ERDC TR-18-15

US Army Corps of Engineers®
Engineer Research and Development Center

ERDC
INNOVATIVE SOLUTIONS for a safer, better world

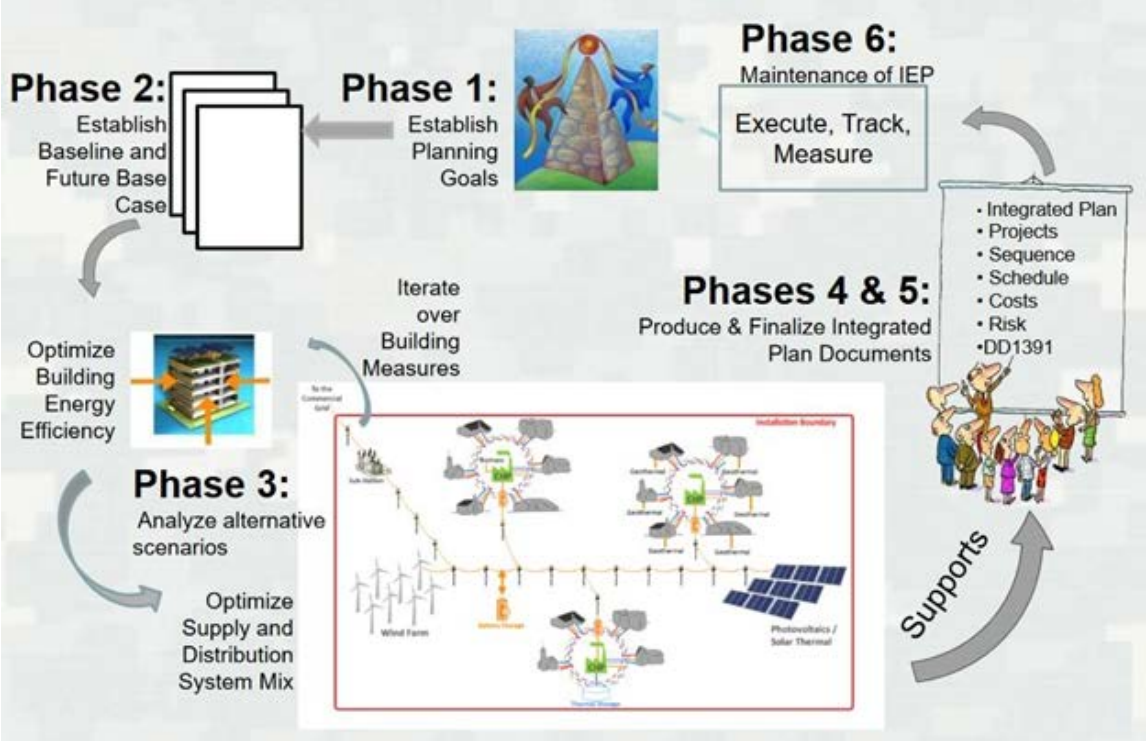
Environmental Security Technology Certification Program (ESTCP)

Technical Transfer of the System Master Planner-Net Zero Planner (SMPL-NZP) Tool™ from Research to Production

Risk Management Framework Guidelines

Richard J. Liesen, Jessica A. Johnson, Matthew M. Swanson, James T. Stinson, and Michael P. Case

September 2018



Construction Engineering Research Laboratory

The U.S. Army Engineer Research and Development Center (ERDC) solves the nation's toughest engineering and environmental challenges. ERDC develops innovative solutions in civil and military engineering, geospatial sciences, water resources, and environmental sciences for the Army, the Department of Defense, civilian agencies, and our nation's public good. Find out more at www.erdc.usace.army.mil.

To search for other technical reports published by ERDC, visit the ERDC online library at http://acwc.sdp.sirsi.net/client/default.

Environmental Security Technology
Certification Program (ESTCP)

ERDC TR-18-15
September 2018

Technical Transfer of the System Master Planner-Net Zero Planner (SMPL-NZP) Tool™ from Research to Production

Risk Management Framework Guidelines

Richard J. Liesen, Matthew M. Swanson, and Michael P. Case

U.S. Army Engineer Research and Development Center (ERDC)
Construction Engineering Research Laboratory (CERL)
2902 Newmark Dr.
Champaign, IL 61824

Jessica A. Johnson and James T. Stinson

U.S. Army Engineer Research and Development Center (ERDC)
Information Technology Laboratory (ITL)
Waterways Experiment Station, 3909 Halls Ferry Road
Vicksburg, MS 39180-6199

Final Report

Prepared for Environmental Security Technology Certification Program/ESTCP Project EW-201578 via MIPR W74RDV51978891

Abstract

The System Master Planner-Net Zero Planner (SMPL-NZP) Tool is an installation energy master planning tool demonstrated via the Environmental Security Technology Certification Program (ESTCP). The goals of this project were to: (1) use the SMPL-NZP Tool as a case study for the new Risk Management Framework (RMF) security process and document for future projects, and (2) develop a standard training course for the tool and demonstrate how modern training can be accomplished and delivered. This project: (1) provided training and tutorial materials for SMPL-NZP Tool users, and (2) pursued RMF Application certification to allow hosting of the SMPL-NZP Tool on DoD servers and Add additional encryption to web services to comply with RMF requirements. A small in-house group was trained on the RMF process, the SMPL-NZP Tool was assessed as an RMF case study, and a user guide was completed. Online training was developed and 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.

Executive Summary

The System Master Planner-Net Zero Planner (SMPL-NZP) Tool is an installation energy master planning tool that was developed through 6.2 research funding and demonstrated in ESTCP project No. 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 Certificate of Networthiness (CoN) era, and then subsequently transitioned to the Risk Management Framework (RMF) process. At the time, the RMF process was very new, and many researchers who were developing Government software tools were unfamiliar with the process, and its cost and requirements. Consequently, the experience gained from guiding the SMPL-NZP tool through this process was used to compile a user's guide for the RMF process.

Before the start of this project, the shortcomings of the SMPL-NZP Tool were identified as:

- Training (events and on-going) took significant time from the development team and customer support.
- The Tool needed some "cleaning" and security work to meet standard for hosting on DoD production servers.

This work resolved these issues and facilitated technology transfer by:

- providing training and tutorial materials for SMPL-NZP Tool users
- achieving RMF Application certification to allow hosting of SMPL-NZP Tool on DoD servers
- adding additional encryption to web services to comply with RMF requirements.

The two primary objectives of this technical transfer project were to:

- use SMPL-NZP Tool as a case study for the new RMF security process, and to document its development for future projects
- develop a standard training course for the tool and demonstrate how modern training can be accomplished and delivered.

This work met its objectives by:

- training a small in-house group on the RMF process
- assessing the SMPL-NZP Tool as an RMF case study
- completing a final report to be used as a user guide
- developing online training and hosting that training on YouTube
- enabling SMPL-NZP Tool to achieve 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 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) (DoD 2007) and CoN systems that were previously in place. The current RMF process and the categorization of assessments are structured differently from the previous systems. For example, in the RMF process, the SMPL-NZP Tool could achieve "Assess Only"; in the old system, it could have achieved a Certificate of Networthiness (CoN).

The Tool proceeded down the Assess and Authorize Path. Advantages of undergoing this rigorous security assessment and of meeting RMF requirements are that the process assures a secured dataset and produces a documented log of the system's approved architecture and its uses. 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 for use in the U.S. Army Engineer Research and Development Center (ERDC) Center for the Advancement of Sustainability Innovations (CASI), which provides ERDC ownership for the Tool.

Contents

Tables

Preface

Funding for this demonstration was provided by the Environmental Security Technology Certification Program (ESTCP) under Fiscal Year 2014 (FY14) Energy and Water Project EW-201578, "Technical Transfer of Net Zero Planner Tool from Research to Production Platform" via Military Interdepartmental Purchase Request (MIPR) No. W74RDV51978891. The ESTCP technical monitor was Scott Clark.

The work was managed by the Energy Branch (CFE) of the Facilities Division (CF) of ERDC-CERL. At the time of publication, Giselle Rodriguez was Chief, CEERD-CFE; L. Michelle Hansen was Chief, CEERD-CF; and Kurt Kinnevan, CEERD-CZT was the Technical Director. The Deputy Director of ERDC-CERL was Dr. Kirankumar V. Topudurti and the Director was Dr. Lance D. Hansen. Speler Montgomery was Chief, CEERD-IES; and Dr. Jerrell R. Ballard was chief, CEERD-IE. The Deputy Director of ERDC-ITL was Patti Duett and the Director was Dr. David A. Horner.

COL Ivan P. Beckman was Commander of ERDC, and Dr. David W. Pittman was the Director.

1 Introduction

1.1 Background

The U.S. Army Corps of Engineers (USACE) System Master Planner-Net Zero Planner (SMPL-NZP) Tool is an installation energy master planning tool that being developed for users throughout the U.S. Department of Defense (DoD). To successfully transfer such a program from the research platform to a production environment, the program must be stable, scalable (i.e., capable to serve a large number of users), and accredited (i.e., it must meet the DoD criterion for Risk Management Framework [RMF] accreditation).

1.1.1 Stability

In a general sense, no software program is ever "completed." Programs inevitably go through updates and version upgrades as customer needs and computing environments change. However, in development stages, it can be difficult to obtain a stable, release version of software due to "scope creep," which commonly occurs when the user and development teams expand the originally defined scope of work to include additional features, which in turn impacts the developers efforts to formulate final data structures and algorithms.

Nevertheless, it is necessary to have a full featured, stable version of the developed software to start the transfer process from research to production. To attain that stable platform, developers must take certain measures, e.g., put a freeze on the addition of interface features, and complete database and system modifications necessary to meet security and functionality requirements. Developers made appropriate changes to the SMPL-NZP Tool™ and settled on a release version before the start of RMF documentation. This is further discussed in the Lessons Learned section of this report.

1.1.2 Scalability

A software system operating in the research environment may be limited in the number of users it can serve. To transition a system from one that can serve only small numbers of users to one with the capability to reach across all of DoD requires that the system be transferred to a scalable platform (an enterprise production environment), and that the system be prepared to scale with the growing customer demand.

To make a successful transition to an enterprise production environment, a software system must first address any gaps that may impact scalability. In the case of the SMPL-NZP Tool™, one targeted gap impacting scalability was user training. A lack of user training can impact a system by significantly limiting its availability to users. The number of users, or growth in the user base will be directly limited by the availability of trainers and training materials, until those resources are made readily available across the entire potential user-base.

1.1.3 Accreditation

When the stable software system has addressed gaps impacting its scalability, and has been prepared on a functional level for a transition to an enterprise production environment, it must still meet DoD requirements for accreditation. To meet DoD requirements, a system must meet legislative requirements. One requirement states that the system must attain an Authority To Operate (ATO) to be considered for use in an enterprise production environment. Previously, the path to software accreditation for use in an enterprise production environment was the DoD Information Assurance Certification and Accreditation Process (DIACAP). On 12 March 2014, DoD released guidance to supersede DIACAP with the Risk Management Framework (RMF) for DoD Information Technology (IT) (DoD 2014).

According to Office of Management and Budget (OMB) policies (OMB 2010), under National Institute of Standards and Technology (NIST) enforcement, all information systems must undergo annual review that ensures that the minimum security standards of the Federal Information Security Management Act (FISMA), Section 3544(b)(5) 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, and RMF accreditation is the DoD criteria for any software system pursuing an ATO.

The newly released, still-evolving RMF requirements affect DoD and, specifically, U.S. Army Corps of Engineers (USACE) activities. Few publications or resources are available to provide guidance on the new RMF accreditation process. Currently, users must dedicate time and resources to identifying RMF requirements and navigating the available documentation. This work therefore provides the added benefit of documented expe-

rience and lessons learned on preparing for and navigating an RMF accreditation to an ATO, which should decrease resources required for future systems that undergo RMF accreditation.

This work was undertaken to demonstrate the shortest known path to transition a software system from a research and development environment, with limited user capacity, to the point where it receives an ATO and becomes enterprise production ready. To achieve this, there was a need to provide field-tested paths and to apply lessons learned to prepare for and undergo an RMF accreditation; and to author and publish training materials that address usability concerns and that close the gap on system scalability.

1.2 Objectives

The overall objective of this work was to transition the SMPL-NZP Tool™ from the research environment to a production environment with the capability to serve a single Corps District, with a scalable capacity that will allow the tool to serve the entire DoD. Specific objectives were to:

- make the SMPL-NZP Tool™ easier to use through the development of tutorials, training events, and a streamlined software interface
- ready the tool for transfer to a scalable platform, to enable the tool's functionality to expand to match the scale of growing customer demand
- establish system scalability by creating and publishing innovative training solutions, then the system is ready for transition.
- Prepare the system for RMF accreditation, which will approve the system for transition to a scalable platform in an enterprise production environment.

1.3 Regulatory drivers

DoD, Army Corps of Engineers Information Technology (ACE-IT), Defense Information Security Agency (DISA) requires any system hosted on stated environment to possess an ATO. The ATO may only be obtained by successful completion of an RMF accreditation. The RMF is the unified information security framework for the entire Federal government that is replacing the legacy Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) processes within Federal government departments and agencies, the Department of Defense (DoD) and the Intelligence Community (IC).

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

DoDI 8500.01 (DoD 2014a) replaces the former DoD Directive 8500.1 (DoD 2002) and defines DoD policies for protecting and defending information and information technology, now officially dubbed "Cybersecurity" in place of "Information Assurance."

DoDI 8510.01 (DoD 2014b) 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 DoDI 8500.2, "Information Assurance (IA) Implementation" (DoD 2003), are now provided by reference to the applicable NIST and CNSS publications, i.e., NIST Special Publication (SP) 800-53 (NIST 2013) and Committee on National Security Systems Instructions [CNSSI] No. 1253) (CNSSI 2014).

2 Technology Transfer Description

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

2.1 Technology transfer overview

RMF accreditation is intended to ensure that any system placed on a given network will neither pose nor expose any significant security threat to that network. The technology demonstrated here is a field trial, which includes documentation of RMF preparation and lessons learned. Preparing for an RMF accreditation assessment is a lengthy process. A documented field trial and lessons learned document will significantly improve the flow for future projects that must successfully complete 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*[*] (BAI 2018) and other RMF resources such as the RMF Knowledge Service (RMFKS 2014). This study also describes the implementation of elements that helped achieve the required scalability of a production ready system.

A gap analysis of the SMPL-NZP Tool™ identified obstacles to system scalability. Specifically, the findings showed that a lack of training materials would slow the scaling of the software system to an enterprise production environment. The analysis also indicated that the lack of a stable platform would delay documentation and scalability. These findings drove the requirement to develop easily distributable effective training materials, and to set requirements for a release version of the software system. Published research on the topic (Windermere 2016) indicate that training videos provide the most efficient and effective training material for this kind of software product.

[*] BAI is an information security consulting and training company that provides resources for RMF.

Training materials were developed, and methods were successfully devised and implemented to prepare the SMPL-NZP Tool™ for RMF accreditation for an ATO. The developed training videos successfully mitigated issues with scalability. Together, these measures prepared 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 and limitations to considering the elements of a production ready system (including data security) and RMF requirements before system development. However, an understanding of production requirements and RMF is a necessary to properly consider these factors.

The advantages of subjecting a planned system to a rigorous security assessment and ensuring that the system will meet RMF requirements are that these early steps ensure a secured dataset, and provide a documented log of the approved architecture and uses of the system. This provides a necessary baseline for monitoring and counteracting any breaches to certified system or data use.

Limitations of early planning for system transition to a production environment and for RMF accreditation are that these steps impact the Software Development Lifecycle (SDLC) and the flexibility of system architecture and modules. The rigid and complex requirements of RMF can delay SDLC timelines. 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, lengthy CCB requirements and rigid regulations that govern production hosting environments can limit hardware acquisition and reduce the flexibility of selecting hosting locations.

3 Test Case Description and Conditions

The 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 for the SMPL-NZP Tool™ to prepare for transition to an enterprise production environment.

An enterprise production environment would allow the SMPL-NZP Tool™ to expand upon and ensure that the desired user base had access to the necessary tools and resources. At the time of the RMF study, the development of the SMPL-NZP Tool™ was nearing completion, and the system was beginning to gain traction in the field. 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.

The SMPL-NZP Tool™ provided a good case for demonstrating RMF requirements and production ready system elements because there was a clear need for the software system, because there was a lack of competition for the technology, and because the developmental stage of the software was uniquely suited it for the RMF Study.

3.1 Milestones and status for the technical transfer from research to production

Table 1 lists the SMPL-NZP Tool™ milestones presented at the beginning of the study of transition from a research environment to a production environment. **Milestones** are listed as defined at the beginning of the SMPL-NZP Tool™'s Transfer from Research to Production. **Status** updates are listed according to Fiscal Year 2016 (FY16) year-end status for each milestone. **References** correspond to information and evidence that support 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 the SMPL-NZP Tool™ from research to production.

Milestones	Status	Reference
Make database changes to meet security requirements	Database changes were made to meet initial security requirements, before 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, before 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	The SMPL-NZP Tool™ completed a full system description with boundary definitions as defined in the ERDC Research and Development Environment. The SMPL-NZP Tool™ boundaries with-in the targeted Corps Net enclave are to be negotiated in the Memorandum of Understanding (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, before 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.	

Milestones	Status	Reference
Submission of documentation for RMF- Assess Only	The 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. The 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: the SMPL-NZP Tool™ 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	The 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. The 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 to the planning for authorization package preparation, 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

Milestones	Status	Reference
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 system's owner, audience, information types hosted or transferred, hosting enclave, and many more factors determine 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 that such a document is neither a reasonable nor a 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 system's 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 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 system's 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 that such a document is neither a reasonable nor a 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 system's 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 system specific security requirements.	Section 5.1.3 all & Section 5 all

Milestones	Status	Reference
SMPL-NZP Tool™ Video Tutorials		
Develop Tutorial video Scripts and SMPL-NZP Tool™ 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 to 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

3.2 SMPL-NZP Tool™ RMF Process™

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

- **Make database changes to meet security requirements:** Make any database modifications necessary to mitigate security infractions. Make changes before 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 before 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 before 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:** Completed
- **Interface feature freeze for the RMF process:** Make any interface modifications necessary accommodate functionality, as requested by the customers for ease of use. Make changes before 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 before the beginning of RMF documentation
- **Document database, services, and other changes from development:** Complete testing of modifications and additions made before the beginning of RMF documentation
- **Submission of documentation for RMF – Assess Only:** Complete a full RMF accreditation assessment package, undergo RMF preassessment and develop any supporting documentation and Plan of Action and Milestones (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.

3.3 Software security report

Software security reports include:

- Software Security Report Draft
- Final Software Security Process Report.

3.4 SMPL-NZP Tool™ video tutorials

- **Develop Tutorial video Scripts and the 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 Training and Scalability Requirements for Successful Technology Transfer

A significant amount of training was required to convey the extensive and complex processes involved in using the SMPL-NZP Tool™ to provide data for Sustainability Component Plans (SCPs). Since in-person training events are both time consuming and expensive, an automated form of training was designed to reduce both cost and time requirements, and to increase scalability across multiple districts and installations. Note that, while developing these training videos was part of this project, a fully encompassing training solution could not be developed without a prepared release version of the software system.

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. In FY15, district personnel requested a reoccurring, bi-weekly virtual training session. A schedule was developed to walk users through the SMPL-NZP Tool™ in approximately 20 sessions. This schedule was also used to organize the development of training videos. The training was split into two sections: course videos and training sessions, and training scripts were developed to address specific guideline topics.

The video scripts were modeled on live training events. The first draft video was produced using the trainees as the test group. After the first draft video was reviewed and accepted, 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. Trainees provided feedback on the effectiveness of training materials and made recommendations for improved material. The final videos were then modified and released.

Course videos include the full version of recorded training sessions designed to educate installation-level planners. Each video has an average run-time of 45 minutes. The videos guide the user through all scenarios they will encounter when following the steps and processes of the tool. Course videos also include a “question and answer” section that offers additional helpful information and addresses potential knowledge gaps.

The training videos are recorded by a training professional and are meant to guide the user through a standard tool process. The videos are relatively short by design, to focus on and demonstrates some specific, detailed aspects and scenarios of the tool. The concise and topic specific content is meant to benefit users who want to know how to access and use a specific part of the tool.

The final documentation for the full tutorial includes a video playlist for each set of videos. Each playlist guides the viewer through the material in a specific order. District and installation personnel all over the world can freely access the full set of training materials to viewed and re-viewed them at their own pace. At this writing, the videos currently on the YouTube channel, now the standard SMPL-NZP Tool™ new-user training, have already received several hundred views.

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.

Initial plans were to insert all training videos into the SMPL-NZP Tool™ itself. However, a link to the hosting YouTube channel was added to the opening SMPL-NZP Tool™ page so users can access the training before login. This placement offers several benefits. Placing the external links before the login helps maintain system security. Making the SMPL-NZP Tool™ tutorial videos accessible as a standalone, scalable training platform allows the tool to properly transition into a production level with scaled demand without requiring any additional time or monetary commitment from the team. Finally, using a public medium such as YouTube makes the training accessible to all DoD, and invites interest from the public domain in DoD Net Zero initiatives.

4.3 Scalability

Scalability first requires a stable software platform on which to train users. YouTube provides that platform so the training videos can supply the SMPL-NZP Tool™ with the additional scalability it requires to advance to the enterprise production level. The popular, easily accessible YouTube

platform can draw public attention to Net Zero initiatives, bolster public support for the platform, and increase accessibility to government contractors and employees.

Additionally, the easy 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 allows trainees a cost0free way to refresh their training on demand when they begin to encounter real world scenarios while operating the tool.

These benefits contribute greatly to the overall scalability of the SMPL-NZP Tool™ platform. YouTube provides a simple solution that resolves the training scalability problems previously encountered with training on the tool. This training vehicle enables the SMPL-NZP Tool™ to properly scale itself 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. Each training event typically involved the efforts of three people over 4-5 days, and required the group to travel, at a cost of about $20,000 (as 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 Proponent Sponsored Engineer Corps Training (PROSPECT) Training Course has been developed by the USACE Training Center (USACE 2018, p 1/66), and is now an annual event. Students can use these training videos at their own pace to review training, or to explore sections of the Tool in greater depth.

4.5 Accessing the training

The training is available to any individual with access to the internet and the YouTube site (https://www.youtube.com/). The user can search “SMPL-NZP Tool” in the search criteria on the YouTube site to access the full playlist of videos created to support the SMPL-NZP Tool™, or access the SMPL-NZP Tool™ YouTube channel directly through Universal Resource Locator (URL): https://www.youtube.com/channel/UC2sdFPLVc5TENXyuRL4SzNw.

4.6 Technology transfer

Table 2 lists the training and course videos and their runtimes.

Table 2. Tutorial videos for an energy efficiency technology transitioning to a production environment.

No.	Name	Runtime
1	SMPL-NZP Tool Standard Operating Procedure Document	7:08
2	GIS [Geographic Information System] 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
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

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

The videos in the playlist can best be split into two categories: those that seek to demonstrate a process, and those that seek to better explain a process. For example, the “Manage Users” video is around 1 minute long. This

video simply demonstrates 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, videos such as the “MCDA Multi Criteria Decision Analysis Creation Part 1” serve not only as guides on how to use the tool, but also provide 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 Risk Management Framework Guidelines: from SMPL-NZP TOOL Technology Transfer RMF Process Results

These RMF guidelines are based on the findings of the RMF investigation of the SMPL-NZP Tool™ field trial, which is seeking an ATO. These guidelines are presented in the same logical order in which the suggested steps should be performed, according to the results of the investigation.

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, which should minimally cover the basics of RMF. The high level knowledge will benefit the contributors develop an RMF team and prepare for the RMF accreditation assessment. An understanding of the premises and expectations of RMF before beginning the accreditation process will aid in software engineering decisions. Those who receive early high level RMF training will find that this knowledge is essential in helping them navigate the RMF prerequisites of: identifying the system and environment, identifying the targeted hosting location, identifying the RMF stakeholders, and developing an RMF awareness plan.

It is further recommended that any software system preparing for RMF specify a primary Point of Contact (POC) for RMF intelligence. This will be the RMF lead for the system's 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 2018).

See Appendix B, "RMF Prerequisites," Section titled "Understand the RMF Steps" (p 46) for a brief overview of RMF requirements.

5.1.2 Know the system and environment

It is recommended the internal RMF POC, or a delegate, compile a full system description as recommended and outlined in Appendix B, "RMF Prerequisites," Section titled "Know the System and Environment (Information Gathering)" (p 45) and Section titled "Understand the Financial Plan" (p 45). This system description will be the foundation of knowledge in preparation of formal RMF documents and in the formulation of mitigation strategies to close gaps between software engineering and RMF requirements.

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

The *BAI Information Security Consulting & Training RMF for DoD IT Fundamentals* training course (BAI 2018) provides guidance on defining the system boundary as discussed in Appendix B, "RMF Prerequisites," Section titled "Know the System and Environment (Information Gathering)" (p 45).

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 accreditation requires only a risk assessment to define the security posture of the system. In the Assess-Only accreditation 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 (2010) and NIST (2008a,b) 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 2018). 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" (RMFKS 2015).

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 have a physical environment, provide networking capability, offer basic services such as email, and are usually Common Control Providers. Example Enclaves include local area networks and their hosted applications, backbone networks, and data processing centers.

An 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 2018).

MAs administer software updates, maintain the database, and administer web interface updates. MAs develop and maintain the application, and are likely on servers in an enclave, where global work stations may access the application but may not be part of the boundary. Their data sensitivity often increases cyber security risk. MAs typically rely on a GSS for some of their security protection.

Any system classified as an IS, whether it is a 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 in the Knowledge Service document library" (RMFKS 2015).

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 Confidentiality, Integrity, and Availability (CIA) categorization. (See below.) PIT Systems will have unique requirements and security controls. All PIT Systems, like ISs, 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 to the PIT System categories likely fall into the PIT, IT Service, or IT Product category. Systems in these three categories require only the Assess-Only RMF assessment, and the depth of RMF assessment will be determined at the system level.

The following terms are defined in DoDI 8500.01 (DoD 2007), and are listed in the Knowledge Service document library (RMFKS 2015):

- "PIT" includes "both hardware and software that is physically part of, dedicated to or essential in real time to the mission performance of special purpose systems." An example might be a radiology system or X-ray machine.
- An "IT Service" is "a capability provided to one or more DoD entities by an internal or external provided based on the use of information technology and that supports a DoD mission or business process. An IT Service consists of a combination of people processes and technology."
- An "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 accreditation process, and any misclassified systems will not complete RMF accreditation assessment for an ATO.

The SMPL-NZP Tool™ originally planned to complete an RMF Assess-Only authorization package. However, at the time of SMPL-NZP Tool™'s RMF preparation, the RMF Assess-Only requirements had not yet been released. After thorough investigation of the above information, it was found

that, due to its size and nature, the SMPL-NZP Tool™ fit most appropriately into the MA classification, which requires a full RMF Assess and Authorize accreditation assessment.

5.1.4 Identify targeted hosting location

RMF guidance suggests that a software system may undergo an RMF Type Authorization, in which a pre-determined location need not be presented. However, the SMPL-NZP Tool™ investigation determined that 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 Officials (AOs) of each hosting enclave must approve installation of the system into their boundary. SMPL-NZP did not choose to attempt a Type Authorization, but instead moved forward with a Security Authorization Package (SAP) that targeted the Corps Net as the hosting enclave.

In determining a targeted hosting enclave, many factors should be reviewed. The internal RMF POC should document parameters outlined in Appendix C, “Production Environment Hosting Guidance.” Appendix D, “Hosting Comparison_SMPL-NZP Tool™,” includes an example hosting comparison form used to compare SMPL-NZP Tool™ candidate environments.

5.1.5 Identify the RMF stakeholders, develop an awareness plan

RMF accreditation requires an a great deal of approved documentation. It is critical to have an outline of the organization and approving officials. Appendix E, “Identifying RMF Team,” includes an outline of the required RMF representatives and approving officials and their roles and responsibilities as relating to the RMF steps. The approved stakeholders and RMF team will be identified in the RMF Core SAP. The Template SAP is listed in the RMF Knowledge Service (RMFKS 2015).

Training and awareness needs of individual stakeholders and RMF team members should be identified in the early stages of RMF preparation. Appendix F, “Identify Stakeholders and Develop Awareness Training Plan_

SMPL-NZP Tool™," offers guidance on recommended training for participants of different levels of the RMF process.

5.1.6 Understanding risk management

Once the beginning stages of RMF preparation have been completed and an awareness plan has been established, participants should be given the in-depth training identified in the awareness plan before moving forward with RMF documentation.

In the SMPL-NZP Tool™ investigation, PMs 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 2018).

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.

The SMPL-NZP Tool™ was registered in Army Portfolio Management Solution (APMS) for a project number that is needed for eMASS (a web system used for organizational management and tracking).

Each registration system has specific registration requirements. APMS requires system information focusing on scope, components, boundary and financials. 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.

Refer to the organization's Chief Information Officer (CIO) Office for more information on the software systems' required DoD component cyber security program and eMASS instance.

5.2 Initiate and plan

5.2.1 Categorize system (RMF Step 1)

Categorize the system in accordance with the CNSSI 1253 (CNSSI 2014). The system categorization is a formal definition of the information types

processed, stored, and transmitted by the system, which qualify the encompassed business lines. System categorization should include the identification of the final and official system mission statement, as well as, the system's information types. Guidance on development of the mission statement may be found in Reference: NIST SP 800-60, Vol 1 Rev. 1 at the Knowledge Service Document Library (RMFKS 2015). 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 SP 800-60, Vol 2 (NIST 2008b) provide full information type and categorization definitions. Once Information types have been selected and NIST SP 800-60, Vol 2 Special Factors have been reviewed, the provisional impact levels for each CIA Security Objective 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. The AO is defined in Appendix E, "Identifying RMF Team," and varies depending on the final hosting location. Appendix G, "Security Plan: Categorization" includes an example of the SMPL-NZP Tool™ submission.

Finally, identify possible overlays as described in CNSSI 1253 (CNSSI 2014). CNSSI 1253, Appendix F, located in the Knowledge Service Document Library (RMFKS 2015) includes the full list of overlays. Overlays are determined by the types of system data. The eMASS system 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, are:

- 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, includes:

- 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 (RMFKS 2015). Select the identified/ approved CIA categorization. This selection will populate the necessary baseline controls for each given CIA Security Objective. CNSSI 1253, Appendix D, Table D1, in the Knowledge Service Document Library (RMFKS 2015) includes the full baseline security control set.

The system should be registered in eMASS at this stage of RMF accreditation assessment preparation. Based on experience with the SMPL-NZP Tool, it is recommended to work with the spreadsheet and eMASS simultaneously. (See Chapter 7, Implementation Issues – Lessons Learned for the reasons underlying this recommendation.) The eMASS system should be used for control identification, while the spreadsheet is recommended for documenting implementation status.

To manually select the baseline control set, follow CNSSI 1253, Section 3.2.1 and use CNSSI 1253, Appendix D, Table D1, "NSS Security control Baselines"* in the Knowledge Service Document Library (RMFKS 2015).

Apply any overlays identified in the categorization step of RMF from CNSSI 1253: CNSSI Appendix F "Overlays" (RMFKS 2015), and 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" hosted in the Knowledge Service Document Library (RMFKS 2015) for further guidance. Follow this by selecting compensating controls using aforementioned references in addition to NIST SP 800-53, Section 3.2, "Tailoring Baseline Security Controls: Selecting Compensating Controls" (RMFKS 2015). Selecting compensating controls may not be required, use reference materials to determine whether they are needed.

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

* National Security System (NSS)

the following sources, which are hosted on the Knowledge Service Document Library (RMFKS 2015):

- 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."

Assign organization defined parameters by using CNSSI 1253, Appendix E, Table E-1 "Security Control Parameter values for NSS," hosed in the Knowledge Service Document Library (RMFKS 2015). 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," hosted on the Knowledge Service Document Library (RMFKS 2015).

Document all decisions and rational and justify all deviations in the Security Plan. See reference CNSSI 1253, Table D-2, "Additional Security Control Information – Justification" (RMFKS 2015) for NSS Baselines. Once documentation is complete, develop the continuous monitoring strategy.

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

The goal of the CMP is to provide information and documentation supporting informed risk management decisions. The CIA Risk Categorization 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 by demonstrating the effectiveness of security controls, providing a view of

assets, quantifying security metrics, enabling prioritization for mitigation, and clearly identifying deviations from expected results. Finally, Review the Security Plan for any other necessary updates.

Key Documents used in RMF Select Security Controls: Step 2, are:

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

Key Output in RMF Select Security Controls: Step 2, includes:

- Control level CMP, initialized
- Common Control Identification.

5.3 Implement and validate

5.3.1 Implement security controls (RMF Step 3)

Knowledge Service (RMFKS 2015) provides guidance that ensures that controls are implemented consistent with DoD and component architectures and standards, and establishes mandatory configuration settings.

The *BAI Information Security Consulting & Training RMF for DoD IT* (BAI 2018) recommends the beginning approach of a Tabletop review:

- 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 that details the controls addressed and the reasoning.
- Planned implementation items require implementation statements. Implementation statements should prove each item meets requirements, list the responsible party, and give evidence of the 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 that the item is not required.
- Verify Common and N/A 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, are:

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

Key output in RMF Implement Security Controls: Step 3, includes:

- 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 (SAISO). 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 before 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 the interface, and to review documentation. The pre-assessment reports communicate a provisional risk standing and include mitigation strategies.

In accordance with 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.

The SMPL-NZP Tool™ has completed a first round pre-assessment of database and servers, and a security 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 system's 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, are:

- N/A.

Key output in RMF Assess Security Controls: Step 4, include:

- 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 that controls are planned or in-place. All weaknesses identified in the SAR should be traced to one or more planned controls.

The steps in the Authorize System phase are:

- 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, are:

- N/A.

Key output in RMF Authorize System: Step 5, include:

- Prepared POA&M
- Complete SAP
- ATO Memo.

5.5 Maintain and review, decommission

5.5.1 Monitor security controls (RMF Step 6)

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

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

6 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 (summarized in Table 3) demonstrates costing implications specific to the SMPL-NZP Tool™ that were required for implementing RMF, and to impose scalability to match enterprise production quality. These costs are estimated from charges the program received when these steps were accomplished, or from cost estimates derived from surveying other programs in the process. The costs listed in Table 3 show 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.

6.2 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	

The cost elements listed in Table 3 are defined as:

- **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 to plan for adjustments to development and documentation.
- **RMF: Corrective Development**. Unburdened work-hours for corrective development are required to correct any developmental gaps found through the pre-assessment scans that exist outside of RMF requirements.
- **RMF: Architecture Documents**. Complete architecture documents including the Security Plan, Database, System Boundaries, Network, CCB documents, etc. are necessary to meet the RMF requirements.
- **RMF: Formal RMF Assessment**. An External RMF Team spends a week reviewing the 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 work-hours for corrective RMF documentation are required to correct any lacking documentation needed to attain an ATO though RMF.
- **RMF: RMF Completion**. This includes completion of remaining RMF documentation and transition of 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 laboratories. 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 the 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

6.3 Cost drivers

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

- Prior accreditation standing, i.e., if a system has an existing ATO through DIACAP, it will directly influence the needed documentation and software development, 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, and thus the 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 before 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 to 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, which will in turn impact the required funding for the final RMF accreditation assessment.
- Gaps in scalability may impact the development and system modifications necessary to meet production quality. A gap analysis of the SMPL-NZP Tool™ showed a primary gap in production quality training solutions; however, the gap analysis will determine a system's specific scalability needs.
- The nature of the system may drive a need for added personnel and the extent of additional training for those personnel. Reviewing the CIA categorization will determine the security risk categorization of the system that drives the training required for personnel, and the extensiveness of the RMF accreditation assessment. Furthermore, the nature of the software specifics will dictate the learning curve and software train-

ing required to add developmental personnel capable of making modifications to the system. This risk may be minimized by ensuring that individuals are cross trained on specific components of the software.

- The criticality of the need for the software may impact the scaling rate of the system. There may be a need to grow the system at rapid rate if the driving requirement is a critical mission. The rapid expansion rate will directly impact the timeline to complete an RMF accreditation, and also the time and resources needed to complete the transition to an enterprise production environment. The SMPL-NZP Tool™ minimized the risk of expansion rate by producing automated training materials, thereby minimizing the burden on the SMPL-NZP Tool™ development team.

6.4 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 includes the cost to maintain the CCB as well as to undergo annual review.

7 Implementation Issues – Lessons Learned

This chapter documents, discusses "lessons learned," and makes recommendations regarding a number of factors identified in the course of this work that were found to potentially hinder the RMF process. Note that these issues (listed in the following sections) are broadly applicable to RMF process; they are not identified here as specifically hindering the SMPL-NZP Tool™ RMF accreditation assessment. Some of the lessons learned are items that were included in the SMPL-NZP Tool™ in the early or pre-development stages, and were later found to have been elements that would have been helpful if they had been implemented before beginning development. These involve documented strategies that may benefit or mitigate issues during transitional period from development to a production environment.

7.1 Before beginning system development

Before beginning system development, it is recommended to:

- *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 before beginning system development, then the ACP may require redesign and the authentication method may need to be rewritten.
- *Establish the requirements for and draft the Identification and Authentication Policy (IAP).*
- *Design an authentication method that fits a sustainable standard.* Failure to design a sustainable authentication method will require a redesign and rewrite of the authentication method during the RMF process and before gaining RMF accreditation; it will also require a rewrite of the IAP.
- *Design and establish a method for auditing access control, as designed in the ACP.*
- *Design and establish a Configuration Control Policy (CCP) and CCB Charter*. The established guidelines in the CCP will provide software development standards. The RMF accreditation assessment will require implementation and evidence of such for RMF accreditation.
- *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 proven valid through testing before acceptance in RMF.

7.2 During system development

During system development, it is recommended to:

- *Maintain both development documentation and task tracking*. It is recommended that a formal task tracking system instance be established for the development system before beginning system development.
- *Continually update the STP*. Failure to continually update the STP will result in gaps supporting the CCP. Complying with the need to update the STP aids the RMF process by allowing the process to begin with a fully updated system definition, defined in the STP. The establishment of a full system definition provides content for needed system training.

7.3 Before beginning RMF documentation

Before beginning RMF documentation, it is recommended to:

- *Design and release system training materials*. The lack of proper training materials hinders a system's scalability thus impacting its ability to successfully transition to a production environment.
- *Identify the desired final hosting location*. Failure to initiate the RMF accreditation assessment with a predetermined hosting location will result in significant delays and setbacks in the RMF accreditation process. Although it was previously thought that RMF accreditation could easily transition from one production host to another (and documentation states that this is so), it appears logistically implausible at the present time. Because the hosting location significantly impacts RMF, a great deal of time and resources can be conserved by selecting a final hosting location before initiating RMF documentation.
- *Ensure that all key system staff receive high level RMF training*. RMF Fundamentals and RMF in-depth training are offered back-to-back, suggesting to users that they should be taken together. However, BAI offers free online training to those enrolling in their face-to-face training. It is therefore recommended that key staff enroll in the online training before beginning RMF documentation. This will allow them to acquire a basic understanding of the RMF process and expectations. After the initial "getting started phases" of the RMF, it is recommended that all required persons then attend RMF in-depth training. Breaking the training into two sections allows trainees to gain a good understanding of RMF before starting the documentation, and then to acquire a good understanding of the targeted system and its needs before

starting in-depth training. The training recipients will gain much more from the training if they begin with prior high level knowledge, which will form a good knowledge baseline of the systems that RMF needs.

7.4 During RMF documentation

During RMF documentation, it is recommended to have an understanding of the fluid RMF requirements. The eMASS system hosts 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, which has a published control list that is not the latest version of the control list. If the Army eMASS choses to update the published control list before the completion of eMASS input, SMPL-NZP would be required to again start their inputs from the very beginning. It is therefore recommended to visit RMF Knowledge Service and download the latest control list, and to input the controls manually after completing them off-line. This will mitigate the potential need to input the controls multiple times.

7.5 Omissions to avoid

7.5.1 Failure to implement an auditing mechanism

It is critical to implement an auditing mechanism. Failure to do so:

- would leave gaps in full documentation of access
- could present threats via lack of exposure to unwarranted access
- will present the need, at the time of RMF accreditation assessment, to do a full audit of system access, and possibly to revoke all access and reassign access to any necessary users.

7.5.2 No or lacking evidence to prove implemented CCP

The RMF accreditation assessment requires evidence to prove implementation of CCP, which is required to support the CCP for RMF acceptance.

References

BAI. 2018. Learn RMF and more from the best in the business. *BAI Information Security Consulting & Training*. Web site, https://rmf.org/index.php/training-programs

CNSSI (Committee on National Security Systems Instructions). 2014. *Security Categorization and Control Selection for National Security Systems*. CNSSI No. 1253, http://www.dss.mil/documents/CNSSI_No1253.pdf

DoD (U.S. Department of Defense). 2002. DoD Directive (DoDD) 8500.01E. Subject: Information Assurance (IA). (Canceled). Washington, DC: DoD, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

———. 2003. DoD Directive (DoDI) 8500.2. Subject: Information Assurance (IA) Implementation. (Canceled). Washington, DC: DoD, https://biotech.law.lsu.edu/blaw/dodd/corres/pdf/i85002_020603/i85002p.pdf

———. 2007. Department of Defense Instruction (DoDI) 8510.01. Subject: DoD Information Assurance Certification and Accreditation Process (DIACAP). (Canceled). Washington, DC: DoD, http://www.dtic.mil/dtic/tr/fulltext/u2/a551538.pdf

———. 2014a. Department of Defense Instruction (DoDI) 8500.01. Subject: Cybersecurity. Washington, DC: DoD, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

———. 2014b. Department of Defense Instruction (DoDI) 8510.01. Subject: Risk Management Framework (RMF) for DoD Information Technology (IT). Washington, DC: DoD, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

NIST (National Institute of Standards and Technology, formerly National Bureau of Standards). 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication (SP) 800-53. Gaithersburg, MD: NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

———.2008a. *Guide for Mapping Types of Information and Information Systems to Security Categories*. SP 800-60, Volume I, Revision 1, http://csrc.nist.gov/publications/PubsSPs.html

———.2008b. *Appendices*. SP 800-60 Volume II Revision 1, http://csrc.nist.gov/publications/PubsSPs.html

———.2004. *Standards for Security Categorization of Federal Information and Information Systems*. Federal Information Processing Standards Publication (FIPS PUB) 199. Gaithersburg, MD: NIST, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

OMB (Office of Management and Budget). 2010. OMB Memorandum M-10-15. Subject: Y 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Washington, DC: OMB, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-15.pdf

RMFKS (Risk Management Framework [RMF] Knowledge Service). 2015. *RMF Knowledge Service*. Web site, https://rmfks.osd.mil/rmf/Pages/default.aspx https://rmfks.osd.mil/rmf/SiteResources/References/Pages/ReferenceLibrary.aspx

USACE (U.S. Army Corps of Engineers). 2018. Master planning sustainability & resiliency. *2019 Purple Book*. Huntsville, AL: U.S. Army Corps of Engineers Training Center. p. 1/66, http://ulc.usace.army.mil/downloads/purplebook2019.pdf

Windermere, A. 2018. What is the importance of video tutorials to students? *Chron* (Houston Chronicle Online). 30 July 2018, http://work.chron.com/importance-video-tutorials-students-16633.html

Acronyms and Abbreviations

Term	Definition
ACEIT	Army Corps of Engineers Information Technology
ACP	Access Control Policy
ANSI	American National Standards Institute
AO	Authorizing Official
APMS	Army Portfolio Management Solution
ATO	Authority To Operate
C&A	Certification and Accreditation
CA	Certifying Authority
CASI	Center for the Advancement of Sustainability Innovations
CCB	Configuration Control Board
CCE	Cloud Computing Environment
CCP	Configuration Control Policy
CEO	Corporate Executive Officer
CERL	Construction Engineering Research Laboratory
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CMP	Continuous Monitoring Plan
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instructions
COE	Chief of Engineers
CoN	Certificate of Networthiness
CRT	Cyber Readiness Team
DAA	Designated Approving/Accrediting authority
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	U.S. Department of Defense
DoDI	Department of Defense Instruction
ERDC	U.S. Army Engineer Research and Development Center
ERDC-CERL	Engineer Research and Development Center, Construction Engineering Research Laboratory
ESTCP	Environmental Security Technology Certification Program
EW	Energy and Water
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GIG	Global Information Grid
GIS	Geographic Information System

Term	Definition
GSS	General Support System
HPC	High Performance Computing
HQ	Headquarters
IA	Information Assurance
IAP	Identification and Authentication Policy
IC	Intelligence Community
IIS	Internet Information Services
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
ISSM/ISSO	Information System Security Manager/Information System Security Officer
ISSO	Information System Security Officer
IT	Information Technology
ITL	Information Technology Laboratory
JTFTI	Joint Task Force Transformation Initiative
MCDA	Multi-Criteria Decision Analysis
MIPR	Military Interdepartmental Purchase Request
MOU	Memorandum of Understanding
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NSN	National Supply Number
NSS	National Security System
NZP	Net Zero Planner
OMB	Office of Management and Budget
PI	Principal Investigator
PIA	Privacy Impact Assessment
PIT	Platform Information Technology
PM	Project Manager
PM/SM	Project Manager/System Manager
POA	Plan of Action
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPP	Program Protection Plan
PROSPECT	Proponent Sponsored Engineer Corps Training
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAP	Security Authorization Package

Term	Definition
SAR	Security Assessment Report
SCA	Security Control Assessor
SCP	Sustainability Component Plan
SDLC	Software Development Lifecycle
SEP	Security Engineering Plan
SERDP	Strategic Environmental Research and Development Program
SM	Single Manager
SMPL	System Master Planner
SMPL-NZP	System Master Planner-Net Zero Planner
SP	Static Pressure
SQL	Structured Query Language
SRPO	Sustainability and Resiliency Planner and Operations
SSP	System Security Plan
STP	System Test Plan
TR	Technical Report
UR	User Representative
URL	Universal Resource Locator
USACE	U.S. Army Corps of Engineers

Appendix A: Points of Contact

Name	Organization*	Phone	Role in Project
Richard J. Liesen, Ph.D.	ERDC-CERL	217-373-4572	Principal Investigator (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
* Engineer Research and Development Center, Construction Engineering Research Laboratory (ERDC-CERL) Engineer Research and Development Center, Information Technology Laboratory (ERDC-ITL)			

Appendix B: RMF Prerequisites

The following sections detail a "highlights" list of RMF steps.

RMF Prerequisites

Begin the RMF by defining the following the functional terms listed in the following sections.

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.
- Information System Security Manager /Information System Security Officer (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 the System

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

Step 2: Select Security Controls

- Select security controls.
- Identify common control.
- 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 the 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, SAR and POA&M.
- Report security status to AO, AO reviews reported status.
- Implement system decommissioning strategy.

Appendix C: Production Environment Hosting Guidance

Some "highlights" of RMF steps include:

- 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 that 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 an example of SMPL-NZP comparison between hosting enclave as seen in Appendix D, "Hosting Comparison_SMPL-NZP Tool™."
  - Identify the selected DoD Component Cybersecurity Program.

Appendix D: Hosting Comparison SMPL-NZP Tool™

The following sections detail a "highlights" list of RMF steps.

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 for space, desired control, and available funding:

- Two Servers:
  - Structured Query Language (SQL) Server instance.
    - Database server: 8C/16G (2C/16G).
  - Internet Information Services (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 Cloud Computing Environment (CCE).

Identify impacting regulations

Any regulation that 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 may prohibit a system of particular design to be hosted

in a given location. Use this section to identify regulations and system design qualities that may impact the hosting location availability, i.e.:

- Investigate regulations requiring enterprise systems being hosted on DISA.

Identify impacting factors

Identify any outstanding factors that 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 used.
- 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: To be determined 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

The following sections detail a "highlights" list of RMF steps.

Identify Persons by RMF Role/ Responsibility [DIACAP reference]

Tier 3 -System Level

- Information System Security Manager (ISSM)/Information System Security Officer (ISSO) (IAM/ IAO).
  - ISSM.
    * Assigned at the Project level.
    * Develop and maintain organizational cybersecurity program (architecture, requirements, policies, procedures, personnel).
    * Ensure that information owners/stewards are identified.
    * Appoint and oversee Information System Security Officers (ISSOs).
    * Maintain repository for cybersecurity documentation.
    * Monitor compliance with security policy.
    * Act as cybersecurity technical advisor.
    * Respond to cybersecurity incidents and spillage.
  - ISSO.
    * Assigned by the ISSM.
    * Assist ISSM.
    * Enforce cybersecurity policies and procedures.
    * Ensure that users have appropriate clearances and authorization before access is granted.
    * Ensure that cybersecurity documentation is up-to-date and accessible to authorized individuals.
  - Responsibilities.
    * 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 (IO)/Steward.
    - 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/System Manager PM/SM]).
    - ISO.
        * Assumes responsibility of the system's security posture.
        * Plan and budget for security control implementation, assessment and sustainment.
        * Ensure that users and support personnel receive cybersecurity training.
        * Categorize each assigned system.
        * Appoint a User Representative (UR).
        * Develop, maintain and track the Security Plan.
    - PM/SM.
        * Register the system per DoD component procedures.
        * Appoint ISSM for each assigned system.
        * Ensure that each system has an assigned security engineer.
        * Develop a system description.
        * Implement RMF.
        * Ensure that RMF activities are aligned with acquisition process.
        * Enforce AO authorization decision.
        * Develop and track a POA&M for each system.
    - Responsibilities.
    - Step 1. Categorize Role: Categorize.
        * Categorize the information system based on Federal Information Processing Standards (FIPS) 199 (NIST 2004), 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 before 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 that security requirements are integrated into enterprise architecture.
- Responsibilities.
    - Step 2. Select Role: Advisor.
        * Ensure that 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 that security requirements are integrated into information system and product acquisition, design, and configuration.
    - This is a development role.
    - Responsibilities.
    - 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.
  - AO.
    * Make Authorization decisions for IS and PIT systems within their purview.
    * Ensure that RMF tasks are completed and documented.
    * Track POA&Ms.
    * Ensure that appointees to cybersecurity positions have written statements of responsibilities.
  - Responsibilities.
  - 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 that 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.
- Responsibilities.
- 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 before 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.
    - High Performance Computing (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 before 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.
    - Responsibilities.
    - 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 (SAISO)/Information Security Program Office – has SCA function, but may delegate (SAISO – 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.
    - Responsibilities.
    - 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 that risks are viewed consistently from an organization-wide perspective.
- Develops organization-wide risk management strategy.
- Head of Agency (Corporate Executive Officer [CEO]) may fulfill this role or delegate to another official or group/committee.
- Responsibilities.
- Step 1. Categorize Role: Overseer.
- Provide oversight to the categorization process to ensure that 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 that 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.
- Responsibilities.
- Step 1. Categorize Role: Leader.
  * Ensure that 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 that the information system's categorization is approved before 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 that 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 that 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 stakeholders, 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 to some degree with the RMF team:

1. 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.

   a. Organization:
      (1) Frank Holcomb, Associate Director CASI
      (2) Alan Anderson, Technical Director Military Ranges & Lands.
   b. USACE Headquarters (HQ) Proponent:
      (1) Jerry Zeckert, Chief Master Planner, Chief of Engineers (COE)
      (2) Andrea Kuhn, Master Planner, COE.
2. 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.

   a. Program Manager:
      (1) Michael P Case, PhD
      (2) Michael.P.Case@usace.army.mil.
   b. Program Manager
      (1) Richard J Liesen, PhD
      (2) Richard.J.Liesen@usace.army.mil.
3. 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.

a. Development Team:
   (1) James T Stinson, PhD
   (2) James.T.Stinson@erdc.dren.mil.
b. Development Team:
   (1) Timothy W Garton
   (2) Timothy.w.Garton@erdc.dren.mil.
c. Development Team:
   (1) Matthew Swanson, PhD
   (2) Matthew.M.Swanson@usace.army.mil.
d. Technical Writer:
   (1) Jessica A Johnson
   (2) Jessica.A.Johnson@erdc.dren.mil.
e. SMPL-NZP Tool CCB Voting Members, CCB
   (1) SEE CCB (CCB Charter in development).
f. Extended Project Team (Network Team)
   (1) Not responsible for network team RMF training.
g. ERDC, ITL RDE_CCE Representative:
   (1) Jarred R Taylor
   (2) Jarred.R.Taylor@erdc.dren.mil.
h. ERDC, ITL RDE_CCE Representative:
   (1) Sierra C Wells
   (2) Sierra.c.wells@erdc.dren.mil.
i. POCs (The POCs required to complete the RMF Process, Security Team - AO):
   (1) Other (User Representative)
   (2) SMPL-NZP Tool CCB User Representatives
   (3) SEE CCB (CCB Charter in development).

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix G: Security Plan: Categorization

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

September 21, 2018

Innovative solutions for a safer, better world

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.

Contents

Tables

G.1 Mission supported

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

G.2 Information types

G.2.1 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:

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

G.2.2 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:

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

G.2.3 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:

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

G.2.4 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 asso-

ciated 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)}

G.2.5 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:

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

G.2.6 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)}

G.2.7 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)}

G.3 Categorization

G.3.1 Budget formulation

Table G-1 summarizes the selected categorization for budget formulation.

Table G-1. Budget formulation categorization.

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

G.3.2 Capital planning

Table G-2 summarizes the selected categorization for capital planning.

Table G-2. Capital planning categorization.

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

G.3.3 Strategic planning

Table G-3 summarizes the selected categorization for strategic planning.

Table G-3. Strategic planning categorization.

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

G.3.4 Facilities, fleet, and equipment management

Table G-4 summarizes the selected categorization for strategic planning.

Table G-4. 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	—	—

G.3.5 Energy conservation and preparedness

Table G-5 summarizes the selected categorization for energy conservation and preparedness.

Table G-5. 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	—	—

G.3.6 Environmental remediation

Table G-6 summarizes the selected categorization for environmental remediation.

Table G-6. Environmental remediation categorization.

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

G.3.7 Pollution prevention and control

Table G-7 summarizes the selected categorization for pollution prevention and control.

Table G-7. Pollution prevention and control categorization.

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

G.3.8 System

Table G-8 summarizes the selected categorization for the system.

Table G-8. System categorization.

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

REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
09/28/2018	Final	

4. TITLE AND SUBTITLE

Technical Transfer of the System Master Planner-Net Zero Planner (SMPL-NZP) Tool™ from Research to Production: Risk Management Framework Guidelines

5a. CONTRACT NUMBER

MIPR W74RDV51978891

5b. GRANT NUMBER

5c. PROGRAM ELEMENT

6. AUTHOR(S)

Richard J. Liesen, Jessica A. Johnson, Matthew M. Swanson, James T. Stinson, and Michael P. Case

5d. PROJECT NUMBER

ESTCP

5e. TASK NUMBER

EW 201578

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)
Information Technology Laboratory (ITL)
PO Box 9005,
Champaign, IL 61826-9005

8. PERFORMING ORGANIZATION REPORT NUMBER

ERDC TR-18-15

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SERDP/ESTCP
4800 Mark Center Drive, Suite 17D08
Alexandria, VA 22350-3605

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The System Master Planner-Net Zero Planner (SMPL-NZP) Tool is an installation energy master planning tool demonstrated via the Environmental Security Technology Certification Program (ESTCP). The goals of this project were to: (1) use the SMPL-NZP Tool as a case study for the new Risk Management Framework (RMF) security process and document for future projects, and (2) develop a standard training course for the tool and demonstrate how modern training can be accomplished and delivered. This project: (1) provided training and tutorial materials for SMPL-NZP Tool users, and (2) pursued RMF Application certification to allow hosting of the SMPL-NZP Tool on DoD servers and Add additional encryption to web services to comply with RMF requirements. A small in-house group was trained on the RMF process, the SMPL-NZP Tool was assessed as an RMF case study, and a user guide was completed. Online training was developed and 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.

15. SUBJECT TERMS

Energy development, Technology transfer, Risk Management, Computer programming and software, Production management, Cloud computing--Energy consumption

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (include area code)
Unclassified	Unclassified	Unclassified	SAR	82	