FINAL REPORT

Technical Transfer of Net Zero Planner Tool from Research to Production Platform

ESTCP Project ER-201578-T2

MARCH 2018

Dr. Richard Liesen
ERDC-CERL

Distribution Statement A
This document has been cleared for public release

Page Intentionally Left Blank

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
09/06/2018

2. REPORT TYPE
ESTCP Final Report

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Technical Transfer of Net Zero Planner Tool from Research to Production Platform

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Richard Liesen

5d. PROJECT NUMBER
EW-201578

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Engineer Research and Development Center (ERDC)
Construction Engineering Research Laboratory (CERL)
2902 Newmark Dr.
Champaign, IL 61822

8. PERFORMING ORGANIZATION REPORT NUMBER
EW-201578

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Strategic Environmental Research and Development 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)
EW-201578

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A; unlimited public release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This is a study of transitioning a USACE software system or application from the research environment, with a limited use capacity, to a production environment, with a scalable capacity, that is able to serve the entire Department of Defense (DoD). The transition requires the system reach a scalable capacity, as well as undergo an accreditation assessment to receive an Authority to Operate (ATO). Risk Management Framework (RMF) accreditation defines the structure and process by which a software system or application is approved for net worthiness and receive an ATO.

15. SUBJECT TERMS
Net Zero, Software, Energy, Master Planning, Tools, Risk Management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard Liesen
UNCLASS	UNCLASS	UNCLASS	UNCLASS	73	**19b. TELEPHONE NUMBER** *(Include area code)* 217-373-4572

Table of Contents

TABLES iii

ACRONYMS iv

1.0 INTRODUCTION 1

1.1 BACKGROUND 3
1.2 OBJECTIVE OF THE DEMONSTRATION 4
1.3 REGULATORY DRIVERS 4

2.0 TECHNOLOGY DESCRIPTION 6

2.1 TECHNOLOGY OVERVIEW 6
2.2 TECHNOLOGY DEVELOPMENT 6
2.3 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY 6

3.0 TEST CASE DESCRIPTION AND CONDITIONS 8

3.1 MILESTONES AND STATUS FOR THE TECHNICAL TRANSFER FROM RESEARCH TO PRODUCTION 8

4.0 TRAINING AND SCALABILITY 15

4.1 VIDEOS AND TRAINING METHOD 15
4.2 TRAINING MEDIUM 16
4.3 SCALABILITY 16

5.0 RISK MANAGEMENT FRAMEWORK GUIDANCE 20

5.1 GETTING STARTED 20
5.1.1 Understanding RMF 20
5.1.2 Know the System and Environment 20
5.1.3 Identify the System Type and RMF requirement 21
5.1.4 Identify targeted Hosting location 22
5.1.5 Identify the RMF stakeholders, develop an awareness plan 23
5.1.6 Understanding RMF 23
5.1.7 eMASS and Registration 23
5.2 INITIATE AND PLAN 24
5.2.1 Categorize System (RMF Step 1) 24
5.2.2 Select Security Controls (RMF Step 2) 24
5.3 IMPLEMENT AND VALIDATE 26
5.3.1 Implement Security Controls (RMF Step 3) 26

5.3.2 Assess Security Controls (RMF Step 4) 27
5.4 CERTIFY AND ACCREDIT 28
5.4.1 Authorize System (RMF Step 5) 28
5.5 MAINTAIN AND REVIEW, DECOMISSION 29
5.5.1 Monitor Security Controls (RMF Step 6) 29

6.0 COST ASSESSMENT 30
6.1 COST MODEL 30
6.2 COST DRIVERS 31
6.3 ANNUAL ACCREDITATION COST 32

7.0 IMPLEMENTATION ISSUES 33
7.1 Lessons Learned 33

8.0 REFERENCES 35

9.0 APPENDICES 36
Appendix A: Points of Contact 36
Appendix B: RMF Prerequisites 37
Appendix C: Production Environment Hosting Guidance 39
Appendix D: Hosting Comparison_ SMPL-NZP Tool™ 40
Appendix E: Identifying RMF Team 42
Appendix F: Identify Stakeholders and Develop Awareness Training Plan_ SMPL-NZP Tool™ 53
Appendix G: Security Plan: Categorization 55

TABLES

Table 1. Milestones for the Technical Transfer of SMPL-NZP Tool™ from Research to Production

Table 2. Tutorial Videos for an Energy Efficiency Technology transitioning to a production environment

Table 3. Cost Model for an Energy Efficiency Technology transitioning to a production environment

ACRONYMS

- ACEIT: Army Corps of Engineers Information Technology
- ACP: Access Control Policy
- AO: Authorizing Official
- APMS: Army Portfolio Management Solution
- ATO: Authority to Operate
- CA: Certifying Authority
- CCB: Configuration Control Board
- CCP: Configuration Control Policy
- CEO: Chief Executive Officer
- CIA: Confidentiality, Integrity and Availability
- CIO: Chief Information Officer
- CMP: Continuous Monitoring Plan
- CRT: Cyber Readiness Team
- DAA: Designated Approving/Accrediting Authority
- DIACAP: DoD Information Assurance Certification and Accreditation
- DISA: Defense Information Systems Agency
- DoD: Department of Defense
- FISMA: Federal Information Security Management Act
- FY: Fiscal Year
- GSS: General Support System
- IA: Information Assurance
- IAM: Information Assurance Manager
- IAO: Information Assurance Officer
- IAP: Identification and Authentication Policy
- IO: Information Owner
- IS: Information System
- ISA: Information Security Architect
- ISO: Information System Owner
- ISRMC: (DoD) Information Security Risk Management Committee
- ISSE: Information System Security Engineer
- ISSM: Information System Security Manager
- IT: Information Technology
- JTFTI: Joint Task Force Transformation Initiative
- MA: Major Application
- MoU: Memorandum of Understanding
- NIST: National Institute of Standards and Technology
- NZP: Net Zero Planner (old acronym, now just known as the NZP Tool)
- OMB: Office of Management and Budget
- PIA: Privacy Impact Assessment
- PIT: Platform Information Technology
- PM: Program Manager

- POC: Point of Contact
- PPP: Program Protection Plan
- RMF: Risk Management Framework
- SAP: Security Authorization Package
- SAR: Security Assessment Report
- SCA: Security Control Assessor
- SCP: Sustainability Component Plan
- SDLC: Software Development Life Cycle
- SEP: Security Engineering Plan
- SIAO: Senior Information Assurance Officer
- SISO: Senior Agency Information Security Office
- SM: System Manager
- SMPL-NZP: System Master PLanner -NZP
- SP: Security Plan
- SSP: System Security Plan
- STP: System Test Plan
- UR: User Representative
- USACE: United States Army Corps of Engineers

Acknowledgments:

Funding for this demonstration was provided by the Environmental Security Technology Certification Program (ESTCP) – Energy and Water Project # EW-201578-T2. The project team would like to thank and gratefully acknowledge technical guidance provided by the ESTCP Office.

The project team is thankful for the support provided by the following individuals:

Name: Dr. Richard Liesen
Affiliation: ERDC-CERL

Name: Dr. Michael Case
Affiliation: ERDC-CERL

Name: Dr. Matthew Swanson
Affiliation: ERDC-CERL

Name: Mrs. Jessica Johnson
Affiliation: ERDC-ITL

Name: Dr. James Stinson
Affiliation: ERDC-ITL

Name: Mr. Timothy Garton
Affiliation: ERDC-ITL

Executive Summary:

The SMPL-NZP Tool is an installation energy master planning tool that was developed through 6.2 research funding and demonstrated in ESTCP project # EW-201240 with the tag line of "Don't make short term decisions without a long term plan."

This was a Tech Transfer project to provide assistance in moving the SMPL-NZP Tool program from research to a production version. This project was proposed in the CON-Net Worthiness era and then the transition to the RMF process. The RMF process was very new and many researchers who were developing Government software tools were unfamiliar with the process, the cost, and requirements. As SMPL-NZP starting navigating this process we ended up putting together a user's guide for the RMF process as the Tool went through the process.

The Current shortcomings of the SMPL-NZP Tool before the start of the project were identified as:

- Training (events and on-going) takes significant time from the development team and customer support,
- The Tool needed some "cleaning" and security work to be eligible for hosting on DOD production servers

The identified solutions were achieved in this work assisted in the technology transfer through two main approaches:

- Provide training and tutorial materials for SMPL-NZP Tool users.
- Pursue Risk Management Framework (RMF) Application certification to allow hosting of SMPL-NZP Tool on DoD servers and Add additional encryption to web services to comply with RMF requirements.

This technical transfer project had 2 main goals:

- Use SMPL-NZP Tool as a case study for the new RMF security process and document for future projects.
- Develop a standard training course for the tool and demonstrate how modern training can be accomplished and delivered.

Results are a small in-house group was trained on the RMF process, the SMPL-NZP Tool was assessed as an RMF case study, and completed final report as a guide for others. Online training was developed and is hosted on YouTube. At this time the SMPL-NZP Tool has Authority to Operate (ATO) on the ERDC Cloud Computing Environment where it is currently being hosted.

This project was submitted using the knowledge of the DIACAP and CoN systems that were previously in place. The RMF process is structured differently and so is the categorization of assessments. Where a CoN could have been achieved in the old system, an "Assess Only" could be achieved for the SMPL-NZP Tool in the RMF process. The Tool proceeded down the Assess and Authorize Path. Advantages of undergoing rigorous security assessment and meeting RMF requirements are the assurance of a secured data set and a documented log of the approved architecture and uses of the system. The process provides necessary baseline for monitoring and counteracting any breaches to certified system or data use. Finally the SMPL-NZP Tool Program Owner was chosen to be The *ERDC* Center for the Advancement of Sustainability Innovations (*CASI*). It provides ERDC ownership for the Tool.

1.0 INTRODUCTION

This is a study of transitioning a USACE software system or application from the research environment, with a limited use capacity, to a production environment, with a scalable capacity, that is able to serve the entire Department of Defense (DoD). The transition requires the system reach a scalable capacity, as well as undergo an accreditation assessment to receive an Authority to Operate (ATO). Risk Management Framework (RMF) accreditation defines the structure and process by which a software system or application is approved for net worthiness and receive an ATO.

1.1 BACKGROUND

A software system operating in the research environment may be limited in its use capacity. The desire to transition a system from the capability to serve only small numbers of users to the capability to reach across all of DoD presents the need to transfer the system to a scalable platform. This scalable capacity may only be provided by transferring the system from a research and development environment to an enterprise production environment. In order for a system to meet DoD requirements it must meet legislative requirements. The requirement states a system must be accredited and attain an ATO, before consideration for an enterprise production environment. The receipt of an ATO, while it does meet legislative requirements, does not guarantee the systems success in a production environment. The system should also be prepared to scale with the growing customer demand.

In order for a software system to make a successful transition to an enterprise production environment it should address any gaps which may impact scalability. One targeted gap impacting SMPL-NZP Tool™ scalability is user training. The lack of user training impacts a system by significantly impacting the availability to users. The number of users, or user growth will be directly limited to the number of persons available to deliver training, until such time effective training material is made readily available across the entire potential user-base.

A second gap impacting the RMF process is reaching a stable version of the software to start the RMF process. This stable version, or release version, is difficult to obtain due to scope creep from the user and development teams. Scope creep is defined as the infringement upon the original defined scope of work where the users want a few more features and the developers want to have final data structures and algorithms. Even though software is never completed, having a full featured, stable version is necessary to start the process. To attain a stable platform many measures must be taken, including a freeze on the addition of interface features and completion of database and system modifications necessary to meet security and functionality requirements must be completed and changes frozen. SMPL-NZP Tool™ made the appropriate changes and settled on a release version prior to the start of RMF documentation. Issues with this are discussed in the Lessons Learned section. Once a software system has addressed gaps impacting scalability, the system is prepared on a functional level for a transition to an enterprise production environment, but still must meet DoD requirements.

RMF accreditation is the DoD criteria for any software system pursuing an ATO. According to Office of Management and Budget (OMB) policies (OMB Memorandum M-10-15), under National Institute of Standards and Technology (NIST) enforcement, it is required all information systems undergo annual review, ensuring the Federal Information Security Management Act (FISMA, section 3544(b)(5)) minimum security standards are continually met and maintained as outlined by the Joint Task Force Transformation Initiative (JTFTI). The DoD has adopted RMF as the official FISMA standard accreditation.

The RMF accreditation process documentation is a newly required replacement for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. The RMF requirements are newly released and are still in an evolving state. Navigating RMF is a DoD and, specifically, USACE-wide obstacle. Being a new process, there are few publications or resources available providing RMF accreditation guidance. Far too many man-hours and resources must be dedicated to identifying requirements and navigating the available documentation and resources. This study on RMF guidance provides documented experience and lessons learned preparing for and navigating an RMF accreditation to an ATO; decreasing the man-hours and resources required for future systems and application to undergo RMF accreditation. On March 12, 2014, the DOD released guidance to supersede DIACAP. The process is now titled Risk Management Framework (RMF) for DOD Information Technology (IT) and numbered. DOD Instruction 8510.01 (DOD, 2014).

1.2 OBJECTIVE OF THE DEMONSTRATION

The study shall demonstrate the shortest known path for a software system transitioning from a research and development environment, with limited user capacity, to receiving an ATO and becoming enterprise production ready. The study shall achieve this by providing field tested paths and lessons learned in preparing for and undergoing an RMF accreditation, as well as, publishing training material and addressing any usability concerns so as to close the gap on system scalability.

The objective is to transition the SMPL-NZP Tool™ from the research environment with the capability to serve a single district to a production environment with a scalable capacity that is able to serve the entire DoD. Further, this work aims to make the SMPL-NZP Tool™ easier to use through the development of tutorials, training events, and streamlining the interface. The scalability needs to grow with customer demand, but having the tool ready to transfer to a scalable platform needs to be accomplished first.

Having established system scalability, through innovative training solutions, then the system is ready for transition. By undergoing an RMF accreditation the system will be approved for transition to a scalable platform on an enterprise production environment.

1.3 REGULATORY DRIVERS

DoD, Army Corps of Engineers Information Technology (ACEIT), Defense Information Security Agency (DISA) requires any system hosted on stated environment possess an ATO. The ATO may only be obtained by successful completion of an RMF accreditation. Risk

Management Framework (RMF) is the unified information security framework for the entire federal government that is replacing the legacy Certification and Accreditation (C&A) processes within federal government departments and agencies, the Department of Defense (DoD) and the Intelligence Community (IC).

RMF is an integral part of the implementation of FISMA, the Federal Information Security Management Act, and is based on publications of the National Institute of Standards and Technology (NIST) and the Committee on National Security Systems (CNSS). With the publication of DoD Instruction (DoDI) 8500.01 and DoDI 8510.01 in March, 2014, DoD has officially begun its transition from the legacy DIACAP process to the new "RMF for DoD IT" process.

DoDI 8500.01 replaces the former DoD Directive 8500.1 and defines DoD's policies for protecting and defending information and information technology, now officially dubbed "Cybersecurity" in place of "Information Assurance".

DoDI 8510.01 delineates the roles, responsibilities, and high-level life cycle process of the "Risk Management Framework (RMF) for DoD IT" as the replacement for DIACAP. Complete specification of security controls (requirements) and system categorization methodology, formerly published in DoD I 8500.2, are now provided by reference to the applicable NIST and CNSS publications (e.g., NIST SP 800-53 and CNSSI 1253).

2.0 TECHNOLOGY TRANSFER DESCRIPTION

This technology transfer project is to move the SMPL-NZP Tool from a research to a production environment and start the execution of the newly defined RMF process and provide training for the SMPL-NZP Tool software.

2.1 TECHNOLOGY TRANSFER OVERVIEW

RMF accreditation is intended to ensure any system placed on a given network poses nor exposes no significant security threat to that network. The technology demonstrated here is a field trial and documentation of RMF preparation and lessons learned. Preparing for an RMF accreditation assessment is a lengthy process, and a documented field trial and lessons learned document will significantly improve the flow for future projects successfully completing an RMF accreditation and transition to an enterprise production environment in a reasonable amount of time.

2.2 TECHNOLOGY DEVELOPMENT

This study details the implementation of RMF requirements as described in BAI Information Security Consulting & Training and other RMF resources, including RMF Knowledge Service (Knowledge Service, n.d.), as well as, implementation of elements aiding the required scalability of a production ready system. BAI is an information security consulting and training company that provides resources for RMF.

SMPL-NZP Tool™ executed gap analysis identifying hindrances in system scalability. The findings showed a lack of training materials would present interruption in the software system scaling to an enterprise production environment, as well as, showed the lack of a stable platform would delay documentation and scalability

The gap analysis findings drove the requirement of developing easily distributable effective training materials, and setting requirements for a release version of the software system. According to research, documented by journalist Anna Windermere (Windermere, 2016), training videos provide the most efficient – effective training material.

The guidance and methods gathered and implemented successfully prepared SMPL-NZP Tool™ for RMF accreditation for an ATO, and the developed training videos successfully mitigated issues with scalability; all preparing the system for an enterprise production environment where the tool could successfully serve its full potential audience.

2.3 ADVANTAGES AND LIMITATIONS OF RMF

There are significant advantages to considering RMF requirements and elements of a production ready system prior to system development. To consider said factors an understanding of RMF and production requirements is a necessity.

The advantages of undergoing rigorous security assessment and meeting RMF requirements are the assurance of a secured data set and a documented log of the approved architecture and uses of the system. This provides necessary baseline for monitoring and counteracting any breaches to certified system or data use.

Limitations of RMF accreditation and transition to a production environment are the impacts to the Software Development Lifecycle (SDLC) and flexibility of architecture and modules. The SDLC often suffers negative ramifications to timelines due to the rigid and complex requirements of RMF. Under RMF guidelines, software modifications must be carefully reviewed, approved by the Configuration Control Board (CCB) and fully tested. All phases of modifications and modification test plans must be meticulously documented. This process can become time consuming and may stall development. Also, flexibility to hosting locations and hardware acquisition may suffer due to the lengthy CCB requirements, as well as to the production hosting environments' rigid regulations.

3.0 TEST CASE DESCRIPTION AND CONDITIONS

SMPL-NZP Tool™ is the test case used in the demonstration of RMF accreditation and enterprise production environment requirements preparation. The SMPL-NZP Tool™ reached a user volume expansion rate at which it began to outgrow its support capacity. The tool presented no comparable competition in its field, paralleled by significant field need. Expanding support capacity to allow for escalating user volume became mission critical. To provide continued support to the Net Zero mission, it became essential the SMPL-NZP Tool™ prepare for transition to an enterprise production environment.

An enterprise production environment would allow SMPL-NZP Tool™ to expand upon and ensure the desired user base had access to the necessary tools and resources. At the time of the RMF study, SMPL-NZP Tool™ was nearing development completion and beginning to gain field traction. The tool was still in a developmental state where modifications to necessary software modules would have minimal impact to the overall user base. The technology was just preparing to expand beyond its pilot subjects.

SMPL-NZP Tool™ provided a good case for demonstrating RMF requirements and production ready system elements due to its clear software system need, lack of competition for the technology and its developmental stage at the time of the RMF Study.

Following are the SMPL-NZP Tool™ milestones presented at the beginning of the study of transition from a research environment to a production environment.

3.1 MILESTONES AND STATUS FOR THE TECHNICAL TRANSFER FROM RESEARCH TO PRODUCTION

Milestones are listed as defined at the beginning of SMPL-NZP Tool™'s Transfer from Research to Production. **Status** updates are listed according to FY16 year-end status for each milestone. **References** corresponds to information and evidence in support of its listed milestone as discussed in "Technical Transfer of SMPL-NZP Tool™ from Research to Production" final report.

Table 1. Milestones for the Technical Transfer of SMPL-NZP Tool™ from Research to Production

Milestones	Status	Reference
SMPL-NZP Tool™ RMF Process		
Make database changes to meet security requirements	Database changes were made to meet initial security requirements, prior to the beginning of RMF documentation. Further database changes were required per the RMF Pre-Assessment scans.	Section 1.1 para 3 & section 5.3.2 para 3&4

Make database changes to accommodate necessary functionality features	Database changes were made to accommodate necessary functionality, prior to the beginning of RMF documentation. Further database changes were required per the RMF Pre-Assessment scans.	Section 1.1 para 3
Document System Architecture, network architecture, Security Architecture, and any other documentation that will not change with development	SMPL-NZP Tool™ completed a full system description with boundary definitions as defined in the ERDC Research and Development Environment. SMPL-NZP Tool™ boundaries with-in the targeted Corps Net enclave are to be negotiated in the MOU. System and boundary definitions may not be released due to security restrictions.	Section 5.1.2 para 2
Move core functionality to new interface	Completed	
Interface feature freeze for RMF process	Interface changes were made to accommodate necessary functionality, prior to the beginning of RMF documentation. Further modifications were frozen to provide a stable release version for RMF accreditation assessment.	Section 1.1 para 3 & section 4.3 para 1
Complete testing and record/ document test results	Completed. Tracked in OnTime, Issue and defect management system.	
Document database, services, and other changes from development	Completed. Tracked in OnTime, Issue and defect management system.	

Submission of Documentation for RMF- Assess only	SMPL-NZP Tool™ was required to move forward with an Assess and Authorize accreditation assessment package, as opposed to the originally planned Assess-Only accreditation assessment package, due to the size and nature of the system. SMPL-NZP Tool™ has completed the Assess and Authorize accreditation assessment package to the furthest extent with available resources. Due to the obligations to complete the required Assess and Authorize over the planned Assess Only accreditation assessment package, further planning and resources will be required to complete the RMF accreditation assessment package. Note SMPL-NZP ToolTM has completed a set of initial pre-assessment scans. The results may not be released or published due to specific security constraints.	Section 5.1.3 all & Section 5.3.2 para 4
Gain RMF Assess only authorization	SMPL-NZP Tool™ was required to move forward with an Assess and Authorize accreditation assessment package, as opposed to the originally planned Assess-Only accreditation assessment package, due to the size and nature of the system. SMPL-NZP Tool™ has completed the Assess and Authorize accreditation assessment package to the furthest extent with available resources. Due to the obligations to complete the required Assess and Authorize over the planned Assess Only accreditation assessment package, further planning and resources will be required to complete the RMF accreditation assessment package. NOTE: It is key to the successful completion of an RMF authorization package, and planning for authorization package preparation planning that an RMF type authorization be determined at the earliest time possible. The RMF type authorization will directly impact the needed resources and time.	Section 5.1.3 all & Section 5.4.1
Document RMF process	The full life cycle of RMF has been documented with lessons learned included.	Section 5 all

Software Security Report		
Software- security report draft	The SMPL-NZP Tool™ investigation into the RMF process found that the security requirement specification is fluid and dependent up the specific system. A given systems owner, audience, information types hosted or transferred, hosting enclave and may more factors determines the security requirements for that specific system. This said, a software security report would require specific requirements for countless system specification combinations. It has been found such a document is not a reasonable nor useful requirement. However, It is more useful for any system seeking to meet its specific security requirements, to gain a full understanding of RMF through which the systems specific security requirements may be derived. The SMPL-NZP Tool™ moved forward with a full investigation of the RMF process so as to guide its audience through the required information to determine a system specific security requirements.	Section 5.1.3 all & Section 5 all
Final Software-security process report	The SMPL-NZP Tool™ investigation into the RMF process found that the security requirement specification is fluid and dependent up the specific system. A given systems owner, audience, information types hosted or transferred, hosting enclave and may more factors determines the security requirements for that specific system. This said, a software security report would require specific requirements for countless system specification combinations. It has been found such a document is not a reasonable nor useful requirement. However, It is more useful for any system seeking to meet its specific security requirements, to gain a full understanding of RMF through which the systems specific security requirements may be derived. The SMPL-NZP Tool™ moved forward with a full investigation of the RMF process so as to guide its audience through the required information to determine a system specific security requirements.	Section 5.1.3 all & Section 5 all

SMPL-NZP Tool™ Video Tutorials		
Develop Tutorial video Scripts and SMPL-NZP Tool TM insertion location	Fort Worth District requested training near the start of this project. We developed a biweekly outline of topics for online training sessions and used this schedule to develop the related, but condensed and highly edited, training videos. The usual course of action was to prepare for the training session, perform the training session, then use any comment or questions about the session to write the script for the associated training video. This method allowed us to learn from the teaching sessions and produce scripts that directly address common questions. During the project it was determined that adding links to the videos inside the SMPL-NZP Tool would not be best at this time. This was decided because many of the pages are still undergoing changes and adding links at a later time would not require very much effort. As an alternative, the videos were numbered sequentially and placed in a playlist to help the viewer find the topic they are looking for and progress through the training.	section 4.1 para 1 & section 4.2 para 1
Produce first draft video and insert in SMPL-NZP	Draft videos for each topic were usually produced before the training session. The draft video for the first topic was produced on December 15th. It was published to the YouTube site later that week.	Section 4.1 para 2
Produce all draft videos	All draft videos had been produced as of the end of July. These videos were each edited and approved within a week of the production of the draft video. In an effort to add value to the YouTube channel, the training sessions themselves were usually uploaded (unedited) as well. This is meant to provide an additional resource if further understanding of the topic is needed.	Section 4.1 para 2
Review full video set	All of the tutorial videos went through a video editing process and were then re-reviewed by the technical leads of this project before being published to the SMPL-NZP Tool YouTube channel.	Section 4.1 para 2
Insert all videos in the SMPL-NZP Tool	As mentioned above, links to the videos have not been placed on each page of the tool. However, a link to the SMPL-NZP Tool YouTube channel (where all the videos reside) has been placed on the homepage of the SMPL-NZP Tool.	section 4.2 para 2

Final documentation and videos for full tutorial set	A full set of tutorial videos covering usage of the entire tool have been completed. These videos can be found at the following link: https://www.youtube.com/channel/UC2sdFPLVc5TENXyuRL4SzNw	Section 4.1 para 5

The following information, presented in brief in Table 1, provides full description of each milestone:

SMPL-NZP Tool™ RMF Process

- Make database changes to meet security requirements:
  - Make any database modifications necessary to mitigate security infractions. Make changes prior to beginning RMF documentation so as to support a stable release version for RMF accreditation assessment. Further database modifications may be necessary during the final stages of RMF accreditation assessment.
- Make database changes to accommodate necessary functionality feature:
  - Make any database modifications necessary accommodate necessary functionality, as requested by the customers for ease of use. Make changes prior to beginning RMF documentation so as to support a stable release version for RMF accreditation assessment.
- Document System Architecture, network architecture, Security Architecture, and any other documentation that will not change with development:
  - Complete as much system documentation and definition documentation as feasible prior to or in accordance with above mentioned system changes. Complete the documentation prior beginning of RMF documentation, and make necessary changes in the final stages of RMF accreditation assessment as necessary.
- Move core functionality to new interface:
- Interface feature freeze for RMF process:
  - Make any interface modifications necessary accommodate functionality, as requested by the customers for ease of use. Make changes prior to beginning RMF documentation, and freeze changes so as to support a stable release version for RMF accreditation assessment.
- Complete testing and record/ document test results:
  - Complete testing of modifications and additions made prior to the beginning of RMF documentation
- Document database, services, and other changes from development:
  - Complete testing of modifications and additions made prior to the beginning of RMF documentation
- Submission of Documentation for RMF- Assess only:
  - Complete a full RMF accreditation assessment package, undergo RMF pre-assessment and develop any supporting documentation and POA&Ms to complete the package for submission.

- Gain RMF Assess only authorization
    - Receive an ATO via the acceptance of RMF accreditation assessment package.
- Document RMF process:
    - Document the full process of the RMF accreditation assessment preparation and submission to attain an ATO.

Software Security Report

- Software Security Report Draft
- Final Software Security Process Report

SMPL-NZP Tool™ Video Tutorials

- Develop Tutorial video Scrips and SMPL-NZP Tool™ insertion location:
    - Determine the needed content and develop the scripts for training and tutorial videos, and determine the appropriate hosting location in accordance to security restrictions
- Produce first draft video and insert in SMPL-NZP; document the process:
    - Produce a single draft training video. Document the process as a template to streamline further video development and to record supporting evidence to the scalability supported by scalable innovative training solutions.
- Produce all draft videos:
    - Using the afore mentioned production-template, produce all draft training videos
- Review full video set:
    - Review all training videos for accuracy and effectiveness. Make modifications as necessary.
- Insert all videos in the SMPL-NZP Tool:
    - Insert all videos in the SMPL-NZP Tool™ for ease of access, in accordance with security restrictions
- Final documentation and videos for full tutorial set:
    - Produce appropriate documentation and organization tactics to support the effectiveness of a video training solution

4.0 TRAINING AND SCALABILITY REQUIREMENTS FOR SUCCESSFUL TECHNOLOGY TRANSFER

Due to the extensive and complex process of using the SMPL-NZP Tool™ to provide data for Sustainability Component Plans (SCP's), it is found that a significant amount of training must be provided. However, in-person training events are both time consuming and expensive. To combat this problem and increase scalability across multiple districts and many installations, an automated form of training was required. A fully encompassing training solution could not be developed without a prepared release version of the software system. Developing these training videos was part of this project.

4.1 VIDEOS AND TRAINING METHOD

The production of the SMPL-NZP Tool™ training videos came at an opportune time in the transfer of the tool to district personnel. During FY15 district personnel requested a reoccurring virtual training session to occur every two weeks. A schedule was developed to walk through the SMPL-NZP Tool™ in approximately 20 sessions and this schedule guided the framework for deadlines related to development of training videos. The training scripts were developed around these guidelines and training was split into two sections: course videos and training sessions.

The video scripts were modeled to mimic the training offered in live training event. The first draft video was produced using the trainees as the test group. After the review and acceptance of the first draft video, the production of all draft training videos moved forward. It took ~6 to 7 months to film and produce the full suite of training and course videos. The trainees provided feedback on the effectiveness of training materials and provided recommendations for improved material. Modifications were made and the final videos were released to cover information as follows.

Course videos are the full version of recorded training sessions for the purposes of educating installation-level planners. These videos have been included to fully encompass a usage scenario when going through the steps and processes of the tool. Additionally, course videos include a question and answers section potentially addressing valuable-helpful information and knowledge gaps. These videos span an average run-time of forty-five minutes.

Training Videos are demonstrations of specifically detailed aspects and scenarios of the tool. Videos are recorded by a training professional and are meant to guide the user through a standard tool process. These videos are shorter in length and are beneficial for users who wish to know how to access and utilize a specific part of the tool. Training videos are concise and topic specific.

Addressing final documentation and videos for full tutorial set, video playlists have been created for each set of videos. Each playlist guides the viewer through the material in the intended order. These videos allow the material to be viewed and re-viewed by district and installation personnel all over the world. Videos on the channel have already received several hundred views and are now a standard of the SMPL-NZP Tool™ new-user training.

4.2 TRAINING MEDIUM

An innovative aspect to the proposed approach is the use of YouTube to host tutorial videos. YouTube was chosen as the insertion location because it provides free hosting and marketing for the SMPL-NZP Tool™. Open access to these videos allows users to view and share the material, even when outside of DoD networks.

It was initially planned SMPL-NZP Tool™ would insert all training videos in the SMPL-NZP Tool™; however, a link to the hosting YouTube channel was added on the opening page of SMPL-NZP Tool™. This link was intentionally placed for access prior to login. Any external links are prior to the login so as to fortify the systems' security posture.

With the SMPL-NZP Tool™ tutorial videos being accessible as a standalone, scalable training platform the tool can properly transition into a production level with scaled demand not requiring any additional time or monetary commitment from the team. Additionally, utilizing a public medium such as YouTube allows accessibility to the entire DoD and also spurs interest from the public domain toward DoD Net Zero initiatives.

4.3 SCALABILITY

Scalability requires first a stable software platform on which to train users. YouTube training videos provide the additional scalability the SMPL-NZP Tool™ requires to advance to an enterprise production level. With the ubiquity of the YouTube platform and its propensity to draw public attention to Net Zero initiatives, bolstering both public support of the platform and increasing accessibility by government contractors and employees.

Additionally, the accessibility of the YouTube platform decreases the labor and transportation costs associated with providing live training sessions. Since the videos will be accessible on YouTube indefinitely, trainees have the option to re-review valuable training sessions and tutorials. This provides the option for trainees to re-learn any information when they begin to encounter real world scenarios while operating the tool.

These aforementioned benefits wholly contribute to the overall scalability of the SMPL-NZP Tool™ platform. YouTube provides a simple solution to any training scalability problems previously encountered with training on the tool. With YouTube implemented as the training vehicle for the tool, the SMPL-NZP Tool™ can properly scale to meet the increased training and education demands that arise from transitioning the tool to the enterprise production level.

4.4 TIME AND COST SAVINGS

The SMPL-NZP Tool™ development team led many training events before the release of the training videos. These events typically involved the efforts of 3 people over 4-5 days and required travel for the group. The cost for this type of event was approximately $20,000 determined by costs of previous courses. Additionally these efforts removed the development team from their main focus of further advancing the capabilities of the SMPL-NZP Tool™. This was a particularly substantial concern when attempting to extend the SMPL-NZP Tool™ capabilities to additional districts. As of 2017 a Prospect Training Course has been developed and is now and annual event. The training videos are being used by these students, self-paced, as reviews or a deeper dive on sections of the Tool.

4.5 ACCESSING THE TRAINING

The training is available to any individual with access to the internet and the YouTube site. Simply by searching "SMPL-NZP Tool" in the search criteria on the YouTube site, the user can access the full playlist of videos that has been created to go over SMPL-NZP Tool™ material. The SMPL-NZP Tool™ YouTube channel is accessible through the following URL: https://www.youtube.com/channel/UC2sdFPLVc5TENXyuRL4SzNw.

Training and Course videos and their runtimes are listed on the following two pages in Table 2. "Tutorial Videos for an Energy Efficiency Technology transitioning to a production environment."

Technology Transfer

Table 2. Tutorial Videos for an Energy Efficiency Technology transitioning to a production environment

	Name	Runtime
1	SMPL-NZP Tool Standard Operating Procedure Document	7:08
2	GIS and Facility Preparation	13:00
3	Registration	4:03
4	Beginning a Study in the Tool	5:16
5	Adding Facilities to a Study in the SMPL-NZP Tool	5:25
6	Modifying Viewing Facility Data in Study SMPL-NZP Tool	11:31
7	Modifying Viewing Facility Data in Study SMPL-NZP Tool	6:20
8	Enter Utility Consumption Data	5:48
9	Manage Users	1:18
10	Consumption Overview Report and Study Calibration Discussion	6:02
11	Creating Facility Loads Baseline Pt 1	15:28
12	Creating Facility Loads Baseline Pt 2	20:30
13	Creating Facility Loads Baseline Pt 3	5:31
14	Installation - Making and Using Clusters	6:06
15	Installation - Equipment and Measures	23:38

SMPL-NZP Tool™ Training and Course Video listing

Technology Transfer

Table 2. Tutorial Videos for an Energy Efficiency Technology transitioning to a production environment

	Name	Runtime
16	Installation - Constraints and Optimization	13:06
17	Installation - Baseline Results	6:25
18	Facility Baseline Calibration Discussion and Consumption Update	16:17
19	Facility - Creating Base Case and Process Review	30:15
20	Installation- Base-case	36:25
21	Facility Efficiency Measure Costing	27:33
22	Installation - Scale Equipment Costing	33:57
23	Facility Adding the Better Case	33:00
24	Facility Adding the Best Case	7:53
25	Facility Report Review	35:36
26	Installation Section - Better and Best Scenarios	21:18
27	Creating Additional Supply Scenarios (Cogeneration and Renewables)	42:37
28	MCDA Multi Criteria Decision Analysis Creation Part 1	26:32
29	MCDA Multi Criteria Decision Analysis Creation Part 2	43:52

SMPL-NZP Tool™ Training and Course Video listing

As illustrated by Table 2, the videos vary significantly in length. The goal was to produce 5-15 minute videos in order to make it easier to learn the material, but some of the later topics required more time to explain important details.

The videos included in the playlist can best be split into two categories: videos that seek to demonstrate a process and videos that seek to better explain a process. For instance, the "Manage Users" video is around one minute long. This video is purely to demonstrate how to change the permissions of users in your study. There is no extended explanation required with the process but rather a brief demonstration of which settings the user should alter to give the desired

permissions to the specific study user. On the other hand, there are videos such as the "MCDA Multi Criteria Decision Analysis Creation Part 1" which not only serves as a guide on how to use the tool, but also provides a deep analysis and explanation of how to examine the data within the tool and apply it to your study. In general, the later videos that cover demonstrate and explain more complicated processes have the longest durations.

5.0 RISK MANAGEMENT FRAMEWORK GUIDANCE: from SMPL-NZPTool Technology Transfer RMF Process Results

This presentation of RMF guidance is based on the findings of the RMF investigation and SMPL-NZP Tool™ field trial, seeking an ATO. The guidance is presented in the logical order by which the results suggest steps be performed.

5.1 GETTING STARTED

5.1.1 Understanding RMF

It is recommended all key software system or application contributors, involved in the early stages of RMF, receive high level RMF training. Training should cover the basics of RMF. The high level knowledge will benefit the contributors in developing an RMF team and preparing for the RMF accreditation assessment. Understanding the premises and expectations of RMF before beginning the accreditation process will aid in software engineering decisions. Those receiving early high level RMF training will be key in navigating the RMF prerequisites: identifying the system and environment, identifying the targeted hosting location, identifying the RMF stake holders and developing an RMF awareness plan.

It is further recommended any software system preparing for RMF specify a primary POC for RMF intelligence. This will be the RMF lead for the systems' internal RMF training and preparation efforts.

In the SMPL-NZP Tool™ investigation Program/Project Managers (PMs), Lead Developers and the Information System Security Engineer (ISSE) received or were briefed on RMF fundamentals as outlined in the BAI Information Security Consulting & Training RMF for DoD IT Fundamentals training course (BAI Information Security Consulting & Training , 2014).

See Appendix B: RMF Prerequisites, Understand the RMF Steps for a brief overview of RMF requirements.

5.1.2 Know the System and Environment

It is recommended the internal RMF POC, or delegate, compile a full system description as recommended and outlined by Appendix B: RMF Prerequisites, Understand the System and Environment and Understand the Financial Plan. This system description will be the foundation of knowledge in preparation of formal RMF documents and in mitigation strategies, to close gaps on software engineering and RMF requirements.

SMPL-NZP Tool™ completed a full system description with boundary definitions as defined in the ERDC Research and Development Environment. SMPL-NZP Tool™ boundaries with-in the targeted Corps Net enclave are under negotiations in the MOU.

Refer to BAI Information Security Consulting & Training RMF for DoD IT Fundamentals training course (BAI Information Security Consulting & Training , 2014) for guidance on defining the system boundary as discussed in Appendix B: RMF Prerequisites, Understand the System and Environment.

5.1.3 Identify the System Type and RMF requirement

All systems must be RMF assessed and registered. Not all systems require a full Assess and Authorize accreditation. Some require only the Assess-Only portion of RMF accreditation. The Assess and Authorize accreditation assessment requires an authorization through the full RMF life cycle where the Assess-Only requires only a risk assessment to define the security posture of the system. In Assess-Only the requirement for depth of RMF assessment is determined at the system level for insertion into the Enclave or hosting environment.

To determine the appropriate RMF accreditation the system type must first be defined. A system is first classified as an Information System (IS), Platform Information Technology (PIT) System, Information Technology (IT) Service, or an IT Product. The system classification determines the RMF requirements.

OMB and NIST publications identify two types of Information Systems (ISs): General Support System (GSS) or Enclave and Major Application (MA). A GSS is defined as "Interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people (BAI Information Security Consulting & Training , 2014)," according to BAI RMF for DoD IT Fundamentals. And an Enclave is defined as "A collection of information systems connected by one or more internal networks under the control of a single authority and security policy. These systems may be structured by physical proximity or by function, independent of location as listen in CNSSI 4009, National Information Assurance (IA) glossary. Found in the Knowledge Service document library (Knowledge Service, n.d.)" A GSS or Enclave assumes the highest security category of the ISs that they host. Its security needs are determined by the hosted systems. Enclaves has a physical environment, provides networking capability, offers basic services such as email and is usually a Common Control Provider. Example Enclaves include local area networks and their hosted applications, Backbone networks and Data processing centers.

A MA is defined as "An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application (BAI Information Security Consulting & Training , 2014)," according to BAI RMF for DoD IT Fundamentals. MA's administer software updates, maintain the database, and administer web interface updates. MA's develop and maintain the application, are likely on servers in an enclave, global work stations may access the application – but may not be part of the boundary and their data sensitivity often increases cyber security risk. MA's typically rely on a GSS for some of their security protection.

Any system classified as a IS be it GSS, Enclave or MA is required to undergo the full RMF life cycle of Assess and Authorize accreditation assessment before gaining an ATO.

PIT Systems encompass "A collection of PIT within an identified boundary under control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location, as read in DoDI 8500.01, Cybersecurity as found on Knowledge Service document library (Knowledge Service, n.d.)." These may be special purpose weapons or medical systems, and may or may not be connected to the DoD network. PIT

systems often have a higher impact level on Integrity or Availability from the CIA categorization see below. PIT Systems will have unique requirements and security controls. All PIT Systems, like IS's, must undergo the full RMF life cycle of Assess and Authorize accreditation assessment before gaining an ATO.

Systems not belonging to the IS (GSS, Enclave or MA) or PIT System categories likely fall into the PIT, IT Service or IT Product category. Systems in these three categories are required only the Assess-Only RMS assessment, and the depth of RMF assessment will be determined at the system level.

The following are defined under DoDI 8500.01 as listed in the Knowledge Service document library (Knowledge Service, n.d.):

- PIT includes "both hardware and software that is physically part of, dedicated to or esential in real time to the mission performace of special purpose systems." An example might be a radiology ysstem or X-ray machine.
- IT Service is "a capability provided to one or more DoD entities by an internal or external provided basedon the use of informaiton technology and that supports a DoD mission or business process. An IT Service consists of a combination of people processes and technology."
- IT Product includes "Individual IT hardware or software items. Products can be commercial or government provided and include, but are not limited to, operating systems, office productivity software, firewalls and routers."

It is important to properly define the system type so as to follow the appropriate RMF accreditation requirements. All systems type classifications will be assessed in the accreditaiton process, and any misclassified systems will not complete RMF accreditation assessment for an ATO.

SMPL-NZP Tool™ origionally planned to complete an RMF Assess-Only authorization package; however, at the time of SMPL-NZP Tool™'s RMF preparation the RMF Assess-Only requiremetns had not yet been released, also it was found after thurough investigation of the above informaiton SMPL-NZP Tool™ fit most appropriately into the MA classification, due to the size and nature of the tool, requiring a full RMF Assess and Authorize accreditaiton assessment.

5.1.4 Identify targeted Hosting location

RMF Guidance suggest a software system may undergo an RMF Type Authorization: one in which a pre-determined location need not be presented; however, the SMPL-NZP Tool™ investigation determined this is not an effective means of attaining an ATO. It is recommended any software system seeking an ATO determine the targeted hosting location before beginning any RMF documentation. The Targeted hosting location will impact every aspect of the RMF accreditation assessment process and documentation.

An RMF Type Authorization is said to be used to deploy copies of a software system in specified environments under a single Authorization Package. The Authorizing Official's (AO's) of each

hosting enclave must approve instillation of the system into their boundary. SMPL-NZP did not choose to attempt a Type Authorization, instead moved forward with a Security Authorization Package (SAP) targeting Corps Net as the hosting enclave.

In determining a targeted hosting enclave, many factors should be reviewed. The internal RMF POC should document parameters as outlined in the Appendix C: Production Environment Hosting Guidance. An Example Hosting comparison form, used to compare SMPL-NZP Tool™ candidate environments, may be referenced in Appendix D: Hosting Comparison_SMPL-NZP Tool™.

5.1.5 Identify the RMF stakeholders, develop an awareness plan

RMF accreditation requires an abundance of approved documentation. It is critical to have an outline of the organization and approving officials. An outline of the required RMF representatives and approving officials and their roles and responsibilities as relating to the RMF steps may be found in Appendix E: Identifying RMF Team. The approved stakeholders and RMF team will be identified in the RMF Core SAP. The Template SAP is listed on RMF Knowledge Service (Knowledge Service, n.d.).

Training and awareness needs of individual stakeholders and RMF team members should be identified in the early stages of RMF preparation. Guidance is offered on recommended training for participants of different levels of the RMF process in Appendix F: Identify Stakeholders and Develop Awareness Training Plan_ SMPL-NZP Tool™

5.1.6 Understanding RMF

Once the beginning stages of RMF preparation have been completed and an awareness plan has been established, In-depth training should be issued to participants as identified in the awareness plan. Identified personnel should receive in-depth RMF training prior to moving forward with RMF documentation.

In the SMPL-NZP Tool™ investigation, PM's and the ISSE received or were briefed on RMF in depth training as outlined in the BAI Information Security Consulting & Training RMF for DoD IT In-Depth training course (BAI Information Security Consulting & Training , 2014).

5.1.7 eMASS and Registration

Each software system must be registered with its specified DoD component cyber security program, for management and tracking. The registration identifies the system in the system inventory and informs the governing organization of any security implications during continuous monitoring.

SMPL-NZP Tool™ registered in Army Portfolio Management Solution (APMS) for a project number which is needed for eMASS. Each registration system has specific registration requirements. APMS requires system information focusing on scope, components, boundary and financials.

eMASS is a web system used for organizational management and tracking. Each organization has a unique instance of eMASS, and the organization determines the level of detail to be

provided in the SP. The security categorization is included, and the SP may be included or attached in the eMASS system.

For more information on the software systems' required DoD component cyber security program and eMASS instance refer to the organization's CIO Office.

5.2 INITIATE AND PLAN

5.2.1 Categorize System (RMF Step 1)

Categorize system in accordance with the CNSSI 1253. The system categorization is a formal definition of the information types processed, stored and transmitted by the system, qualifying the encompassed business lines. System categorization should include the identification of the final and official system mission statement, as well as, the systems information types. Guidance on development of the mission statement may be found in Reference: NIST SP800-60_Vol1 Rev1at the Knowledge Service Document Library (Knowledge Service, n.d.). Once the Mission statement and Information types have been established then the RMF should move forward with system categorization.

The information types as defined in NIST SP800-60_Vol2 (Knowledge Service, n.d.) provide full information type and categorization definitions. Once Information types have been selected and NIST SP800-60_Vol2 (Knowledge Service, n.d.) Special Factors have been reviewed, the provisional impact levels for each security objective: Confidentiality, Integrity and Availability (CIA) categorization is established.

Submit the Mission statement, Information Types and CIA security objective impact levels categorization to the proper Approving Official (AO) or delegate for approval. AO is defined in Appendix E: Identifying RMF Team, and varies on the final hosting location. An example of the SMPL-NZP Tool™ submission has been provided in Appendix G: Security Plan: Categorization.

Finally, Identify possible overlays as process is described in CNSSI 1253, reference CNSSI 1253 appendix F as located in the Knowledge Service Document Library (Knowledge Service, n.d.) for the full list of overlays. Overlays are determined by the types of system data. eMASS will be used to identify necessary overlays. The SMPL-NZP Tool™ did not require any overlays.

Key documents used in RMF Categorize System: Step 1
CNSSI 1253
NIST SP 900-60 Vol I Process Guidance
NIST SP 800-60 Vol II Appendices of Security categorization recommendations/ rationale

Key output in RMF Categorize System: Step 1
RMF CIA Security Objectives and Impact Levels Categorization

5.2.2 Select Security Controls (RMF Step 2)

Download the Security Authorization Package (SAP) with the latest list of controls from the Knowledge Service Document Library (Knowledge Service, n.d.). Select the identified/ approved CIA categorization. This selection will populate the necessary baseline controls for each given CIA security objective. See CNSSI 1253 Appendix D, Table D1 as hosted in the

Knowledge Service Document Library (Knowledge Service, n.d.) to reference the full baseline security control set.

The system should be registered in eMASS at this stage of RMF accreditation assessment preparation. SMPL-NZP experience recommends working with the spreadsheet and eMASS simultaneously. See Lessons learned for reasoning, section 7.1. eMASS should be used for control identification, while the spreadsheet is recommended for documenting implementation status.

For manually selecting the baseline control set follow CNSSI 1253, section 3.2.1 and use CNSSI 1253, Appendix D, Table D1 "NSS Security control Baselines" as hosted in Knowledge Service Document Library (Knowledge Service, n.d.).

Apply any overlays as identified in in the categorization step of RMF from CNSSI 1253: CNSSI appendix F "Overlays" (Knowledge Service, n.d.), then tailor the security controls baseline.

Follow component and local policy for tailoring the security controls baseline. Reference CNSSI 1253, section 3.2.2 Tailor the initial security control set and SP 800-53, section 3.2 "Tailoring Baseline Security Controls: Applying scope considerations" as hosted in Knowledge Service Document Library (Knowledge Service, n.d.) for further guidance. Follow by selecting compensating controls using afore mentioned references in addition to NIST SP800-53, Section 3.2 Tailoring Baseline security controls: Selecting Compensating controls (Knowledge Service, n.d.). Selecting compensating controls may not be required, determine by use of reference material.

Follow component and local policy and guidance for supplementing security control Baselines. Determine if any additional controls are required for technology, threats, enhanced assurance requirements etc... by referencing CNSSI 1253: section 3.2.2, Tailor the Initial Security Control Set, NIST SP 800-53 Section 3.2 Tailoring Baseline Security Controls: Supplementing Security Control Baselines, NIST SP 800-53 section 3.4 Documenting Control Selection Process, Implementation Tip, NIST SP 800-53 section 2.5 Assurance and Trustworthiness, NIST SP 800-53 Appendix E: Assurance and Trustworthiness as hosted on Knowledge Service Document Library (Knowledge Service, n.d.).

Assign organization defined parameters by using CNSSI 1253 Appendix E, Table E-1 "Security Control Parameter values for NSS" hosted on Knowledge Service Document Library (Knowledge Service, n.d.), and finally Identify the Common controls.

Follow component and local policy and guidance for Common control Selection. Reference DoDi 8510.01, Paragraph 2.b (1), common control identification and NIST SP 800-53, section 3.2 Tailoring Baseline, Identifying and Designating Common Controls as hosted on Knowledge Service Document Library (Knowledge Service, n.d.)

Document all decisions and rational and justify all deviations in the Security Plan (SP). See reference CNSSI 1253, Table D-2, Additional Security Control Information – Justification (Knowledge Service, n.d.) for NSS Baselines. Once documentation is complete, then develop the continuous monitoring strategy.

Develop control level Continuous Monitoring Plan (CMP). The RMF accreditation will require each control be continuously monitored and proof of such. Each selected control requires a monitoring strategy. The SMPL-NZP CMP strategy includes a manual audit each fiscal year (FY) via Interview, test and/ or examination to assess each control. The CMP will be added to the Security Plan (SP).

The goal of the CMP is to provide information and documentation supporting informed risk management decisions. The Risk categorization (CIA) is the determining factor in frequency and rigor of monitoring, but all CMP must demonstrate subsets of all controls are assessed annually.

The CMP documents how continuous monitoring conveys security posture through demonstrating the effectiveness of security controls, providing a view of assets, quantify security metrics, enable prioritization for mitigation and clearly identifying deviations from expected results.

Finally, Review the Security Plan (SP) for any other necessary updates.

Key Documents used in RMF Select Security Controls: Step 2

- CNSSI 1235
- DoDi 8510
- NIST SP 800-53, Rev 4

Key Output in RMF Select Security Controls: Step 2

- Control level CMP, initialized
- Common Control Identification

5.3 IMPLEMENT AND VALIDATE

5.3.1 Implement Security Controls (RMF Step 3)

Knowledge Service (Knowledge Service, n.d.) provides guidance ensuring controls are implemented consistent to DoD and component architectures and standards and establishes mandatory configuration settings.

The beginning approach of a Tabletop review is recommended in BAI RMF Training (BAI Information Security Consulting & Training , 2014). This approach includes:

- Document the status of security controls as Implemented, Planned or Not Applicable (N/A) and document implementation and justification statements.

        - Implemented items will require justification, detailing the control addressed and reasoning
        - Planned implementation items require implementation statements. Implementation statements should prove each item meets requirements, list the responsible party and give evidence of desired outcome and how to test. Note: eMASS provides limited space so be prepared to reference supporting documentation.
        - N/A items require justification statements. Justification must provide valid proof item is not required.
    - Verify Common and NA controls
    - Initiate System Security Plan (SSP)
    - Identify additional implementation resources

The table top review is followed by the documentation of the Security Engineering Plan (SEP). The SEP includes the Privacy Impact Assessment (PIA) and Program Protection Plan (PPP)

Key documents used in RMF Implement Security Controls: Step 3

- CNSSI 1235
- DoDi 8510
- NIST SP 800-53, Rev 4

Key output in RMF Implement Security Controls: Step 3

- SSP, initialized
    - Control Implementation and Justification
    - SEP
    - PIA

5.3.2 Assess Security Controls (RMF Step 4)

Identify the security control assessment team and prepare for the security control assessment according to the plan. The Security Assessment Plan (SAP) will be developed by the Security Control Assessor (SCA) and approved. The SCA is assigned by the Senior Agency Information Security Officer (SISO). See Appendix E: Identifying RMF Team™ for more information on RMF roles and responsibilities. In the security control assessment, the RMF team should be prepared to address procedures involved to examine, interview and/ or test controls.

The SAP includes a round or testing prior to the formal security assessment. This Pre-assessment will ensure preparation for the formal RMF accreditation assessment. The Pre-assessment will exploit manual reviews, testing procedures and automated tools to analyze and scan the servers, database and interface and review documentation. The Pre-assessment reports communicate a provisional risk standing and include mitigation strategies.

In accordance to the pre-assessment report and security requirements, modifications should be made to the databases, servers, interface, documentation, and policies. Any high-level security infractions should be addressed by these measures.

SMPL-NZP Tool™ has completed a first round of pre-assessment via database, servers and application vulnerability scan. Mitigation strategies or justifications (see POA&M in section 5.4) have been written for all high-level security infractions, but have not yet been implemented.

The Security Assessment Report (SAR) is the output of the formal Security Control Assessment. The SAR communicates the systems risk standing and identifies a proposed mitigation strategy for any posed risk.

Following are the steps in Security Control Assessment phase:

- Develop and Approve the Security Assessment Plan (SAP)
- Assess Security Controls
- SCA Prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Key documents used in RMF Assess Security Controls: Step 4

- N/A

Key output in RMF Assess Security Controls: Step 4

- SAP
- SAR

5.4 CERTIFY AND ACCREDIT

5.4.1 Authorize System (RMF Step 5)

Using the evidence gathered in the SAR, the RMF team should prepare the POA&M to support evidence controls are planned or in-place. All weaknesses identified in the SAR should be traced to one or more planned controls.

Following are the steps in the Authorize System phase:

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO
- AO Conducts final Risk Determination
- AO Makes authorization decision

Key documents used in RMF Authorize System: Step 5

- N/A

Key output in RMF Authorize System: Step 5

- Prepared POA&M
- Complete SAP
- ATO Memo

5.5 MAINTAIN AND REVIEW, DECOMISSION

5.5.1 Monitor Security Controls (RMF Step 6)

A CMP should be established and implemented. The CMP should cover policy and include directive following:

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR, and POA&M
- Report security status to AO
- AO reviews report status
- Implement System Decommissioning strategy

6.0 COST ASSESSMENT

The documented estimates of a project undergoing transfer to an enterprise production environment include estimates specific to the SMPL-NZP Tool™ transfer.

6.1 COST MODEL

The cost model demonstrates costing implications specific to the SMPL-NZP Tool™ as were required for implementing RMF, as well as imposing scalability to match enterprise production quality. These costs are estimated from charges the program received when these steps were accomplished, or from cost estimates from surveying other programs in the process. This is what a program should initially budget to execute the RMF process for each of the steps taking into account the caveats specified below from lessons learned.

Technology Transfer

Table 3. Cost Model for an Energy Efficiency Technology transitioning to a production environment

Cost Element	Estimated Costs ($K)
RMF: Security Control Status	40
RMF: Informal Assessment	15
RMF: Corrective Development	30
RMF: Architecture Documents	25
RMF: Formal Assessment	50
RMF: Corrective RMF Documentation	10
RMF: Document Completion	10
RMF: Configuration Control Board (CCB)	20
Scalability: Feasibility Study	
Scalability: Training Development	

- RMF: Security Control Status: Self-assessment and authorization package completion are necessary to complete the RMF requirements.
- RMF: Informal Assessment: pre-assessment scans (internal security group scans) are necessary to determine current RMF standing and plan for adjustments to development and documentation.
- RMF: Corrective development: Unburdened man hours for corrective development are required to correct any developmental gaps which are found, through the pre-assessment scans, to exist outside of RMF requirements.
- RMF: Architecture documents: Complete architecture documents including Security Plan, DB, System Boundaries, Network, CCB documents, etc... Which are necessary to meet the RMF requirements.
- RMF: Formal RMF Assessment: An External RMF Team spends a week reviewing RMF package and system through manual review and automated tools and scans. The formal assessment is required to attain an ATO through RMF.
- RMF: Corrective RMF Documentation: Unburdened man hours for corrective RMF documentation are required to correct any lacking documentation needed to attain an ATO though RMF.
- RMF: RMF completion: Complete remaining RMF documentation and transition the system to a production environment
- RMF: Configuration Control Board (CCB): Set up a CCB with a charter and select users from Corps Districts and ERDC-Labs. The CCB will be required to fulfill requirements as defined in the RMF security documentation and to maintain the ATO through RMF.
- RMF: Scalability Feasibility study: A study must be conducted to determine the scalability needs for a system transferring to a production environment.
- Training development: In the specific case of SMPL-NZP Tool™ the scalability study revealed a gap in training. SMPL-NZP required the development of training materials to meet the scalable user volume

6.2 COST DRIVERS

Subject-specific factors may impact the necessary funding required during RMF implementation and transition to an enterprise production environment.

- Prior accreditation standing, i.e. if a system has an existing ATO through DIACAP, will directly influence the needed documentation and software development needs and thus resources required to navigate an RMF accreditation assessment.
- Prior RMF knowledge possessed by the development team may impact the required training and learning curve, thus time and resources required to navigate an RMF accreditation assessment.
- Existing resources, i.e. the size of the existing development team, will directly impact the need for acquired resources while navigating an RMF accreditation assessment.
- The current stage of software development and the state of pre-existing documentation, i.e. the documentation completed prior-to and during

development, will directly impact the time and resources required to navigate an RMF accreditation assessment.

- License cost for updating software technologies will directly impact the cost of an RMF accreditation. RMF accreditation may require technologies be updated to the latest available version.
- Proximity of the software development team to the software hosting location and of the hosting location to the nearest RMF assessment team may require more travel to complete the RMF accreditation. Impacting the required funding for the final RMF accreditation assessment.
- Gaps in scalability may impact the development and system modifications necessary to meet production quality. SMPL-NZP Tool™ showed a primary gap in production quality training solutions; however gap analysis will determine a systems specific scalability needs.
- The nature of the system may drive a need for added personnel and the extent of additional training to those personnel. Reviewing the CIA categorization will determine the security risk categorization of the system driving the training required for personnel and extensiveness of the RMF accreditation assessment. Further, the nature of the software specifics will dictate the learning curve and software training required to add developmental personnel capable of making modifications to the system. This risk may be minimized by ensuring individuals are cross trained on specific components of the software.
- The driving software need may impact the scaling rate of the system. There may be a need to grow the system at rapid rate, when the driving requirement is a critical mission. The rapid expansion rate will directly impact the timeline to complete an RMF accreditation and thus the time and resources needed to complete the transition to an enterprise production environment. SMPL-NZP Tool™ minimized the risk of expansion rate by producing automated training materials, thus minimizing the burden on the SMPL-NZP Tool™ development team.

6.3 ANNUAL ACCREDITATION COST

RMF accreditation requires a continuous monitoring policy. This policy requires a full annual review to all implemented controls. Maintaining an ATO though RMF cost an average of $20K annually. This cost includes the cost to maintain the CCB as well as undergo annual review.

7.0 IMPLEMENTATION ISSUES

7.1 Lessons Learned

Documented identification of factors which were found to hinder the RMF process. The issues listed are not identified as specifically hindering the SMPL-NZP Tool™ RMF accreditation assessment. Some of the lessons learned are items which SMPL-NZP Tool™ included at the early or pre-development stages, and found later that it was helpful to have implemented these prior to beginning development. These are the documented strategies which may benefit, or mitigate issues, transitioning to a production environment.

- Prior to beginning system development establish a dynamic Access Control Policy (ACP). Every hosting site has different requirements, if the policy is not established and dynamic enough to cover standard requirements prior to beginning system development, then the ACP may require redesign and the authentication method may require being re-written.
- Prior to beginning system development establish the requirements for and draft the Identification and Authentication Policy (IAP).
- Prior to beginning system development design an authentication method which fits a sustainable standard. Failure to design a sustainable authentication method will require a redesign and re-write of the authentication method during the RMF process and before gaining RMF accreditation, as well as, requiring a re-write of the IAP.
- Prior to beginning system development design and establish a method for auditing access control, as designed in the ACP.
    - Failure to implement an auditing mechanism would leave gaps in full documentation of access
    - Failure to implement an auditing mechanism could present threats via lack of exposure to unwarranted access
    - Failure to implement an auditing mechanism will present the need, at the time of RMF accreditation assessment, to do a full audit of system access and possibly to revoke all and reassign access to any necessary users.
- Prior to beginning system development design and establish a Configuration Control Policy (CCP) and CCB Charter. The established guidelines in the CCP will provide to software development standards. RMF accreditation assessment will require implementation and evidence of such for RMF accreditation.
- Prior to beginning system development design and establish a System Test Plan (STP). Failure to establish an STP will result in
    - No or lacking evidence to validate the ACP and auditing method, which will be required for RMF accreditation. The access control auditing mechanism must be prove valid through testing prior to acceptance in RMF.
    - No or lacking evidence to prove implemented CCP, which will be required for RMF accreditation. Evidence of an implemented test plan is required to support the CCP for RMF acceptance.
- During system development maintain, both, development documentation and task tracking. It is recommended that a formal task tracking system instance be

established for the development system prior to beginning system development. Failure to maintain both results in

  - No or lacking evidence to support claimed implemented CCP. Evidence of an implemented STP is required to support the CCP for RMF acceptance.

- During system development continually update the STP. Failure to continually update the STP will result in gaps supporting the CCP. Compliance results in aiding the RMF process by beginning with a fully updated system definition, defined in the STP. The establishment of a full system definition provides content for needed system training.
- Prior to beginning RMF documentation design and release system training materials. The lack of proper training materials hinders a systems scalability thus impacting its ability to successfully transition to a production environment.
- Prior to beginning RMF documentation identify the desired final hosting location. Failure to initiate the RMF accreditation assessment with a hosting location pre-determined will result in significant delays and set-backs toward RMF accreditation. It was previously though the RMF accreditation could easily transition from one production host to another, while documentation states this as so – logistically it appears implausible at the given time. Due to the impacting nature of hosting location on RMF, significant time and resources will be preserved by selecting a final hosting location prior to initiating RMF documentation.
- Prior to beginning RMF documentation all key system staff should receive high level RMF training. RMF Fundamentals is offered back-to-back with RMF in-depth which would lead users to believe they should be taken together. BAI Information Security Consulting & Training offers free online training to those enrolling in the face-to-face training, thus the recommendation would be to utilize the online training, for key staff, prior- to beginning RMF documentation. This will offer a basic understanding of the RMF process and expectations. After the initial “getting started phases” of the RMF, then it is recommended for all required persons to attend RMF in depth training. Breaking the training into two sections allows a good understanding of RMF prior to starting the documentation, and then a good understanding of the targeted system and its needs prior to starting in-depth training. The training recipients will gaining much more from the training with prior high level knowledge leading to a good baseline understand of the systems RMF needs.
- During RMF documentation have an understanding of the fluid RMF requirements. eMASS host the controls used in RMF categorization. There are several instances of eMASS, all of which may host different versions of the controls. SMPL-NZP uses the Army instance of eMASS, whose published control list is not the latest version of the control list. If Army eMASS choses to update the published control list prior to the completion of eMASS input, SMPL-NZP would be required to start their inputs from the very beginning. Rather it is recommended to visit RMF Knowledge Service and download the latest control list – inputting the controls manually after completing them off-line. This will mitigate the potential for having to input the controls multiple times.

8.0 REFERENCES

BAI Information Security Consulting & Training . (2014). *BAI informaiton Security Consulting & Training Risk Management Framework (RMF)* . Retrieved from BAI Training Programs: https://rmf.org/index.php/training-programs

Knowledge Service. (n.d.). Retrieved from RMF Knowledge Service : https://rmfks.osd.mil/rmf/Pages/default.aspx

Knowledge Service. (n.d.). *RMF Knowledge Service* . Retrieved from KS REfereence Library: https://rmfks.osd.mil/rmf/SiteResources/References/Pages/ReferenceLibrary.aspx

Windermere, A. (2016). *what is the Importance of Video Tutorials to Students?* Retrieved from Chron: http://work.chron.com/importance-video-tutorials-students-16633.html

9.0 APPENDICES

Appendix A: Points of Contact

POINT OF CONTACT Name	ORGANIZATION Name Address	Phone Fax E-mail	Role in Project
Richard J. Liesen, Ph.D.	ERDC, CERL	217-373-4572	PI – Energy Modeling Lead
Matthew M. Swanson, Ph.D.	ERDC, CERL	217-377-9337	Training Development - Lead
Michael P. Case, Ph.D.	ERDC, CERL	217-373-7259	SMPL-NZP Tool™ Program Manager
James T. Stinson, Ph.D.	ERDC, ITL	601-631-4494	Software Engineer - RMF
Timothy W. Garton	ERDC, ITL	601-634-2596	Software Engineer - RMF
Jessica Johnson	ERDC, ITL	601-634-5401	Software Engineer - RMF

Appendix B: RMF Prerequisites

This is a highlights list of RMF steps.

RMF Prerequisites

Begin the RMF by defining the following:

Know the System and Environment (Information Gathering)

- System name
- System mission and principal functions
- Type of information processed and its sensitivity
- User community
- System location
- System Components and connectivity
- System boundary
- Current authorization status

Understand the Financial Plan

- User Community (Current/Targeted)
- Funding
- Understand expected growth

Know the Players *(see Identifying Team)*

- Authorizing Official (AO) or AO Designated Representative
- ISSM/ISSO
- Information Owner(s)
- Other Key Resources

Know the Requirements

- Which DoD component cybersecurity program
- "Unique" security requirements
- Formal or Informal risk assessment

Understand the RMF Steps

Step 1: Categorize System

- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan
- Register system with component cybersecurity program
- Assign qualified personnel to RMF Roles

Step 2: Select Security Controls

- Select security controls
- Common control identification
- Apply overlays and tailor
- Develop system-level continuous monitoring strategy

- Review and approve the system security plan and continuous monitoring strategy

Step 3: Implement Security Controls

- Implement control solutions consistent with DoD component cybersecurity architectures
- Document security control implementation in the security plan

Step 4: Assess Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5: Authorize System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR, and POA&M) to AO
- AO conducts final risk determination
- AO Makes authorization decision

Step 6: Monitor Security Controls

- Determine impact of changes to system and environment
- Assess selected controls annually, conduct needed remediation and update security plan(SP), SAR and POA&M
- Report security status to AO, AO reviews reported status
- Implement system decommissioning strategy

Appendix C: Production Environment Hosting Guidance

This is a highlights list of RMF steps.

Production Environment Hosting Guidance

- Identify possible hosting locations
  - See Appendix D: Hosting Comparison_SMPL-NZP Tool™ for detailed information on Corps Net and DISA hosting
  - Identify a POC for each potential location
  - Identify online resources for each potential location
  - Identify for each potential location:
    - Pricing
    - Maintained control options
    - Hardware availability
    - Physical location
    - Technical requirements for hosting
  - List external resources which may be able to help in identifying hosting locations
    - Find a mentor: someone who has completed RMF and has previously done hosting location comparisons
- Note Impacting Regulations
    - Example: Some systems are required to be hosted on DISA and do not have an option. DISA regulation may be located at http://www.disa.mil/
  - Note Impacting Factors:
    - Example: How hosting in one location over another impacts the perception of a system
- Compare/contrast options
  - Show Example of SMPL-NZP comparison between hosting enclave as seen in Appendix D: Hosting Comparison_SMPL-NZP Tool™
- Identify selected DoD Component Cybersecurity Program

Appendix D: Hosting Comparison_ SMPL-NZP Tool™

This is a highlights list of RMF steps.

Hosting Comparison

System: SMPL-NZP Tool suite

Hosting considerations:

- DISA
- Corps Net

Identify Individual Hosting Requirements

(Use this section to identify the technical and functional hosting requirements – space, desired control, available funding)

- Two Servers:
  - SQL Server instance
    - Database server: 8C/16G (2C/16G)
  - IIS server Instance
    - Web Server: 4C/16 G (2C/8G)
- Desired control
  - Does not require Admin rights to server (prefer not to have admin rights to server)
  - Does not require access to the server
  - Would like to have database owner account, would accept an edit account
- Funding
  - See financial Plan
  - See current Hosting costs for CCE

Identify Impacting Regulations

(Any regulation which may impact the availability of hosting locations, i.e. some regulations may require a system of particular design to be hosted in a given location or prohibit a system of particular design to be hosted in a given location. Use this section to identify regulations and system design qualities which may impact the hosting location availability)

- Investigate regulations requiring enterprise systems being hosted on DISA

Identify impacting Factors

(Identify any outstanding factors which may impact the decision of a hosting location)

- SMPL-NZP Tool would like to be accepted as an Official Corps Application: Investigate implications of hosting location
- SMPL-NZP will require a hole punched – Is anyone willing to do so, do we really want to do it that way?

Resources

- DISA Resources
  - http://www.disa.mil/~/media/Files/DISA/Services/Computing/FY17Rates.pdf

    - http://www.disa.mil/Computing/Server-Hosting/Server-Hosting-and-Virtualization
- Corps Net Resources
    - No applicable web resources at this time

Point of Contact

- DISA: No listed POC, Web resources utilized
- Corps Net : Corps Net Infrastructure Operations Team Lead

Pricing

- DISA: see DISA pricing as listed under DISA Resources, web resources
- Corps Net: Corps Net pricing currently under negotiation

Control Options

- DISA : No known control options
- Corps Net : TBD: under MOU negotiations

Hardware Availability

- DISA: available for negotiation under MOU
- Corps Net: to be negotiated under MOU

Physical Location

- DISA
    - Servers located at Huntsville, AL Redstone Arsenal
    - Server Proximity: No close proximity to any development
- Corps Net
    - servers are located in Vicksburg, MS ERDC ITL bldg. 8000
    - Server proximity: Same Building as development Team

Appendix E: Identifying RMF Team

This is a highlights list of RMF steps.

<u>Identify Persons by RMF Role/ Responsibility [DIACAP reference]</u>

Tier 3 -System Level

- **Information System Security Manager (ISSM)/Information System Security Officer (ISSO) [IAM/ IAO]**
  - <u>ISSM</u>
    - Assigned at the Project level
    - Develop and maintain organizational cybersecurity program (architecture, requirements, policies, procedures, personnel)
    - Ensure information owners/stewards are identified
    - Appoint and oversee ISSOs
    - Maintain repository for cybersecurity documentation
    - Monitor compliance with security policy
    - Act as cybersecurity technical advisor
    - Respond to cybersecurity incidents and spillage
  - <u>ISSO</u>
    - Assigned by the ISSM
    - Assist ISSM
    - Enforce cybersecurity policies and procedures
    - Ensure users have appropriate clearances and authorization before access is granted
    - Ensure cybersecurity documentation is up-to-date and accessible to authorized individuals
  - <u>Responsibilities</u>
    - Step 1 Categorize Role: Supporter
      - Support the information owner/information system owner to complete security responsibilities
    - Step 2 Select Role: Supporter
      - Support the information system owner in selecting security controls for the information system
      - Participate in the selection of the organization's common security controls and in determining their suitability for use in the information system
      - Review the security controls regarding their adequacy in protecting the information and information system
    - Step 6 Monitor role: Supporter
      - Support the information owner/information system owner to complete security responsibilities
      - Participate in the formal configuration management process

- **Information Owner/ Steward (IO)**
    - Official with statutory, management or operational authority for specified information
    - Responsible for establishing policies and procedures for its generation, collection, processing, dissemination and disposal
    - May or may not be the Information System Owner
    - A single system may contain information from multiple IOs

- **Information System Owner (ISO) [Program Manager PM/ System Manager SM]**
    - <u>ISO</u>
        - Assumes responsibility of the system's security posture
        - Plan and budget for security control implementation, assessment and sustainment
        - Ensure users and support personnel receive cybersecurity training
        - Categorize each assigned system
        - Appoint a User Representative (UR)
        - Develop, maintain and track the Security Plan (SP)
    - <u>PM/SM</u>
        - Register the system per DoD component procedures
        - Appoint ISSM for each assigned system
        - Ensure each system has an assigned security engineer
        - Develop a system description
        - Implement RMF
        - Ensure RMF activities are aligned with acquisition process
        - Enforce AO authorization decision
        - Develop and track a POA&M for each system
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Categorize
        - Categorize the information system based on FIPS 199, NIST SP 800-60, and organizational guidance
        - Document the categorization decision
        - Gain approval for the categorization decision
        - Maintain the categorization decision
    - Step 2 Select Role: Selector
        - Select, tailor, and supplement the security controls following organizational guidance, documenting the decisions in the security plan with appropriate rationale for the decisions
        - Determine the suitability of common controls for use in the information system

        - Determine the need for use restrictions in the information system
        - Determine the assurance measures that meet the NIST SP 800-53 minimum assurance requirements selected for the system
        - Document the tailored and supplemented set of security controls in the security plan in sufficient detail to enable a compliant implementation of the control
        - Define the continuous monitoring strategy for the information system
        - Obtain approval for the tailored and supplemented security controls, common controls, compensating controls, use restrictions, and assurance requirements prior to their implementation
        - Review the security controls periodically and, when necessary, update the security control selections
        - Maintain and update the system security plan
    - Step 6 Monitor Role: Monitor
        - Develop and document a continuous monitoring strategy for their information systems
        - Participate in the organization's configuration management process
        - Establish and maintain an inventory of the information system's components
        - Conduct security impact analyses on all changes to their information systems
        - Conduct security assessments of security controls according to their continuous monitoring strategies
        - Prepare and submit security status reports at the organization-defined frequency
        - Conduct remediation activities as necessary to maintain the current authorization status
        - Update the selection of security controls for the information system when events occur that indicate the baseline set of security controls is no longer adequate to protect the system
        - Update critical security documents on a regular basis
        - Review reports from common control providers to verify that the common control continues to provide adequate protection for the information system

- **Information Security Architect (ISA)**
    - Ensures security requirements are integrated into enterprise architecture
    - <u>Responsibilities</u>
    - Step 2 Select Role: Advisor

        - Ensure the selection of security controls is consistent with the enterprise architecture, including reference models and segment and solution architectures

- **Information System Security Engineer (ISSE)**
    - Ensures security requirements are integrated into information system and product acquisition, design and configuration
    - This is a development role
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Advisor
        - Provide advice in establishing or validating the system boundary
        - Provide advice in describing the information system, its functions, and information types
    - Step 2 Select Role: Advisor
        - Provide advice in describing the system and its functions, information types, operating environments, and security requirements
        - Review the adequacy of the security controls and their ability to protect the information system and its information
        - Assist in tailoring the security controls
        - Assist in determining the assurance measures that can be used to meet the minimum assurance requirements
    - Step 6 Monitor role: Advisor
        - Provide advice on the continuous monitoring of the information system
        - Provide advice on the impacts of system changes to the security of the system
        - Participate in the configuration management process
        - Participate in any acquisition/development activities that are required to implement a system change
        - Implement approved system changes

- **Authorizing Official (AO) [Designated Approving/ accrediting authority – DAA]**
    - Senior level government employee within mission owner organization – appointed by component Head
    - Authorization Decision cannot be delegated
    - <u>AO</u>
        - Make Authorization decisions for IS and PIT systems within their purview
        - Ensure RMF tasks are completed and documented

        - Track POA&Ms
        - Ensure appointees to cybersecurity positions have written statements of responsibilities
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Approver
        - Review and approve the security category and impact level assigned to the information types and information system
    - Step 2 Select Role: Approver
        - Review the security plan to determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system
        - Determine if the security plan correctly identifies the potential risk to organizational operations, assets, individuals, other organizations, and the Nation and recommend changes to the plan if it is insufficient
        - Approve the selected set of security controls, including all tailoring and supplementation decisions, any use restrictions, and the minimum assurance requirements

    - Step 6 Monitor Role: Approver
        - Ensure the security posture of the organization's information systems is maintained
        - Review security status reports and critical security documents and determine if the risk to the organization of operating the system remains acceptable
        - Determine whether significant information system changes require reauthorization actions for the information system under their purview
        - Reauthorize information systems when required

- **User representative (UR)**
    - Represent the operational interests of the user community in the RMF process
    - Role is typically filled by UR on CCB
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Advisor
        - Identify mission, business, and operational security requirements
        - Identify data elements and information types contained in the information system
        - Identify how the information types are used to support the mission/business requirements
    - Step 2 Select Role: Advisor
        - Identify mission, business, or operational security requirements

        - Report any weaknesses in, or new requirements for, current system operations
    - Step 6 Monitor Role: Advisor
        - Identify changes to mission, business, or operational security requirements
        - Report any weaknesses in, or new requirements for, current system operations
        - Submit and justify system change requests to the information owner/information system owner or through the organization's formal configuration management process

- **Assessment Teams (certification Teams)**
    - Step 6 Monitor Role: Assessor
        - Develop a security assessment plan for each subset of security controls that will be assessed
        - Submit the security assessment plan for approval prior to conducting the assessment
        - Conduct the assessment of security controls as defined in the security assessment plan
        - Update the security assessment report on a regular basis with the continuous monitoring assessment results
        - HPC Cyber Readiness Team (CRT)

Tier 2 (Organizational Level)

- **Security Control Assessor (SCA) [Certifying Authority – CA]**
    - The SCA will be hired, provide assessment teams and produce the Security Assessment Report (SAR)
    - Step 1 Categorize Role: Assessor
    - Step 2 Select Role: Assessor
    - Step 6 Monitor role: Assessor
        - Develop a security assessment plan for each subset of security controls that will be assessed
        - Submit the security assessment plan for approval prior to conducting the assessment
        - Conduct the assessment of security controls as defined in the security assessment plan
        - Update the security assessment report on a regular basis with the continuous monitoring assessment results

- **Common Control Provider**
    - Responsible for the development, implementation, assessment and monitoring of common controls (i.e., security controls inherited by information systems).
    - This is the (targeted) enclave and/or governing organization

- <u>Responsibilities</u>
- Step 1 Categorize Role: categorizer
    - Determine the most appropriate and cost-effective security category and impact level for the common controls to best accommodate the information systems using the controls
    - Document the categorization decision in a system security plan or equivalent document
    - Gain approval for the categorization decision
    - Maintain the categorization decision
- Step 2 Select Role: Selector
    - Tailor and supplement the common security controls following organizational guidance
    - Document the assigned common security controls for the organization in sufficient detail to enable a compliant implementation of the control and maintain the documentation
    - Disseminate the security documentation associated with the common controls to information system owners that employ the common control in their information system
    - Define the continuous monitoring strategy for the common controls
- Step 6 Monitor Role: Monitor
    - Develop and document a continuous monitoring strategy for their assigned common controls
    - Participate in the organization's configuration management process
    - Establish and maintain an inventory of components associated with the common control
    - Conduct security impact analyses on all changes that affect their common controls
    - Conduct security assessments of the common security controls as defined in the common control provider's continuous monitoring strategy
    - Prepare and submit security status reports at the organization-defined frequency
    - Conduct remediation activities as necessary to maintain the current authorization status
    - Update critical security documents on a regular basis and distribute them to individual information owners/ information system owners and other senior leaders

- **Senior Agency Information Security Officer (SISO)/ Information Security Program Office – has SCA function, but may delegate [SIAO – has CA function]**
    - Government Employee only

- Directs agency efforts to achieve more secure information and systems in accordance with FISMA
- Serves as primary liaison between CIO and other information security personnel within the agency
- May serve as authorizing official AO designated representative or Security Control Assessor
- <u>Responsibilities</u>
- Step 1 Categorize Role: Coordinator
    - Establish and implement the organization-wide categorization guidance
    - Coordinate with the enterprise architecture group to integrate organizational information types into the enterprise architecture
    - Define organization-specific information types (additional to NIST SP 800-60) and distribute them to information owners/information system owners
    - Lead the organization-wide categorization process to ensure consistent impact levels for the organization's information systems
    - Acquire or develop categorization tools or templates
    - Provide security categorization training
- Step 2 Select Role: Coordinator
    - Develop organization-wide security control selection guidance consistent with the organization's risk management strategy
    - Assign responsibility for common controls to individuals or organizations
    - Establish and maintain a catalog of the organization's common security controls
    - Review the common security controls periodically and, when necessary, update the common security control selections
    - Define and disseminate organization-defined parameter values for relevant security controls Acquire/develop and maintain tools, templates, or checklists to support the security control selection process and the development of system security plans
    - Develop an organization-wide continuous monitoring strategy
    - Provide training on selecting security controls and documenting them in the security plan
    - Lead the organization's process for selecting security controls consistent with the organizational guidance
- Step 6 Monitor Role: Coordinator
    - Establish, implement, and maintain the organization's continuous monitoring program
    - Develop organizational guidance for continuous monitoring of information systems

        - Develop configuration guidance for the organization's information technologies
        - Consolidate and analyze plans of action and milestones to determine organizational security weaknesses and deficiencies
        - Acquire/develop and maintain automated tools to support security authorization and continuous monitoring
        - Provide training on the organization's continuous monitoring process
        - Provide support to information owners/information system owners on how to develop and implement continuous monitoring strategies for their information systems

Tier 1 (Executive Level)

- **Risk Executive, DoD Information Security Risk Management Committee (ISRMC) [Defense Information Systems Network – DISN-/ Global Information Grid –GIG- Flag Panel]**
    - Government employee only
    - Individual or group that helps ensure risks are viewed consistently from an organization-wide perspective
    - Develops organization-wide risk management strategy
    - Head of Agency (CEO) may fulfill this role or delegate to another official or group/committee
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Overseer
        - Provide oversight to the categorization process to ensure organizational risk to mission and business success is considered in decision making
        - Provide an organization-wide forum to consider all sources of risk, including aggregated risk from individual information systems
        - Promote collaboration and cooperation among organizational entities
        - Facilitate the sharing of security risk-related information among authorizing officials
    - Step 2 Select Role: Overseer
        - Define the organization's risk management strategy with respect to the selection of security controls
        - Promote the use of common controls to more effectively use organizational resources
        - Promote collaboration and cooperation among organizational entities
    - Step 6 Monitor Role: Overseer
        - Provide oversight to the risk management process to ensure organizational risk to mission and business success is considered in decision making

        - Provide an organization-wide forum to consider all sources of risk, including aggregated risk from individual information systems
        - Promote collaboration and cooperation among organizational entities
        - Facilitate the sharing of security risk-related information among authorizing officials

- **Chief Information Officer (CIO)**
    - Government employee only
    - Develops and maintains information security policies and procedures to address all applicable requirements
    - Reports annually to the agency head on the effectiveness of the Information security program
    - The CIO is a government appointment
    - <u>Responsibilities</u>
    - Step 1 Categorize Role: Leader
        - Ensure an effective categorization process is established and implemented for the organization
        - Establish expectations/requirements for the organization's categorization process
        - Provide resources to support information and information system categorization
        - Establish organizational relationships and connections
        - Ensure the information system's categorization is approved prior to selecting and implementing the security controls
    - Step 2 Select Role: Leader
        - Establish expectations for the security control selection and ongoing monitoring processes to provide a more consistent identification of security controls throughout the organization
        - Provide resources as needed to support information system owners when selecting security controls
        - Ensure the organization's risk management strategy is integrated into the enterprise architecture
        - Participate in the selection and approval of organizational level common security controls
        - Maintain organizational relationships and connections
    - Step 6 Monitor Role: Leader
        - Ensure an effective continuous monitoring program is established for the organization
        - Establish expectations/requirements for the organization's continuous monitoring process
        - Provide funding, personnel, and other resources to support continuous monitoring

        - Maintain high-level communications and working group relationships among organizational entities
        - Ensure that information systems are covered by an approved security plan, are authorized to operate, and are monitored throughout the system development life cycle

- **Chief Executive Officer (CEO) Head of Agency**
    - Government employee only
    - Overall responsibility to provide information security protection
    - Establishes and maintains organization-wide commitment to information security and risk management

Appendix F: Identify Stakeholders and Develop Awareness Training Plan_ SMPL-NZP Tool™

Identify the stake holders, by the following groups, based on what they need to know and their level of involvement with the RMF process. The identified stakeholders will be involved with the RMF team to some capacity

Executive Level (Those providing funding or providing the need for the product)

- No Formal RMF training required
- High level understanding of RMF approval implications needed

Organization
Frank Holcomb, Associate Director CASI
Alan Anderson, Technical Director Military Ranges & Lands

USACE HQ Proponent
Jerry Zeckert, Chief Master Planner, CoE
Andrea Kuhn, Master Planner, CoE

Mid-Management Level (Those responsible for funding and Requirements)

- Minimum RMF training required
- High level understanding of RMF needed
- Need to understand the responsibilities of their role

Program Manager
Michael P Case, PhD
Michael.P.Case@usace.army.mil

Program Manager
Richard J Liesen, PhD
Richard.J.Liesen@usace.army.mil

Project Team (Development Team, Technical Writers and CCB)

- Detailed RMF training required
- All developers must understand the full requirements of RMF development needs
- Only the ISSE will require knowledge to full RMF documentation needs, ISSE can advise development team

Development Team
James T Stinson, PhD
James.T.Stinson@erdc.dren.mil

Development Team
Timothy W Garton
Timothy.w.Garton@erdc.dren.mil

Development Team
Matthew Swanson, PhD
Matthew.M.Swanson@usace.army.mil

Technical Writer
Jessica A Johnson
Jessica.A.Johnson@erdc.dren.mil

SMPL-NZP Tool CCB Voting Members, CCB
SEE CCB (CCB Charter in development)

Extended Project Team (Network Team)

- Not responsible for network team RMF training

ERDC, ITL RDE_CCE Representative
Jarred R Taylor
Jarred.R.Taylor@erdc.dren.mil
ERDC, ITL RDE_CCE Representative
Sierra C Wells
Sierra.c.wells@erdc.dren.mil

POC's (The POC's required to complete the RMF Process, Security Team - AO)

Other (User Representative)

SMPL-NZP Tool CCB User Representatives
SEE CCB (CCB Charter in development)

Appendix G: Security Plan: Categorization

Engineer Research and Development Center

Net Zero Planner

System Categorization

SP-CAT-01.01

Dr. Michael P. Case, Dr. Richard J. Liesen, Dr. Mathew M. Swanson

CEERD-CERL

2902 Newmark Drive

Champaign, IL 61826-9005

Dr. James T. Stinson, Jessica A. Johnson, Timothy W. Garton

CEERD-ITL

3909 Halls Ferry Road

Vicksburg, MS 39180-6199

October 29, 2018

Innovative solutions for a safer, better world

THIS PAGE INTENTIONALLY LEFT BLAN

Contact Information

Name	Email	Phone Number
Case, Dr. Michael P.	Michael.P.Case@usace.army.mil	(217)373-7259
Liesen, Dr. Richard J.	Richard.J.Liesen@usace.army.mil	(740)366-0165
Swanson, Dr. Mathew M.	Matthew.M.Swanson@usace.army.mil	(217)377-9337
Stinson, Dr. James T.	James.T.Stinson@erdc.dren.mil	(601)631-4494
Johnson, Jessica A.	Jessica.A.Johnson@erdc.dren.mil	(601)634-5401
Garton, Timothy W.	Timothy.W.Garton@usace.army.mil	(601)634-2596

Abstract

This document covers the selection of information types associated with the System Master PLanner - Net Zero Planner (NZP) application along with the associated categorization in accordance with CNSSI 1253 for the three security objectives; Confidentiality, Integrity, and Accessibility (CIA). All categorization is in accordance with NIST SP 800-60 recommendations with adjustments noted as necessary.

Figures, Tables, and Equations

Figures

No table of figures entries found.

Tables

Table 1 - C.2.3.1 Budget Formulation Categorization 7
Table 2 - C.2.3.2 Capital Planning Categorization 7
Table 3 - C.2.3.4 Strategic Planning Categorization 7
Table 4 - C.3.1.1 Facilities, Fleet, and Equipment Management Categorization 8
Table 5 - D.7.2 Energy Conservation and Preparedness Categorization 8
Table 6 - D.8.2 Environmental Remediation Categorization 9
Table 7 - D.8.3 Pollution Prevention and Control Categorization 9
Table 8 – System Categorization 9

Equations

No table of figures entries found.

Mission Supported

The Sustainability and Resiliency Planner and Operations (SRPOTM) system provides installation and community sustainability planning, decision support, simulation, and research services in the areas of energy, water, solid waste, and storm water. SRPOTM includes the SMPL-NZPTM Tool. These services are offered to DoD Components (Army, Air Force, Navy, Marine Corps), Federal agencies, and state and local governments.

Information Types

C.2.3.1 Budget Formulation

Budget Formulation involves all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities. Subject to exception conditions described below, the recommended security categorization for the budget formulation information type is as follows:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

C.2.3.2 Capital Planning

Capital Planning involves the processes for ensuring that appropriate investments are selected for capital expenditures. The recommended provisional security categorization for capital planning information is as follows:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

C.2.3.4 Strategic Planning

Strategic Planning entails the determination of long-term goals and the identification of the best approach for achieving those goals. The recommended provisional security categorization for strategic planning information is as follows:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

C.3.1.1 Facilities, Fleet, and Equipment Management

Facilities, Fleet, and Equipment management involves the maintenance, administration, certification, and operation of office buildings, fleets, machinery, and other capital assets considered as possessions of the Federal government. Impacts to some information and information systems associated with facilities, fleet, and equipment management may affect the security of some key national assets (e.g., nuclear power plants, dams, and other government facilities). The following recommended provisional categorization of the facilities, fleet, and equipment management information type is particularly subject to change where critical infrastructure elements or key national assets are involved:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

D.7.2 Energy Conservation and Preparedness

Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency. The recommended security categorization for the energy conservation and preparedness information type is as follows:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

D.8.2 Environmental Remediation

Environmental remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities. The following security categorization is recommended for the environmental remediation information type:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

D.8.3 Pollution Prevention and Control

Pollution prevention and control includes activities associated with the establishment of environmental standards to control the levels of harmful substances emitted into the soil, water and atmosphere. The following security categorization is recommended for the pollution prevention and control information type:
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Categorization

C.2.3.1 Budget Formulation

The selected categorization for budget formulation is summarized in Table 1 below.

Table 1 - C.2.3.1 Budget Formulation Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	-	-	-
Justification	-	-	-

C.2.3.2 Capital Planning

The selected categorization for capital planning is summarized in Table 2 below.

Table 2 - C.2.3.2 Capital Planning Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	-	-	-
Justification	-	-	-

C.2.3.4 Strategic Planning

The selected categorization for strategic planning is summarized in Table 3 below.

Table 3 - C.2.3.4 Strategic Planning Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	-	-	-
Justification	-	-	-

C.3.1.1 Facilities, Fleet, and Equipment Management

The selected categorization for strategic planning is summarized in Table 4 below.

Table 4 - C.3.1.1 Facilities, Fleet, and Equipment Management Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	M	-	-
Justification	Building utilization needs to be protected from unauthorized access	-	-

D.7.2 Energy Conservation and Preparedness

The selected categorization for energy conservation and preparedness is summarized in Table 5 below.

Table 5 - D.7.2 Energy Conservation and Preparedness Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	M	-	-
Justification	Installation plans need to be protected from other installations and unauthorized access	-	-

D.8.2 Environmental Remediation

The selected categorization for environmental remediation is summarized in Table 6 below.

Table 6 - D.8.2 Environmental Remediation Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	M	L	L
Adjustment	-	-	-
Justification	-	-	-

D.8.3 Pollution Prevention and Control

The selected categorization for pollution prevention and control is summarized in Table 7 below.

Table 7 - D.8.3 Pollution Prevention and Control Categorization

Step	Confidentiality Impact	Integrity Impact	Availability Impact
Provisional	L	L	L
Adjustment	-	-	-
Justification	-	-	-

System

The selected categorization for the system is summarized in Table 8 below.

Table 8 – System Categorization

Confidentiality Impact	Integrity Impact	Availability Impact
Moderate	Low	Low
Overall Information System Impact: Moderate		

References

"CNSSI No. 1253", 27-March-2014. [Online]. Available: https://www.cnss.gov. [Accessed: 08-June-2016]
"Special Publication 800-60 Volume I Revision 1", "Guide for Mapping Types of Information and Information Systems to Security Categories", August-2008. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed: 08-June-2016]
"Special Publication 800-60 Volume II Revision 1", "Appendices", August-2008. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html [Accessed: 08-June-2016]