Redspin
A Division of Clearwater

WHITEPAPER

10 Excellent Tips to Smooth Out Your CMMC Assessment

The Documents and Artifacts Edition

While organizations await the formal rollout of the Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC), they have instituted the Joint Surveillance Voluntary Assessment Program (JSVAP). This program allows organizations seeking certification (OSCs) to undergo a Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) high certification assessment conducted jointly by the DCMA DIBCAC and an authorized CMMC Third-Party Assessment Organization (C3PAO).

Over the course of the last year, as we've helped multiple organizations successfully complete a Joint Surveillance Voluntary Assessment Program (JSVAP) assessment, a few common trends have become apparent.

> **One of these trends is that the organizations who successfully navigated the JSVAP had a good understanding of what is required in their documentation and relevant artifact evidence.**

While there are many who debate the need for extensive documentation or artifacts to support their internal cybersecurity program as it relates to Controlled Unclassified Information (CUI), NIST 800-171 r2 addresses the documentation primarily in Appendix E. In this Appendix, there are tailoring items denoted as "NFO," which means items that are "Expected to be routinely satisfied by nonfederal organizations without specification" (NIST, 2020).

The inclusion of these items should be apparent, but more specifically, many organizations are struggling with how to properly address 3.12.4, which addresses the need to develop, document,...

Redspin, an early adopter working with Cyber-AB to help define the program, is the first Authorized CMMC C3PAO and is a RPO.

and update system security plans (SSPs). Also, many organizations are providing artifacts to support certain configurations but are neglecting to provide artifacts that support all of the components of the particular practice.

As a reminder, objective evidence, which SSPs and artifacts are a part of, should be both adequate and sufficient for a particular objective. Adequacy means that the evidence being provided should apply to the specific objective being assessed. For instance, you shouldn't provide an artifact that contains password configuration parameters for an objective being assessed against how you identify your users. Sufficiency means that the artifact(s) being provided meet the scope of the objective. For this criteria, you can provide a screenshot of your user list for all of your endpoint systems, but if networking gear or other services are included in the boundary, then you have to provide access lists for them as well.

In this whitepaper, we are going to address the top 10 ways you can help your assessment go smoothly from a documentation and artifact perspective. These 10 items, if addressed, can ensure the assessors and your team understand how the CUI is being protected.

1. HAVE AN SSP THAT SPEAKS TO HOW THE "SYSTEM" IS IMPLEMENTED

This one seems like a no-brainer. However, often the SSPs being provided speak to either the intended state of the system or provide very generic statements. Either of these cases will not provide the "warm and fuzzy" from the assessors that you are actually doing what you are required to do.

Speaking to the intended state of the system tells the assessors that you do not currently have the system configured per the requirements. Instead, you intend to have it configured this way at some point in the future. A JSVAP assessment, or ultimately a Cybersecurity Maturity Model Certification (CMMC) assessment, occurs at a point in time. By speaking to the intended state, you are stating up front that this is not the current configuration and will make the assessors, at minimum, dig deeper into how you have things. It could also necessitate that the assessment be stopped and have to be rescheduled.

Additionally, organizations should not provide generic statements as the SSP is supposed to be "how" you are implementing the individual practices. For example, SSPs have been submitted with a statement for AC-3.1.1 saying, "We limit system access". While identifying that the organization limits system access, it doesn't provide the context into "how" the organization is doing this, nor does it identify if this statement pertains to users, processes, or devices, which are all requirements of the practice.

2. ADDRESS EACH OF THE OBJECTIVES IN THE SSP

One of the best ways an organization can ensure they don't fall prey to the generic statement issue is to address each objective in the CMMC Assessment Guide for each SSP practice area. Each practice will have at least one objective to address. By addressing each objective, the organization identifies to the assessor(s) that they understand what the practice is

saying and have given some thought to how the organization is going to address it.

For instance, let's look at AC-3.1.1 again. In this practice, specifically referenced as AC.L1-3.1.1 in the CMMC Assessment guides, there are six different objectives:

a. Authorized users are identified
b. Processes acting on behalf of authorized users are identified
c. Devices authorized to connect to the system are identified
d. System access is limited to authorized users
e. System access is limited to processes acting on behalf of authorized users
f. System access is limited to authorized devices

For each of these objectives, the organization should have a statement/paragraph as to how the objective is being addressed. This doesn't mean you have to list out all of the authorized users specifically in the SSP, but for objective A, the statements should identify how authorized users are being identified for each component of the system. If this is accounted for by Single Sign-On (SSO) mechanisms, then state that and what components are accounted for with this. Then, identify how, for any components not covered by SSO, the organization is identifying the authorized users. As an additional note, if SSO is utilized, the assessor should want to see where this is configured. Also, the SSP can point to other policies, procedures, plans, or even other areas in the SSP. However, ensure that the references are accurate and maintained in accordance with organizational requirements.

3. ENSURE EACH OF THE COMPONENTS OF YOUR SYSTEM IS ACCOUNTED FOR

This is probably one of the most missed items in any SSP we have reviewed. This item speaks to the sufficiency of the information being provided. Often, organizations provide a statement regarding how they are addressing a practice but only speak to one element of the system.

For instance, let's say the organization has Microsoft Government Community Cloud-High (GCC-H) in place. Generally, they will provide how they are addressing the objective via GCC-H but will leave other key elements excluded. One of these elements may be how they are accounting for the backup service/system and how they ensure it is meeting practice 3.1.1. Also, maybe they allow printing of CUI but neglect to include how they are managing the authorized users of the printers.

Another example is an on-prem implementation that has Windows, Cisco, Linux, MFDs, and various services (AV, VM, etc.) in place. For 3.1.1, if it stores, processes, transmits, or provides security protection for the "System", then it is in scope for the assessment.

4. IF REFERENCING, ENSURE YOU POINT TO THE SPECIFIC ITEM

Earlier, it was mentioned that an organization can refer to other documents or other areas of the SSP when providing statements on specific practice areas. This is actually advisable as often the other documents may be updated to reflect new technologies or processes, and it may not be feasible to update the SSP each time one of these items changes.

However, too often what occurs is that the reference inside the SSP is inaccurate or points

to a general document instead of pointing out exactly where in the document the practice/objective is being met. Also, the document naming may not be intuitive, so unless specifics are identified, then the ability to ensure traceability is lost. For instance, let's use the following example or scenario from an actual assessment:

During a review of the SSP, it is identified that for item AC.L2-3.1.19, the process by which CUI is encrypted for mobile devices are included in the Access Control Policy. However, when the Access Control Policy is reviewed, it only has statements to secure mechanisms on endpoint devices. This doesn't identify **how** the organization is ensuring that CUI is encrypted on mobile devices. After further digging, it is found that the "How" is included in the mobile device setup procedures that were not provided as part of the artifact package.

While this example is generalized, several things should be evident. One, the SSP traceability is broken, so the statement in the SSP is not accurate. Two, the actual information needed isn't just a statement saying it is done but rather how the organization is addressing the objective. Three, the SSP needs to be updated. This final item also brings into question the organizational review process as now the assessor will probably look at the revision dates on the various documentation in order to identify if the Mobile CUI encryption requirement was initially in the referenced policy and has been moved, or if it was never included in that document to begin with. This information should be included in the revision history of the documents in question.

5. MAKE SURE YOUR SSP IS UP-TO-DATE

While this item should be self-explanatory, often what is being provided are SSPs that have not been updated for over a year. This means that often, the information contained within the SSP is no longer valid, or at a minimum, the validity of the information would be called into question.

As part of organizational governance practices, the SSP should be updated at the same cadence as other documentation. A good rule of thumb is that this occurs at least annually but should occur when there are any material changes to the information within the SSP. This could be when a new system or service is added or removed from the boundary that the SSP covers. Depending on the construction of the SSP, this could also necessitate updating multiple sections.

For example, let's say the organization updates its vulnerability management detection service. In this example, the boundary diagram should be updated, the data flow diagrams should be updated, and then each practice that pertains to the new service would need to be addressed as well (Access Control, Identification and Authentication, Audit and Accountability, Risk Assessment, etc.). The updates should include the removal of the old service items as well as adding in the new service information. By ensuring that the SSP is constructed and updated in this way, it, in essence will provide you with a checklist for all the artifacts that should be provided.

6. ORGANIZE YOUR ARTIFACTS

The artifacts are probably the largest amount of information an organization will provide as

part of an assessment. These artifacts can be screenshots, report snippets, configuration information, examples, or other items that the organization provides to support the objectives. With this massive amount of information, if it is not structured coherently, then the assessors may be confused as to what artifact goes with which practice.

One of the easiest ways to ensure the organization's artifacts are organized is to combine them into folders listed with each practice. In doing so, when the information is provided to the assessors (which includes DCMA DIBCAC for JSVAPs), then they can quickly and easily identify which items are being addressed. It should be noted that this could also require the same artifact to be included in different folders as screenshots, etc., since the artifact may apply to more than one practice.

Additionally, organizing the artifacts provides the organization to (more appropriately) tell their "story" of how they are protecting the confidentiality of CUI. Starting with the SSP mentioned previously, the artifacts provide a level of assurance that the items are properly configured. Also, while it will not preclude the need to show live demonstrations, it will provide the ability to focus the conversation with the assessors as each component should be addressed.

7. MAKE SURE YOU HAVE ARTIFACTS FOR EACH COMPONENT

This is probably one of the most overlooked areas when compiling documentation and artifacts. While there are multiple types of categorizations for the system components, the focus here is on those that store, process, or transmit CUI, as well as those systems and services that provide security protections for the CUI. When compiling information around these items, most organizations do a good job for the areas that concern data (CUI) storage and endpoint devices (desktops/laptops). However, the shortfall comes as there are more components to a CUI boundary than just these two areas.

For those devices or services that store, process, or transmit CUI, this includes technology, people, and places (physical structures). Organizations often neglect to identify specific processes or procedures around networking devices, mobile devices (smartphones/tablets), or non-Windows-based systems. This is why understanding the CUI data flow is so important, as every location where CUI is located must be accounted for. Organizations should ensure as they go through the objectives, they collect the needed information for each of these components.

As an example, for AC.L1-3.1.1, the organization must provide evidence showing how they identify authorized users for each of these components. As another example, when you are addressing the practice concerning Security and Privacy banners, the organization needs to make sure they are accounting for these on each component. If you are using Linux devices as part of your boundary, and they store, process, or transmit CUI, then the organization must ensure there is the appropriate Security and Privacy banner.

Components that provide security services can be one or many multiple things depending on how the organization has constructed its boundary. Each of these could be in play, and the organization must have an understanding of how the security protection assets are

accessing the organizational CUI data. If using onsite appliances, be prepared to show how it is protecting the data, how access is provisioned, and any other NIST 800-171 (CMMC L2) practice that could pertain to the asset.

Additionally, if an organization is using a cloud service, the organization must have an understanding of which security responsibilities reside with the third-party service and which reside with the organization itself. This also speaks to there being no current reciprocity between CMMC and any other attestation. The notion that assessors have been following currently is based on DFARS 7012 which requires FedRAMP Moderate or equivalent. However, the organization cannot simply state compliance as assessors will still want to ensure the organization has done its due diligence. At a minimum, as the organization is preparing for assessment, they should be prepared to answer questions regarding these cloud services to include who has access to the data on the service side.

8. IF USING THIRD-PARTY EXTERNAL SERVICE PROVIDERS (ESPS), ACCOUNT FOR THEM

As mentioned, the current notion is that third parties have to be FedRAMP Moderate or equivalent. However, this process is arduous, and not every ESP will go through formal FedRAMP certification. Regardless of if the ESP is FedRAMP Moderate certified or not, the onus is on the organization seeking certification (OSC) to ensure the ESP is addressing the proper requirements for the protection of CUI. The most important part of this process is to ensure the OSC addresses whose responsibility it is to properly configure certain items to meet NIST 8001-171 practices (OSC or ESP). This should fall under organizational Vendor Security Management (VSM) procedures, but that process may or may not account for NIST 800-171 items.

Organizations should be prepared to provide information on these ESPs and how communications are protected. Questions that organizations should be asking themselves are (as an example): What data do the back-end services have access to? Do they properly control access in their environment? Who is accessing the organizational data? While these aren't the only questions to be asking, they allude to the necessity of the organization to have an understanding of not only its internal systems but all of its external services as well.

9. DOCUMENT WHO IS RESPONSIBLE FOR WHAT ITEMS

When you go into an assessment, the assessors are going to want to speak to the individuals in your organization that are responsible for the various practices. Often, much like other items we have talked about, this is accounted for at the top level and main services or systems. However, it is when the organization does not understand its own boundary that this becomes problematic. As part of an assessment the assessors can ask questions of these individuals and they should be prepared to answer them. If the organization has Linux as part of the environment, have a Linux admin ready to answer the questions as an example.

Outside of the technology, CMMC is not an Information Technology (IT) or Information Security (IS) assessment alone. The process will also require additional individuals in organizations to understand their responsibility to protect CUI. For instance, AC.L1-3.1.22 speaks to controlling information posted or processed on publicly accessible information systems. When you bring this into the assessment, it includes the information posted on organization websites, social media, or other channels. This type of information is more than

likely not created by your IT or IS individuals but rather by the Marketing, Public Relations, or potentially Sales departments. Be prepared to have these individuals answer questions and provide the required evidence of the practice objectives. Make sure these folks are documented to be able to lead the assessment discussion. This can be accomplished via a Risk Responsibility Matrix or similar item that provides almost a checkbox list of who needs to be in the assessment for which sections.

10. HAVE CERTIFICATE NUMBERS AVAILABLE

To this point, we have talked about specific documentation that has to be constructed by the organization, artifacts in the form of screenshots or other items, and documenting who is going to be in the assessment. The final item in the list is very straightforward. This item is simply having encryption certificate numbers available for any encryption that is used to protect the confidentiality of CUI. These certificate numbers should be for the FIPS 140-2 **validated** modules used. The certificate numbers can be provided in a central list or in the specific sections that correspond to the encryption in either the SSP or policy-type documentation.

Often, this is overlooked or misunderstood in that FIPS 140-2 compliant or type encryption is used. This is not the same as the Validated requirement and could cause a halt to official CMMC assessments. Under the JSVAP, there is more wiggle room, but currently, FIPS 140-2 Validated encryption has to be in place. If the organization is unsure whether the encryption meets these requirements, simply ask the vendor. If they have been through the validation certification, they will probably be more than happy to tell you about it.

Assessors will use these certificate numbers and verify them against the list located here. (https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search)

While many of these items may seem “elementary, my dear Watson”, they are still issues in many of the assessments that are being conducted. At the end of the day, ensure that whoever is managing your CMMC program has a solid understanding of the assessment process. This can, and probably should, include sending at least one person to a CMMC Certified CMMC Professional (CCP) class to gain detailed insight into what the organization should understand.

Also, if you are using a third-party organization to help you prepare, be aware that not all organizations of this type are the same. Ensure they have a solid understanding of what the requirements of CMMC are AND how they are going to be assessed.

If you have questions about CMMC documentation + artifacts and how they impact the CMMC journey, reach out to us, we are happy to have a discussion.

www.redspin.com
info@redspin.com

10 Effective Strategies to Optimize Your Documents and Artifacts for a Smooth Assessment:

- ☑ Have an SSP that speaks to how the "system" is implemented
- ☑ Address each of the objectives in the SSP
- ☑ Ensure each of the components of your system is accounted for
- ☑ If referencing, ensure you point to the specific item
- ☑ Make sure your SSP is up-to-date
- ☑ Organize your artifacts
- ☑ Make sure you have artifacts for each component
- ☑ If using third-party external service providers, account for them
- ☑ Document who is responsible for what items
- ☑ Have certificate numbers available

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

CYBER AB CMMC CERTIFICATION AUTHORIZED C3PAO

CYBER AB CMMC CERTIFICATION REGISTERED PRACTITIONER ORGANIZATION RPO

CAICO CERTIFIED CMMC PROFESSIONAL

CAICO LTP

WHY REDSPIN

- Over 100 security advisors and assessors ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including the first successful Joint Surveillance Voluntary Assessment Program (JSVAP) assessment
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helping countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
800.721.9177
www.redspin.com