interface specifications; Elements including design libraries; Tools including design tools and test tools; Technical data including test data; and Information on element and system lifecycle processes
- Impacts of approved changes to [FACILITY NAME] system security **CCI-003160**. This includes the identification and tracking of security flaws **CCI-003161**. Security flaws will be tracked and flaw resolution within the [FACILITY NAME] system will be reported to the ISSM **CCI-003162, CCI-003163**.

Developer Security Testing/Evaluation (SA-11) - for Moderate Impact level systems:

The [FACILITY NAME] SO will ensure that contracts/agreements are written to ensure that the developer of the system will create, document, and implement the [FACILITY NAME] security assessment plan **CCI-003171, CCI-003172. [**This includes]:

- The types of analyses, testing, evaluation, and reviews of software and firmware components **CCI-003173**
- The depth and coverage to perform unit, integration, system, and/or regression testing/evaluation **CCI-003174**
- The types of artifacts produced during testing and evaluation **CCI-003175, CCI-003176**

Risk Management Framework
System and Communication Protection (SC) Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to System Communications Protection (SC), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 – Applicable Baseline SC Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
SC-1**	System and Communications Protection Policy and Procedures
SC-5	Denial of Service Protection
SC-7*	Boundary Protection
SC-12	Cryptographic Key Establishment and Management
SC-13*	Cryptographic Protection (N/A?)
SC-15*	Collaborative Computing Devices
SC-20*	Secure Name/Address Resolution Service (authoritative source) [May be N/A]
SC-21*	Secure Name/Address Resolution Service (recursive or cashing resolver)
SC-22*	Architecture and Provisioning for Name/Address Resolution [May be N/A]
SC-39*	Process Isolation
SC-41*	Port and I/O Device Access
Additional Controls for Security Impact Level: Moderate	
SC-2*	Application Partitioning
SC-4*	Information in Shared Resources
SC-7(3)*	Boundary Protection - Access Points
SC-7(4)	Boundary Protection – External Telecommunications Services
SC-7(5)*	Boundary Protection - Deny by Default/Allow by Exception
SC-7(7)*	Boundary Protection – Prevent Split Tunneling for Remote Devices
SC-7(18)	Boundary Protection – Fail Secure
SC-8*	Transmission Confidentiality and Integrity
SC-8 (1)*	Transmission Confidentiality and Integrity – Cryptographic or Alternate Physical Protection
SC-10*	Network Disconnect
SC-17*	Public Key Infrastructure Certificates
SC-18*	Mobile Code

Control Number (NIST)	Control Name
SC-19	Voice Over Internet Protocol [May be N/A]
SC-23*	Session Authenticity
SC-24*	Fail in Known State
SC-28*	Protection of Information at Rest

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.
** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 SC Organizational Policy Controls

Broadly implemented SC policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific SC safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Denial of Service Protection (SC-5)

The [FACILITY NAME] system is susceptible to the following Denial of Service attacks [list DoS type of attacks; consider packets of information from other networks]. In addition to strong physical security, denial of service protections shall be configured IAW applicable Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) **CCI-001093, CCI-002385, CCI-002386**.

3. Boundary Protection (SC-7)

The [FACILITY NAME] system [describe external and internal boundaries as well as subnetworks]. Communications and system events will be logged and monitored IAW the [FACILITY NAME] *Audit & Accountability Policy and Procedures document* **CCI-001097**. The [FACILITY NAME] system [describe publicly accessible system components that are physically and/or logically separated from internal organizational networks] **CCI-002395, CCI-001098**.

SC-7(3) Boundary Protection-Access Point for Moderate Impact level systems:

External connections to the [FACILITY NAME] system is defined on the architecture diagrams and are as follows: [list access points to system]. [Describe access control mechanisms] **CCI-001101**.

SC-7(4) Boundary Protection-External Communication Services for Moderate Impact level systems:

External communication services for the [FACILITY NAME] system is defined on the architecture and network diagrams and are as follows: [list access points of external communication services to system]. [Describe the traffic flow policy, and any acceptations, for each managed interface for each external telecommunication service. Describe how confidentiality and integrity of information being transmitted across each interface for each external telecommunication service is protected] **CCI-001102, CCI-001103, CCI-001105, CCI-002396**. Traffic flow policies for each external telecommunication service are reviewed semi-annually. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need **CCI-001106, CCI-001108**.

SC-8 Transmission Confidentiality and Integrity Services for Moderate Impact level systems:

Transmission confidentiality and integrity of transmitted information for the [FACILITY NAME] system is protected. In addition to strong physical security, transmission of information shall be configured IAW applicable Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) **CCI-002418.**

SC-8(1) Transmission Confidentiality and Integrity Services - Cryptographic or Alternate Physical Protection for Moderate Impact level systems:

Cryptographic mechanisms to prevent unauthorized disclosure of information are implemented and system is configured IAW applicable Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) **CCI-002421.**

4. Cryptographic Key Establishment and Management (SC-12)

[FACILITY NAME] systems that have external communication channels enabled, PKI must be enabled. Establish and manage cryptographic keys for required cryptography employed within the information system in for key generation, distribution, storage, access, and destruction as defined in DoDI 8520.02 "Public Key Infrastructure and Public Key Enabling" and DoDI 8520.03 "Identity Authentication for Information Systems." **CCI-002433, CCI-002434, CCI-002435, CCI-002436, CCI-002437, CCI-002438, CCI-002439, CCI-002440, CCI-002441, CCI-002442.**

5. Cryptographic Protection (SC-13)

[FACILITY NAME] systems that require protection of classified information are have Cryptographic protection measures enabled. [Describe NSA-approved cryptography; for provision of digital signatures and hashing: FIPS-validated cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards]. For system components that have applicable STIGs or SRGs, the components will ensure that the [ORGANIZATION] has configured the information system in compliance with the applicable STIGs and SRGs **CCI-002450**.

6. Collaborative Computing Devices (SC-15)

[FACILITY NAME] systems have the following remote and collaborative computing capabilities: [Describe remote/computing capabilities capabilities]. For information system components that have applicable STIGs or SRGs, the organization being inspected/assessed must comply with the STIG/SRG guidance **CCI-001150, CCI-001152**.

SC-18 Mobile Code for Moderate Impact level systems:

[Defines acceptable and unacceptable mobile code and mobile code technologies. Establishes usage restrictions and authorizations for the use of mobile code. Establish policy to monitor and control the use of mobile code within the information system.] **CCI-001160, CCI-001161, CCI-001163, CCI-001164, CCI-001165.**

SC-19 Voice Over Internet Protocol for Moderate Impact level systems:

[Most FRCSs do not use VoIP. If applicable, establishes usage restrictions for Voice over Internet Protocol (VoIP) technologies, based on the potential to cause damage to the information system if used maliciously. Establish policy to authorize, monitor and control VoIP.] **CCI-001173, CCI-001175, CCI-001176, CCI-001177.**

7. Secure Name / Address Resolution Service (Authoritative Source) (SC-20)

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are

examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data **CCI-001178, CCI-002462, CCI-001179, CCI-001663**.

8. Architecture and Provisioning for Name/Address Resolution (SC-22)

Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists) **CCI-001182, CCI-001183**.

SC-28 Protection of Information at Rest for Moderate Impact level systems:

[Identify the information at rest that is to be protected by the information system. At a minimum, this includes Personal Intensification Information (PII) and classified information] **CCI-001199, CCI-002472**.

9. Port and I/O Device Access (SC-41)

Access to the ports and Input/Output (I/O) devices on the [FACILITY NAME] systems are physically secured IAW the [FACILITY NAME] *Physical & Environmental Policy and Procedures document*. Logical disabling of ports and I/O devices are implemented IAW the [FACILITY NAME] *Access Control Policy and Procedures document* and applicable STIGs and SRGs. **CCI-002545, CCI-002544.**

Risk Management Framework
System and Information Integrity (SI) Policy and Procedures
[FACILITY NAME]

Prepared for: [ORGANIZATION NAME]

Table of Contents

Table 1 - Revision History

Revision	Date	Name	Description
1.0	08/2019		Initial Draft

Approvals Page

_____ _____

[Enter SO Name] Date
System Owner (SO)

_____ _____

[Enter ISSO Name] Date
Information System Security Officer (ISSO)

_____ _____

[Enter ISSM Name] Date
Information System Security Manager (ISSM)

1. Baseline Controls & Rationale

A summary of the organizational policy security controls unique to System Information Integrity (SI), is provided in Table 2. The controls define the safeguards and countermeasures required for [FACILITY NAME] systems and were selected using the NIST SP 800-82 Revision 2, Appendix G, ICS Overlay. The table in this section summarizes the selected Control Name, NIST Reference Number and Impact Level. A list of the [FACILITY NAME] systems and applicable security categorization impact level (Low or Moderate) is provided in [FACILITY NAME]'s *Control System Security Program Policies and Procedures – Overview* document.

Table 2 - Applicable Baseline SI Security Controls

Control Number (NIST)	Control Name
Controls for Security Impact Level: LOW	
SI-1**	System and Information Integrity Policy and Procedures
SI-2*	Flaw Remediation
SI-3*	Malicious Code Protection
SI-4*	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-12	Information Handling and Retention
SI-17	Fail Safe Procedures
Additional Controls for Security Impact Level: MODERATE	
SI-2 (2)*	Flaw Remediation – Automated Flaw Remediation Status
SI-3 (1)*	Malicious Code Protection – Central Management
SI-3 (2)*	Malicious Code Protection – Automatic Updates
SI-4 (2)	Information System Monitoring – Automated Tools for Real-Time Analysis
SI-4 (4)	Information System Monitoring – Inbound and Outbound Communication Traffic
SI-4 (5)	Information System Monitoring -System-Generated Alerts
SI-7*	Software, Firmware, and Information Integrity
SI-7 (1)*	Software, Firmware, and Information Integrity – Integrity Checks
SI-7 (7)*	Software, Firmware, and Information Integrity – Integration of Detection and Response
SI-8	Spam Protection [May be Not Applicable to FRCS]
SI-8(1)	Spam Protection – Central Management [May be Not Applicable to FRCS]
SI-8 (2)	Spam Protection – Automatic Updates [May be Not Applicable to FRCS]
SI-10*	Information Input Validation
SI-11*	Error Handling
SI-16*	Memory Protection
SI-17*	Fail Safe Procedures

*Also included in System Specific Security Requirements list. See Appendix A in the Control System Security Program Policies and Procedures – Overview document.

** Addressed in Control System Security Program Policies and Procedures – Overview document

1.1 Technical Controls and Configuration

Security controls and configurations that are unique to an architecture or individual systems - such as system settings, hardware design features and system/firmware update procedures - are not related to policy. Implementation requirements for these controls are summarized in the [FACILITY NAME] System Specific Security Requirements List in Appendix A of the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. These controls are not addressed in this organizational policy.

1.2 SI Organizational Policy Controls

Broadly implemented SI policies and procedures are summarized in the [FACILITY NAME] *Control System Security Program Policies and Procedures – Overview document*. The text in the following sections address details regarding the implementation of specific SI safeguards and countermeasures applicable to related [FACILITY NAME] control systems. The security control baseline was tailored for low-impact [and moderate-impact] systems.

2. Flaw Remediation (SI-2)

Flaws within the [FACILITY NAME] system will be identified through formal and informal identification **CCI-001225**. Formal identification includes [all alerts and bulletins from the Industrial Control System-Computer Emergency Response Team (ICS-CERT) and the United States Cyber Command (USCYBERCOM) Information Assurance Vulnerability Alerts (IAVA)]. The identification of security vulnerabilities or unmitigated flaws may also be formally identified by the Security Control Assessor-Validator (SCA-V) during a Risk Management Framework (RMF) assessment.

Informal identification of flaws can include but are not limited to:

- Vendor/manufacturer updates
- Security Content Automation Protocol (SCAP) tool use
- Scanning tools provided by the [FACILITY NAME enclave]
- Observations by [FACILITY NAME] users and administrators

After the identification of a flaw, the ISSM will report the affected system(s) to the SO, who will in turn report the status of the system to the USCYBERCOM or the ICS-CERT **CCI-001226.** The system ISSM will enter the identified flaw into the DoD mandated RMF automated database, Enterprise Mission Assurance Support System (eMASS), as a Plan of Actions and Milestones (POA&M) vulnerability. The POA&M entry will include a clear description of the mitigating actions planned with reasonable suspense dates given. Procedures in the [FACILITY NAME] *Configuration Management Policy and Procedures document* will be followed, including obtaining Configuration Control Board (CCB) approval of system updates **CCI-001230**.

The ISSM will ensure software and firmware updates are tested for effectiveness and potential side effects prior to installation on the system. The ISSM will obtain confirmation of prior testing for any vendor-provided system updates **CCI-001228, CCI-001229, CCI-002602, CCI-002603.** All flaw remediation, and security-related software and firmware updates to vulnerable systems will be completed as soon as possible or within 30-days of release, as applicable, per DoD defined regulations **CCI-002605, CCI-002607, CCI-001227**.

SI-2(2) Flaw Remediation – Automated Status for Moderate Impact level systems:

The [FACILITY NAME] system uses automated mechanisms [list automated mechanisms] to determine the state of information system components with regard to flaw remediation **CCI-001233**.

3. Malicious Code Protection (SI-3)

The [FACILITY NAME enclave] will employ antivirus software on all Windows systems (see Hardware and Software lists and the Service Level Agreement (SLA)). Software will be DoD-approved and will be configured IAW Security Technical Implementation Guides (STIGs) **CCI-002619, CCI-002620, CCI-002621, CCI-002622**. Antivirus software will perform real-time scans of files from external sources at network entry/exit points and will be updated whenever new releases are available as noted in the [FACILITY

NAME] Configuration Management Policy & Procedures **CCI-001240, CCI-002624, CCI-001242.** Periodic scans will be conducted every 7 days and will comply with applicable STIGs/SRG guidance **CCI-001241.** Antivirus software will perform block and quarantine malicious code and address the receipt of falls positives, sending alerts to administrators immediately in response to malicious code detection **CCI-001243, CCI-001245.**

The ISSM or SA will update the antivirus software and signatures quarterly, at a minimum. During updates, the ISSM or SA will inspect quarantined items and manually remove legitimate malicious code and resolve any false positives. The ISSM or SA will coordinate with [ORGANIZATION NAME Incident Response Reporting chain] for analysis to determine if it is a false positive or active virus. All detected viruses must be reported immediately through the Incident Response Plan reporting chain.

SI-3(1) Malicious Code Protection- Central Management for Moderate Impact level systems:

The [FACILITY NAME enclave] centrally manages malicious code protection mechanisms **CCI-001246**.

SI-3(2) Malicious Code Protection- Automatic Updates for Moderate Impact level systems:

The [FACILITY NAME enclave] automatically updates malicious code protection mechanisms **CCI-001247**.

4. Information Monitoring (SI-4)

The [FACILITY NAME] system, is monitored for unauthorized use or intrusion by the ISSM and SA, and actions are taken as defined in [FACILITY NAME] Access Control, Media Protection and Configuration Management Policy and Procedure documents. These actions include [account, audit log and event log reviews]. Each component has device-level monitoring capabilities, to include network packets at entry/exit points. The DoD has defined the compromise indicators as [define frequency (i.e. real-time intrusion detection)] and/or when there are threats identified by authoritative sources **CCI-002641, CCI-002642, CCI-002643, CCI-002644, CCI-002645, CCI-002646, CCI-002647, CCI-002648, CCI-002649, CCI-002650, CCI-002651, CCI-002652, CCI-002654, CCI-001255, CCI-001256**. Whenever there is an indication of increased risk to organizational operations and assets - based on law enforcement information, intelligence information, or other credible sources of information – information monitoring actives will be conducted **CCI-001257**.

SI-4(2) Malicious Code Protection- Central Management for Moderate Impact level systems:

The [FACILITY NAME enclave] employs automated tools to support near real-time analysis of events **CCI-001260**.

SI-4(4) Malicious Code Protection- Automatic Updates for Moderate Impact level systems:

The [FACILITY NAME enclave] monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions **CCI-002661, CCI-002662**.

SI-4(5) Malicious Code Protection- Automatic Updates for Moderate Impact level systems:

The ISSM receives real time intrusion detection and when there are threats identified by authoritative sources (e.g. CTOs) and IAW CJCSM 6510.01B incident categories I, II, IV, & to reflect the occurrence of a compromise or a potential compromise **CCI-002664**.

5. Security Alerts, Advisories and Directives (SI-5)

The ISSM will remain up to date on current events by subscribing to security alerts and advisories from ICS-CERT, USCYBERCOM IAVM [Define agency providing support such as the[Network Enterprise Center (NEC) notification systems], vendor specific security alerts, and news sites **CCI-001285**. [FACILITY NAME enclave] inherits security alert capability from ICS-CERT, USCYBERCOM IAVM [Define agency providing support] and vendor specific notifications which generates internal security alerts, advisories, and directives to the ISSM as deemed necessary. The ISSM will determine if any of the published events impact the FACILITY NAME system and notify the SO and SA, as necessary **CCI-001286, CCI-002693**. The ISSM [and the ORGANIZATION NAME Incident Response Reporting chain] are both responsible for the reporting and acknowledgement of notifications within the specified time frame in an official message **CCI-001287, CCI-001289**.

SI-7 Software, Firmware and Information Integrity for Moderate Impact level systems:

The SO defines the software, firmware, and information which will be subjected to integrity verification tools to detect unauthorized changes. The following tools used to provide integrity checks [define tools] **CCI-002703, CCI-002704.**

SI-7(1) Software, Firmware and Information Integrity for Moderate Impact level systems:

The information system performs an integrity check of firmware on start-up, [defined transitional state or defined security-relevant events]. The Configuration of the integrity verification tools must be reviewed annually by the ISSM. **CCI-002705, CCI-002706, CCI-002707, CCI-002708, CCI-002710, CCI-002711, CCI-002712.**

SI-7(7) Software, Firmware and Information Integrity for Moderate Impact level systems:

The following security relevant changes must be incorporated in the Incident Response procedures and capabilities. [LIST] **CCI-002719, CCI-002720.**

SI-10 Information Input Validation for Moderate Impact level systems:

The [ORGANIZATION NAME] defines inputs to the system and conducts a validity check of these inputs. [Describe validity check: Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-

defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.] **CCI-001310, CCI-002744.**

6. Information Handling and Retention (SI-12)

The ISSM, and SA are required to handle and retain system information IAW all applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements when managing the [FACILITY NAME] system. The [FACILITY NAME] *Media Protection Policy and Procedures document* shall be followed. All applicable security related references can be found at the Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) website **CCI-001315, CCI-001678**.

SI-16 Memory Protection for Moderate Impact level systems:

The [FACILITY NAME enclave] implements security safeguards to protect the information system's memory from unauthorized code execution. The [FACILITY NAME] *Access Control Policy and Procedures document* shall be followed. [Describe security safeguards: Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.] **CCI-002823, CCI-002824**

7. Fail Safe Procedures (SI-17)

The following conditions result in the implementation of fail safe procedures: [Identify conditions] **CCI-002773.** Fail safe procedures are implemented as follows: [Identify procedures; Consider personnel to be alerted and specific instructions on steps to take (e.g. do nothing, reestablish system settings, shut down, restart or contact designated personnel). The [FACILITY NAME] *Contingency Planning Policy and Procedures document* provides system safe mode settings and details **CCI-002774.**

Appendix F: Performance Metric Data

DEMONSTRATION FEEDBACK

Review of the Draft FRCS RMF Tool

22 August 2019

Prepared For:

Fort Belvoir - Night Vision and Electronics Sensor Directorate (NVESD)

Environmental Security Technology Certification Program (ESTCP)

Conducted By:

Beth Hill

Spectrum Solutions, Inc.

114 Castle Drive

Madison, AL 35758

Contents

1. Overview

Spectrum Solutions, Inc. was asked by Fort Belvoir's Night Vision and Electronics Sensors Directorate (NVESD) to review the Facility-Related Control System (FRCS) Risk Management Framework (RMF) Self-Assessment Tool developed by IPERC, Inc. The FRCS RMF Self-Assessment tool and the accompanying User Guide were reviewed. The FRCS RMF Self-Assessment Tool is specific to FRCS but it can be tailored to other types of systems. The observations made during the review are captured within this document.

There are six steps in the RMF process. The end-goal of the RMF process is to obtain an Authority to Operate (ATO). According to the User Guide, the FRCS RMF-Self-Assessment Tool aids in helping users to step through the first three steps of the RMF Process.

2. Advantage of the FRCS RMF Self-Assessment Tool

The enterprise Mission Assurance Support System (eMASS) is a web-based application that has many functions and features that can be overwhelming to an individual that does not have the experience in RMF. Even with training in eMASS, a user can be overwhelmed and reluctant to use eMASS. Thus, the FRCS RMF Self-Assessment Tool can help an inexperienced individual to navigate through the first three steps of the RMF process.

Also, the FRCS RMF Self-Assessment Tool can save time in completing the self-assessment. Instead of the eMASS user completing the first three steps in eMASS, the user can utilize the FRCS RMF Self-Assessment spreadsheet to complete the first three steps in the RMF process. eMASS is not available to contractor facilities unless the Government provides the contractor with a government-furnished equipment (GFE) (laptop) along with a user account. The FRCS RMF Self-Assessment tool can be used by someone when the user does not have an eMASS account.

3. Limitations of the FRCS RMF Self-Assessment Tool

There are few disadvantages of using a tool like the FRCS RMF Self-Assessment Tool and the advantages far outweigh the disadvantages. But, with any tool, there are limitations to what the user can do.

One limitation of the FRCS RMF Self-Assessment Tool is being limited to performing a self-assessment on only one information system. Since the tool is not database, previous self-assessments cannot be stored. Instead, the user will need to have multiple copies of the tool when a self-assessment is performed for multiple information systems.

4. Review of User Guide

Spectrum Solutions personnel reviewed the User Guide that accompanies the FRCS RMF Self-Assessment Tool. The information below contains the observations and suggestions made as a result of the review.

4.1. Observations from the User Guide

The User Guide includes an "Overview" section that briefly provides a brief explanation of the FRCS RMF Self-Assessment Tool. The "Overview" section is concise and direct. Spectrum Solutions suggests the following things to be considered to include in the "Overview" section:

- Explain the benefit of using the FRCS RMF Self-Assessment Tool.

- Explain the purpose of the Tool.
- Explain the scope of the Tool, i.e., applicable only to Department of Army, DoD, etc.
- Explain how the tool can be obtained. Is there a license that is necessary? Who is the point of contact?
- Since the Tool includes a database with data that is used to populate worksheets based on the user's response, explain how the data is kept relevant. How often is the data reviewed and updated?
- Explain how version control is performed. How does the user know he/she has the most recent copy of the tool and User Guide?
- Explain the deliverables that are available when finishing a self-assessment using the Tool.
- Consider the possibility that the user has completed steps 1 and 2 of the RMF process outside of the Tool but wants to use the Tool to complete Step 3. Can this be accomplished?

5. Observations of the RMF Self-Assessment Tool

Spectrum Solutions personnel reviewed the prototype RMF FRCS Self-Assessment Tool (dated 20190715). Overall, the Tool is convenient, very easy to use, and simple to follow. The "Start Here Instructions" was very detailed and easy to understand. This tab explains to the user the purpose of the remaining tabs and what cells are required.

5.1. Observations from the "System Info Form" Tab

The second tab entitled "System Info Form" is where RMF Team Members and contact information is added. There are a few required cells in this form. The entry fields are text boxes which allows the user to effortlessly enter the person's name, organization, and contact information.

The following observations and suggestions were made during the review by Spectrum Solutions personnel:

- eMASS requires some of the fields to be populated and some fields are optional. The Tool should indicate which fields are required in eMASS. The cells that are required by the Tool are colored peach. Are these fields required in eMASS, as well?
- Because the RMF process involves many Roles in differing organizations, there are several RMF Team Members (Roles) listed that can be populated. However, there the varying roles are not defined. Unless the user is experienced with the RMF process, the user will not recognize the difference between these many roles. Spectrum Solutions suggests the Roles be defined according to responsibilities in DoDI 8510.01, DoDI 8500.01, CNSSI 1253, etc.
- Also, what happens when the name of a role is not already in eMASS? Does eMASS generate an error if a name is not found in the list?
- For the System Information portion of the worksheet, there is a drop-box to select the type of system. How is the list populated? What if there are multiple types of FRCS wrapped up into one ATO?
- For the "DoD Component Information" portion of the worksheet, the fields are not clear. For example, a beginner user will not understand the definition of "DoD Activity".

5.2. Observations from the "Security Cat Form"

The third tab, entitled "Security Cat Form", helps the user determine the Confidentiality, Integrity, and Availability of the FRCS based on the NIST 800-60 V1&2. The information types are listed based on the FRCS System Type on the previous worksheet. The Tool generates the list of information types but the list can be customized.

Also, the Tool also generates the impact levels of Confidentiality, Integrity, or Availability (low, moderate, high) but the user is also allowed to adjust the impact level and provide a justification. The end result of this worksheet is the overall impact level and the overall security categorization.

The following are observations and suggestions made by the Spectrum Solutions personnel:

- There are cells to describe how information type is contained in the system. Are these cells used in eMASS, other areas of the Tool, or the reports that are generated from the Tool? If so, how?
- The information contained in columns F, G, and H contain helpful information and special factors to consider while determining the impact levels.

5.3. Observations from the "Control Info Form"

The fourth tab, entitled "Control Info Form", contains the Implementation Plan for the system, which lists all the security controls in the baseline, which is determined from the Security Categorization in form 3.

The following are observations and suggestions made by the Spectrum Solutions personnel:

- Even though the Tool does not require all cells to be populated per the requirements in eMASS, does the user (someone with escalated privileges) have the ability to require the cells to be populated? There are some organization within the Army that require all cells of the Implementation Plan to be populated, even though eMASS does not require this information.
- For not applicable controls, can the default N/A justification statement be changed?
- How is the information in Column I, "Comments", used? Is it used elsewhere in the Tool, in eMASS Implementation Plan, or in the reports generated from the Tool? Same question applies to the information in Column J, "Responsible Entities".

5.4. Observations from the "TRExport Form"

The fifth tab, entitled "TRExport Form", contains the Test Result Import Template, which must be completed in order to complete the self-assessment portion and must be imported into eMASS. This is perhaps the most beneficial form in the Tool. Instead of the user sitting in front of eMASS, which requires an eMASS Account and SIPR token (if classified), the user instead can use the Tool to perform the self-assessment. However, this spreadsheet can also be exported/imported via eMASS.

6. Conclusion

The FRCS RMF Self-Assessment Tool can be very beneficial to users that are not very experienced with RMF. The RMF process involves several instructions and directives, which can be overwhelming. This Tool combines the requirements from the directives and instructions and helps the user to determine the security categorization and security control baseline.

QUESTION	USER RESPONSE	NOTES 1/2
Name of Person Evaluating Tool:	**Anon for Chinook Systems**	
Contact information (email)	**(See comments)**	for future correspondence
Job Title of Person Evaluating Tool:	**Control Systems Cybersecurity Specialist**	This data will be used to group responses
Years of Experience with RMF Process:	**5**	This data will be used to group responses
Did you have the opportunity to use the RMF Tool to complete RMF Steps 1-3	**yes**	If yes, please consider completing Sheet 2
Did/Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you assess risk in your control system?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you reduce risk in your control system environment?	1 Not at all	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?	1 Not at all	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
How would you rate the overall usefulness of the FRCS RMF Tool?	2 A little useful	(1) Not useful; (2) A little useful; (3) Useful; (4) Very useful; (5) Indispensable
Do you intend to use the RMF Tool for future projects?	as a reference document - almost a dynamic textbook	Yes/No with additional comments welcomed!
Would you be willing to provide a written endorsement of		If Yes, please be sure your contact information is provided
Are there other features that you would like to see added to future versions of the RMF Tool?	Context sensitive and dynamically generated policy and procedure documentation	

(continued) QUESTION	USER RESPONSE	NOTES 2/2			
Do you have any additional comments?	The information populated within this evaluation is based upon interviews with multiple respondents and their experiences with four different projects. The projects ranged in scope from relatively contained (i.e., ATO for a single panel) to complex (i.e., multiple buildings within a campus-like facility). Information collection activities are a major variable when it comes to identifying Labor Hours consumed. This is illustrated in the difference between hours identified within this survey (both with and without using Tool) and total duration for RMF Process. Where duration on subject projects ranged from 4-18 months, the hours for the particular data entry was less than 40 hours. This difference is attributable to the extensive discovery process and organizational activities associated with getting the information in order to enter it into the Tool (or eMASS). When considering the variance between the hours identified (in this survey) and total duration, some observed that the data entry	Comments on usefulness and suggestions welcomed!			

QUESTION	USER RESPONSE	NOTES
Name of Person Evaluating Tool:	**Alex Gordon**	
Contact information (email)	**agordon@gbpts.com**	for future correspondence
Job Title of Person Evaluating Tool:	**Cyber Security SME**	This data will be used to group responses
Years of Experience with RMF Process: **if you have previous experience, please also consider**	**6**	This data will be used to group responses If you have previous experience, please consider
Did you have the opportunity to use the RMF Tool to	**Yes**	
Did/Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you assess risk in your control system?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you reduce risk in your control system environment?	1 Not at all	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?	3 A good amount	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
How would you rate the overall usefulness of the FRCS RMF Tool?	3 Useful	(1) Not useful; (2) A little useful; (3) Useful; (4) Very useful; (5) Indispensable
Do you intend to use the RMF Tool for future projects?		Yes/No with additional comments welcomed!
Would you be willing to provide a written endorsement of the RMF Tool on Organizational leader head?		If Yes, please be sure your contact information is provided
Are there other features that you would like to see added		
Do you have any additional comments?		Comments on usefulness and suggestions

QUESTION	USER RESPONSE	NOTES
Name of Person Evaluating Tool:	**Bianca Nacu (Peregrine)**	
Contact information (email)	nacubianca@gmail.com	for future correspondence
Job Title of Person Evaluating Tool:	**Intern**	This data will be used to group responses
Years of Experience with RMF Process: **if you have previous experience, please also consider**	**<1**	This data will be used to group responses If you have previous experience, please consider
Did you have the opportunity to use the RMF Tool to	**Yes**	
Did/Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you assess risk in your control system?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool help you reduce risk in your control system environment?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
Did/Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?	2 A little bit	(1) Not at all; (2) A little bit; (3) A good amount; (4) Significantly; (5) Greatly
How would you rate the overall usefulness of the FRCS RMF Tool?	3 Useful	(1) Not useful; (2) A little useful; (3) Useful; (4) Very useful; (5) Indispensable
Do you intend to use the RMF Tool for future projects?	Yes, if export tool performed its function more effectively	Yes/No with additional comments welcomed!
Would you be willing to provide a written endorsement of the RMF Tool on Organizational leader head?	Yes	If Yes, please be sure your contact information is provided
Are there other features that you would like to see added	-	
Do you have any additional comments?	Further explanation of the "Latest Test Results" portion of TRExport sheet required	Comments on usefulness and suggestions welcomed!

SYMPOSIUM FEEDBACK

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: FRED PARRY
Company: DOMINION ENERGY
Email: Fred.Parry@Dominionenergy.com

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

What about Step 4 & 5? What's the Cost?

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Doug Van Werden
Company: Rock Island Arsenal
Email: douglas.d.vanwerden.civ@mail.mil

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Tapan
Company: USACE
Email: tapan.c.patel@usace.army.mil

Please rate your RMF experience level

☐ Beginner ☐ Intermediate ☒ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Any Additional comments/suggestions/questions?

Awesome!!

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Jim Lee
Company: Cimetrics Inc.
Email: JimLee@Cimetrics.com

Please rate your RMF experience level

☑ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5

Low High

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Charles W. Morris
Company: KBR
Email: charles.morris@us.kbr.com

Please rate your RMF experience level

☐ Beginner ☐ Intermediate ☑ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☑ 3 ☐ 4 ☐ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☑ 3 ☐ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☑ 3 ☐ 4 ☐ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☑ 4 ☐ 5

Low High

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: CHUCK PURCELL
Company:
Email: CHARLES.PURCELL@NOBAS.OF?

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Low High

Any Additional comments/suggestions/questions?

My Role is to be Knowledgeable enough to point a user to the tool.

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Joe Zhou
Company: Slipstream
Email: jzhou@slipstreaminc.org

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: CHUCK HAMMOCK
Company: ANDREWS, HAMMOCK & POWELL
Email:

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5

Low High

Any Additional comments/suggestions/questions?

FRCS RMF Self-Assessment Tool Feedback

Contact Info (optional)

Name: Bryan Urban
Company: Fraunhofer USA
Email: burbanc@fraunhofer.org

Please rate your RMF experience level

☒ Beginner ☐ Intermediate ☐ Expert

Would the FRCS RMF Tool save you time doing your RMF Self-Assessment?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Would the FRCS RMF Tool help you assess risk in your control system?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Would the FRCS RMF Tool facilitate or accelerate obtaining Authorization to Operate?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Do you intend to use the RMF Tool for future projects?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5

Low High

Any Additional comments/suggestions/questions?