Cybersecurity Maturity Model Certification

Report by
Anthony J. Karels

In Partial Fulfillment of the Requirements for the
Degree of
Master in Cybersecurity

Faculté
sciences &
sciences de
l'ingénieur
ubs
Université Bretagne Sud

UNIVERSITÉ BRETAGNE SUD
Lorient, France

Defended 24 June, 2024

ABSTRACT

This project focuses on supporting a Defense Industrial Base (DIB) client within the aerospace research and development sector in their pursuit of the Cybersecurity Maturity Model Certification (CMMC). The goal of the project aims to guide the client through the CMMC certification process, targeting completion by Q1 2025. This corresponding report involves detailed research into the origins, laws, and regulations governing CMMC, and details a seven-step CMMC readiness process.

Key activities include asset designation, documentation, implementation of cybersecurity practices such as flaw remediation and control of remote access, and an emphasis on the importance of proper scoping and documentation. A detailed look into firewalls is presented, along with some advanced functions (such as ZTNA) and how they can help meet numerous compliance controls. Other software tools are also explored to examine their usefulness in helping to organize the certification process.

Moreover, the project provides insights into the working environment at Top Dog PC Services, including the roles and responsibilities of team members. Emphasis is placed on collaborative efforts and the necessity of continuous learning and adaptation, given the organization's first foray into CMMC assessments. The report concludes with recommendations for improving the assessment process, such as enhanced tracking mechanisms, centralized documentation, and additional advisory resources to ensure a comprehensive and compliant approach to CMMC certification. It additionally underscores the critical need for thorough planning and resource allocation to address potential compliance gaps effectively.

Keywords: Compliance, Controls, CMMC, CUI, DIB, DoD, Firewall, NIST, Policies, Practices, Scoping

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Number *Page*

Chapter 1

PROJECT OVERVIEW

1.1 Introduction

Beginning 3 May 2024, I began to work full-time on an intensive compliance project with my employer, Top Dog PC Services. I was assigned the task of supporting one of our highly valued Defense Industrial Base (DIB) clients within the aerospace research and development sector in their pursuit of the Cybersecurity Maturity Model Certification (CMMC). Upon joining the project, I found certain steps appeared to have been initiated or completed prior to my involvement. To integrate smoothly into the ongoing efforts, I began by familiarizing myself with these tasks and the broader certification process. My initial focus was on researching the foundational origins, laws, and regulations that govern the certification process.

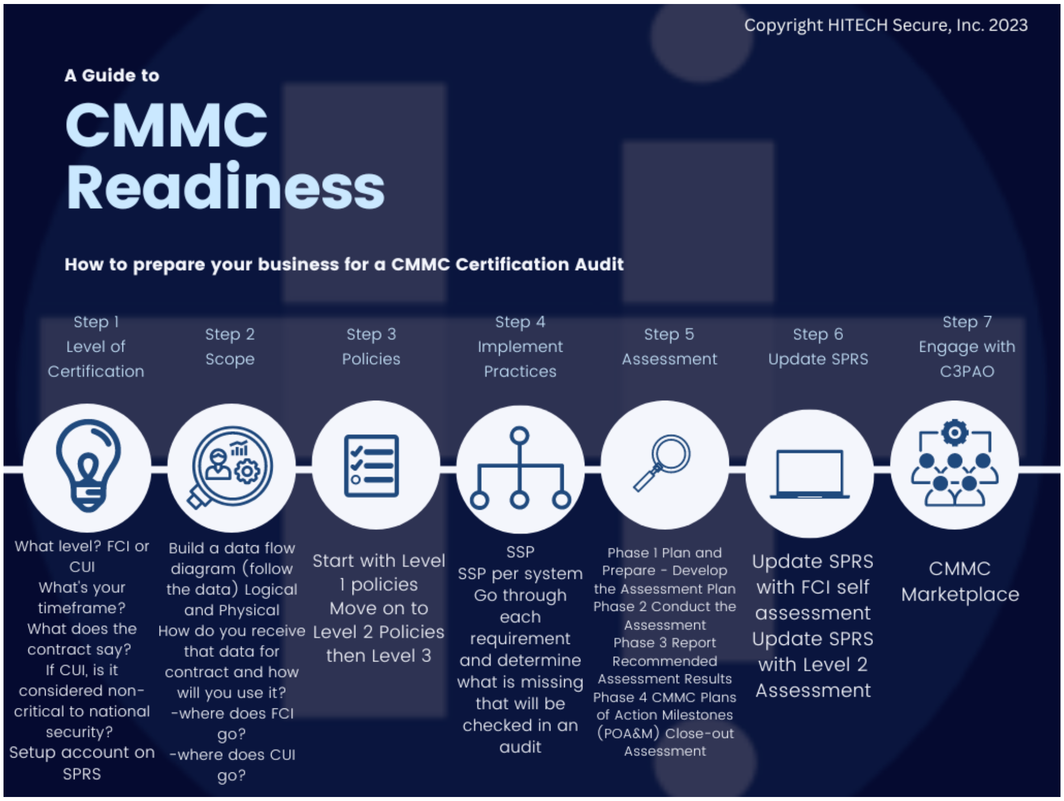
It became evident that achieving CMMC certification is a meticulous endeavor, and it was communicated that our client may not complete the process during the initial six-week period dedicated to my project report. Nonetheless, the client's objective was to achieve certification by Q1 2025, ahead of the anticipated finalization of certification requirements. Additionally, Top Dog PC Services must also achieve certification to continue supporting our client, prompting additional research into our own compliance measures. To guide us, we would be following a seven-step *CMMC Readiness* (1.1) process outlined by our VP and Head of Security Operations.

1.2 Working Environment

All work on this project was primarily conducted at the company offices located in Saint Paul, Minnesota, United States. Top Dog is a Managed Service Provider (MSP) offering fully managed IT support, compliance assessments, and cybersecurity services. The company primarily consists of a help-desk department and a projects department, operating with slightly fewer than 20 full-time employees. My schedule was a typical 8:00 AM to 5:00 PM workday with a one-hour lunch break, Monday through Friday. Each morning there is a 'group huddle' with the entire company conducted via Teams to set the day's agenda and address any concerns, with additional meetings concerning individual departments throughout the week.

My role in the company is that of a Level 2 Project Engineer, focusing on networking, systems administration, cybersecurity, and other related areas. I primarily work under the direction of a project manager, along with two additional Project Engineers. All work on this specific project was performed under the supervision of Jordon Darling, who is both Vice President and the Head of Security Operations. His qualifications include Certified Information Systems Security Professional (CISSP), Certified Virtual Chief Information Security Officer (CvCISO), Certified CMMC Professional (CCP), Microsoft Certified Professional (MCP) x 2, Microsoft Small Business Specialist (SBSC), and Microsoft Specialist (MS).

Due to the project's sensitive nature, the spacific Organization Seeking Certification (OSC) we are working with shall be referred to simply as *the client* throughout this report. Any potentially sensitive information will either be redacted or altered to preserve the client's anonymity and security. Communication was established through their IT/Engineering Manager and an intern assisting with the project. Correspondence with them included both email and weekly Teams meetings on Fridays to review the week's progress.



Copyright HITECH Secure, Inc. 2023

A Guide to

CMMC Readiness

How to prepare your business for a CMMC Certification Audit

Step 1
Level of Certification

What level? FCI or CUI
What's your timeframe?
What does the contract say?
If CUI, is it considered non-critical to national security?
Setup account on SPRS

Step 2
Scope

Build a data flow diagram (follow the data) Logical and Physical
How do you receive that data for contract and how will you use it?
-where does FCI go?
-where does CUI go?

Step 3
Policies

Start with Level 1 policies
Move on to Level 2 Policies then Level 3

Step 4
Implement Practices

SSP
SSP per system
Go through each requirement and determine what is missing that will be checked in an audit

Step 5
Assessment

Phase 1 Plan and Prepare - Develop the Assessment Plan
Phase 2 Conduct the Assessment
Phase 3 Report Recommended Assessment Results
Phase 4 CMMC Plans of Action Milestones (POA&M) Close-out Assessment

Step 6
Update SPRS

Update SPRS with FCI self assessment
Update SPRS with Level 2 Assessment

Step 7
Engage with C3PAO

CMMC Marketplace

Figure 1.1: The CMMC Readiness Roadmap [HITECH Secure, 2023]

Chapter 2

WHAT IS CMMC?

The increased frequency of cyberattacks on the Defense Industrial Base (DIB) has necessitated an urgent need to protect information related to United States national security concerns. Foreign nation-states find it easier to target the DIB rather than the US Department of Defense (DoD) itself because the DIB has not yet prioritized its cybersecurity posture. The idea is that through multiple attacks on the large periphery of DIB contractors, the exfiltration of sufficient unclassified information can, in aggregate, reveal classified information. To enhance the cybersecurity measures of the DIB, the DoD has introduced various cyber resilience initiatives over the years and is presently in the final stages of developing the Cybersecurity Maturity Model Certification (CMMC) version 2.0. In a nutshell, CMMC is the DoD's solution to ensure that all DIB contractors implement a standard set of cybersecurity practices to protect controlled information.

2.1 Controlled Information

There are numerous types of unclassified information that do not meet the specifications for classified information but still must be secured and kept confidential — thus, *controlled*. This includes Federal Contract Information (FCI), Controlled Unclassified Information (CUI), Covered Defense Information (CDI), and others. However, the scope of this report will only discuss FCI and CUI, with a primary focus on CUI. For reference, all CUI is FCI, but not all FCI is CUI. More specific examples of each can be seen in table 2.1, and described as follows:

Federal Contract Information (FCI)

"*Federal Contract Information* means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments." (*48 CFR § 52.204-21* 2016)

Controlled Unclassified Information (CUI)

"*Controlled Unclassified Information* is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency." (*32 CFR § 2002.4* 2016)

FCI	CUI
Contracts	Research And Engineering Data
Subcontracts	Engineering Drawings And Related Lists
Proposals	Specifications
Quotations	Standards
Financial Records	Process Sheets
Audit Reports	Manuals
Pricing Information	Technical Reports
Marketing Plans	Technical Orders
Customer Information	Catalog-Item Identifications
	Data Sets/Studies
	Analyses And Related Information
	Computer Software Executable Code
	Source Code

Table 2.1: Common examples of FCI and CUI.

2.2 Origins of CMMC

The origins of CMMC could be said to have arisen with the requirements set by Executive Order 13556 signed November 4, 2010, which established a program for handling CUI that requires dissemination controls to safeguard its content. Prior to this, agencies and DIB contractors employed policies specific to their own needs and were not standardized across different entities. (Obama, 2010)

This executive order was later codified into Title 32 Code of Federal Regulations (CFR) section 2002, and in 2013 the DoD began implementing these requirements through the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012[1]. The clause required DIB contractors handling CUI to imple-

[1] Safeguarding Covered Defense Information and Cyber Incident Reporting

ment specific cybersecurity controls based on National Institute of Standards and Technology (NIST) SP 800-171 as soon as possible, but not later than 31 December 2017. Although these requirements were in-place, allowances for DIB contractors to self-report their adherence contained in DFARS 252.204-7019[2] meant that there were few controls which could guarantee compliance.

In 2019, the DoD Inspector General issued a report on the audit of protection of DoD CUI on DIB contractor networks, along with the Navy's Cyber Readiness Review which showed little or no progress was made by the DIB in implementing DFARS 252.204-7012. Subsequently, in order to develop a process to validate DIB companies were in-fact protecting CUI, the Defense Contract Management Agency (DCMA) founded the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) to perform compliance assessments. As a result of these individual assessments, DIBCAC began noticing substantial gaps in the implementation of the required NIST standards by much of the DIB. Seeing there are more than 220,000 DIB contractors, it was recognized that performing individual assessments on all of them would be unrealistic.

In response to these wide ranging assessment gaps, the DoD created the CMMC program to verify that DIB contractors were implementing NIST SP 800-171 in accordance with DFARS 252.204-7012 to ensure CUI was adequately secured as required by 32 CFR § 2002. CMMC 1.0 was released in January 2020 and introduced 5 maturity levels, each with specific practices and objectives around securing FCI and CUI. Following a period of public comments concerning the initial program, DoD announced an update to CMMC in November 2021. CMMC version 2.0 reduced the number of maturity levels from 5 tiers to 3, security requirements unique to the program were also eliminated, and other regulatory procedures were changed or dropped in order to streamline the process (see Figure 2.1).

The Cybersecurity Maturity Model Certification (CMMC) Proposed Rule Overview video provided insights into the timeline, highlighting key developments in the certification process and regulatory milestones (Army Multimedia and Visual Information Division, 2024).

[2] Notice of NIST SP 800-171 DoD Assessment Requirements

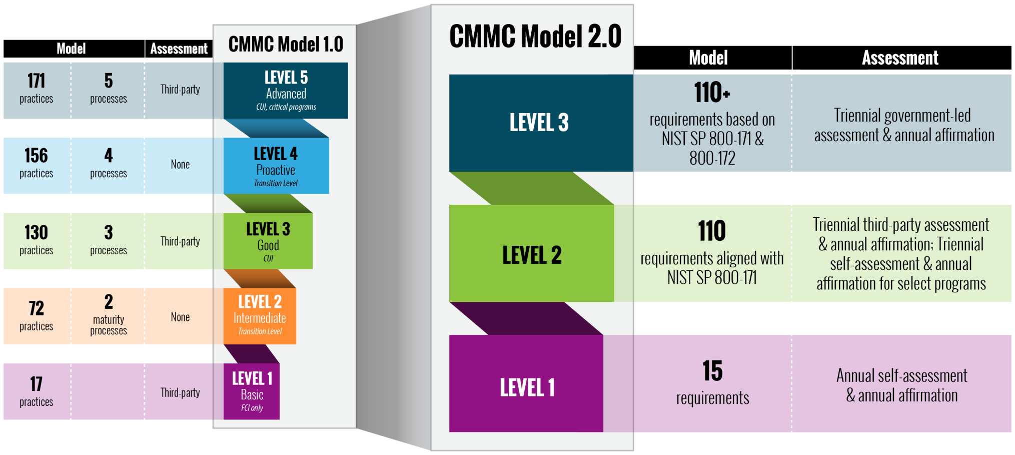


Figure 2.1: Comparison between CMMC 1.0 & CMMC 2.0 [DoD, 2021]

2.3 Certification Levels

Before the update, CMMC 1.0 contained 5 maturity levels, with levels 2 and 4 being transitional. The new CMMC 2.0 model now contains only 3 levels: Foundational, Advanced, and Expert. Each level has a slightly different certification assessment process, becoming more intensive at each successive level. Additionally, all three levels will be required to submit a yearly affirmation and attestation signed by senior management, that compliance will be maintained in-between assessments.

Level 1 - Foundational

The first level is the least restrictive, with only 15 requirements derived from the basic safeguarding requirements found in Federal Acquisition Regulation (FAR) Clause 52.204-21. The assessment is also more lenient than levels 2 or 3, requiring only annual self-assessments to ensure compliance. This level is concerned only with FCI, and is not considered critical to national security.

Level 2 - Advanced

The second level is more arduous in its practice requirements, which have been specifically aligned to follow the controls detailed within NIST SP 800-171 revision 2. This level adds 95 controls to the 15 controls from level 1 for a total of 110 requirements. Since Level 2 certification involves the handling of CUI, it requires an assessment every three years from a Certified Third-Party Assessor Organization (C3PAO).

Level 3 - Expert

The third level is the most stringent out of the three, and includes all 110 requirements from Level 2 and 24 additional requirements which are aligned with NIST SP 800-172. As the highest and most difficult level of certification to obtain, it requires both a Level 2 assessment and a government-led assessment every three years. Level 3 certification deals with CUI from the highest priority programs, and aims to reduce the risk of Advanced Persistent Threats (APT).

2.4 Official Implementation

The timeline for the rollout of CMMC 2.0 will occur in four phases over approximately 2.5 years. During this period, DFARS will gradually incorporate the requirements into new contracts, applying them to all DIB contractors and subcontractors. This process is expected to begin in the first quarter of 2025 and conclude in mid-2028. The phases are:

- **Phase 1:** Level 1 requirements will start appearing in contracts.
- **Phase 2:** Level 2 requirements will begin about 6 months after Phase 1, options to delay may be possible with appropriate approval.
- **Phase 3:** Level 3 requirements will begin about 1 year after Phase 2, and Level 2 requirements will be required in all contracts. An option to delay Level 3 requirements may be possible with appropriate approval.
- **Phase 4:** Certification for all levels will be specified and required in all contracts about 1 year after Phase 3.

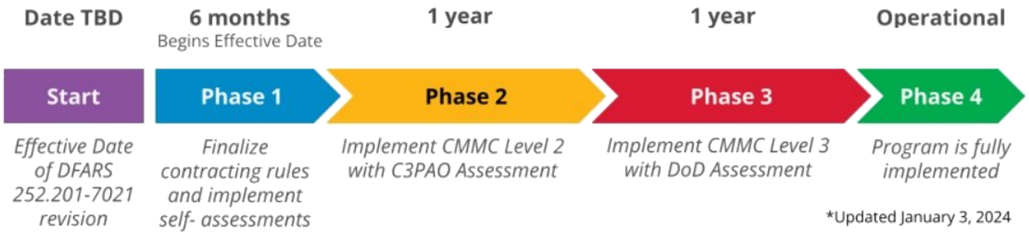

Date TBD
6 months
Begins Effective Date
1 year
1 year
Operational
Start
Phase 1
Phase 2
Phase 3
Phase 4
Effective Date of DFARS 252.201-7021 revision
Finalize contracting rules and implement self- assessments
Implement CMMC Level 2 with C3PAO Assessment
Implement CMMC Level 3 with DoD Assessment
Program is fully implemented
*Updated January 3, 2024

Figure 2.2: CMMC Implementation Timeline [Hive Systems, 2024]

Chapter 3

CERTIFICATION ROADMAP

The CMMC certification process is extremely intricate, necessitating meticulous planning, preparation, revision, and cross-checking to ensure all requirements are satisfied. An holistic understanding of the objectives and requirements of both the CMMC framework and NIST security controls is imperative to successfully pass an assessment. This chapter will go over the CMMC Readiness process implemented and used by Top Dog, which is presented in Figure 1.1.

3.1 Determining Level

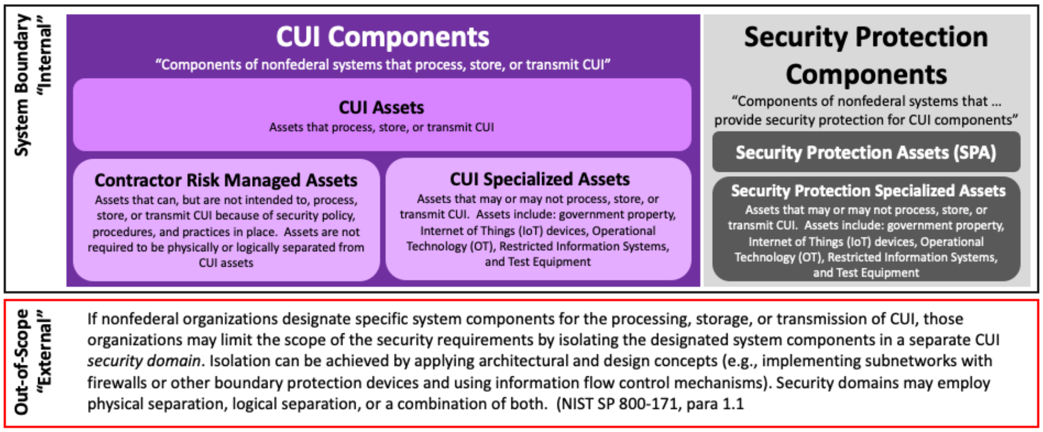
When beginning a CMMC assessment, the first step is to consider what level of certification is required. As previously mentioned, the new CMMC 2.0 guidelines have reduced the number of certification levels from five to three with the aim to reduce confusion and complexity. Verifying the level of certification required by The OSC is a simple matter of reviewing the DFARS contract or proposal, where it shall state the specific level a DIB contractor must be rated at in order to bid on the contract. If not already done so, an account should be registered on the Supplier Performance Risk System (SPRS) portal[1], part of the Defense Information Systems Agency (DISA) Cyber Exchange website, where the Defense Logistics Agency (DLA) can evaluate uploaded SPRS scores.

3.2 Perform Scoping

The process of scoping for a CMMC assessment is extremely important. The artifacts created during the scoping process significantly aid with the implementation of subsequent steps, such as drafting policies, implementing practices, and creation of the System Security Plan (SSP). The point of scoping is to determine and outline the system boundaries through the creation of an exhaustive listing of all system assets, and defining those assets with the intent to identify how CUI is transferred, stored, and processed.

[1] SPRS Portal [https://www.sprs.csd.disa.mil/]

System Boundaries



System Boundary "Internal"

CUI Components

"Components of nonfederal systems that process, store, or transmit CUI"

CUI Assets

Assets that process, store, or transmit CUI

Contractor Risk Managed Assets

Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place. Assets are not required to be physically or logically separated from CUI assets

CUI Specialized Assets

Assets that may or may not process, store, or transmit CUI. Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment

Security Protection Components

"Components of nonfederal systems that … provide security protection for CUI components"

Security Protection Assets (SPA)

Security Protection Specialized Assets

Assets that may or may not process, store, or transmit CUI. Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment

Out-of-Scope "External"

If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. (NIST SP 800-171, para 1.1

Figure 3.1: Scope of Applicability and CMMC Categories [Peak InfoSec, 2022]

NIST SP 800-171 establishes the Scope of Applicability in paragraphs 1.1 and at the start of Chapter 3 (NIST, 2021, p. 10:

> *The term organizational system is used in many of the recommended Controlled Unclassified Information (CUI) security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components.*

Essentially what this means is that the system boundaries for a CMMC assessment are those which process, store, or transmit CUI such as CUI, CRMA, and SA. Additionally in-scope and subject to assessment are the security protection components which are SPA and SPA-SA. While only these system boundaries will be subject to assessment to certify controls are in-place, the out-of-scope assets could also be negatively assessed to ensure they are in-actuality out-of-scope.

External Service Provider

An External Service Provider (ESP) such as a Managed Service Provider (MSP) (like Top Dog) or a Cloud Service Providers (CSP) can fall under the scope of CMMC practices if it handles CUI or provides SPA for the OSC. When assessing an ESP's suitability, we must carefully evaluate several factors. Firstly, examining the ESP's shared responsibility matrix is crucial. This matrix delineates which security control objectives are managed by the provider and which are the contractor's responsibility.

Additionally, contractors should consider the standards and certifications that the ESP adheres to, such as FedRAMP, SOC 2, and CMMC Certification. These accreditations indicate the provider's commitment to meeting stringent security standards, providing confidence in their ability to safeguard sensitive data. Moreover, reviewing the contractual agreements with the ESP—including service-level agreements, memoranda of understanding, and other contracts—is essential. These agreements should explicitly support the contractor's information security objectives and ensure compliance with regulatory requirements like CMMC.

Asset Types

There are 5 categories of assets which must have special attention paid to when scoping, CUI, SPA, CRMA, SA, and Out-of-Scope assets (Figure B.1). Each requires specific attention to whether they require CMMC practices to be implemented, or otherwise be included in the SSP, network diagram, and asset inventory (Figure 3.1):

- **CUI Asset** Assets that process, store, or transmit CUI.
- **Security Protection Asset (SPA)** Assets which provide security functions or capabilities, irrespective of whether or not these assets process, store, or transmit CUI.
- **Contractor Risk Managed Asset (CRMA)** Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place. Not required to be physically or logically separated from CUI assets.
- **Specialized Asset (SA)** Assets that may or may not process, store, or transmit CUI.
- **Out-of-Scope Asset** Assets that cannot process, store, or transmit CUI.

Asset Inventory

The asset inventory is a comprehensive list of all IT resources within an organization, including hardware, software, and data. This inventory is crucial for identifying and

	CUI	SPA	SA	CRMA	OoS
Implement CMMC	✓	✓			
System Security Plan	✓	✓	✓	✓	
Network Diagram	✓	✓	✓	✓	✓
Asset Inventory	✓	✓	✓	✓	

Table 3.1: Asset Designation and Documentation Matrix.

managing the security posture of each asset. After conducting a thorough assessment of all devices, they can be assessed by function and categorized into one of the five asset types in a categorization matrix which will help define the system boundaries.

Network Topology

The network topology is the arrangement and interconnection of various network devices and systems within an organization's IT infrastructure. It includes the physical and logical design of the network, illustrating how different nodes like servers, workstations, routers, switches, and security devices such as firewalls are connected and communicate. Properly documenting and securing network topology is crucial for achieving CMMC compliance, as it helps identify potential vulnerabilities and ensures that cybersecurity controls are effectively implemented across the network.

Data Flow Diagram

The Data Flow Diagram (DFD) illustrates how data moves through an organization's information systems. It shows the sources, destinations, storage points, and paths that data takes as it flows through processes and between different network components. Creating a DFD helps organizations understand and document how sensitive data like FCI and CUI is handled, which is essential for identifying potential vulnerabilities and ensuring that appropriate cybersecurity controls are in place to protect data integrity and confidentiality.

3.3 Write Policies

Having comprehensive policies in-place is fundamental to meeting and being in compliance with the CMMC guidelines. Policies are foundational to an organization's cybersecurity framework, and essentially become *the rules of the game* which must be followed once implemented. Effective policies ensure that everyone in the organization understands what their roles and responsibilities are, and provide a clear roadmap for practicing and enforcing good security controls.

When writing policies for CMMC, it is essential to align them with every domain and every practice within the 17 domains (listed in Table 3.2), ensuring that each has a corresponding policy written for it. This involves a thorough understanding of the CMMC framework, specifically including the assessment objectives of each practice, in order to build a detailed and specific policy which covers all relevant aspects of it. Each policy must clearly define its scope, objectives, and the responsibilities of various stakeholders within the organization.

In addition to being comprehensive, policies must also be practical and enforceable. This means that the policies should be realistic, taking into account the organization's resources, infrastructure, and operational context. They should include step-by-step procedures for implementing the necessary controls and mechanisms for monitoring and measuring compliance. It is also important to regularly review and update the policies to ensure they remain relevant and effective in the face of evolving threats and changes in the organizational environment.

Finally, effective communication and training are critical to the successful implementation of CMMC policies. Once the policies are developed, they must be clearly communicated to all employees, contractors, and stakeholders. Regular training sessions and awareness programs should be conducted to educate everyone on the importance of the policies and their role in ensuring cybersecurity. This not only helps in achieving CMMC compliance but also in building a strong security culture within the organization.

3.4 Implement Practices

As discussed earlier, each level of the CMMC 2.0 framework incorporates practices aligned with the controls specified in relevant cybersecurity standards and regulations. Level 1 practices align with the controls outlined in FAR Clause 52.204-21, which also align with NIST SP 800-171. Level 2 practices are wholly aligned with NIST SP 800-171, and comprise the main focus of this report. The additional controls introduced at Level 3 detailed in NIST SP 800-182 however, are beyond the scope of the project.

Practices & Controls

It is important to note the slight difference between the terms *controls* and *practices*, which are sometimes used interchangeably but do have some slight differences:

- **Controls:** Controls refer to specific technical or administrative measures that are implemented to mitigate risks and achieve cybersecurity objectives. These are detailed requirements that specify how certain aspects of information security should be managed, such as access control, encryption, and incident response.

- **Practices:** Practices encompass a broader range of activities or actions that organizations should undertake to achieve a desired level of cybersecurity maturity. They can include implementing controls but also extend to policies, procedures, guidelines, and organizational behaviors that contribute to effective cybersecurity management.

Code & Practice Domain	**Description**
(AC) Access Control	Limit access to authorized users
(AM) Asset Management	Manage and maintain organizational assets
(AU) Audit & Accountability	Implement auditing mechanisms
(AT) Awareness & Training	Educate personnel on cybersecurity risks
(CM) Configuration Management	Establish and maintain baseline configurations
(IA) Identification & Authentication	Identify and authenticate users
(IR) Incident Response	Detect, report, and respond to incidents
(MA) Maintenance	Perform routine maintenance
(MP) Media Protection	Protect and control media
(PS) Personnel Security	Screen personnel prior to employment
(PE) Physical Protection	Protect physical assets
(RE) Recovery	Develop and implement recovery plans
(RM) Risk Management	Identify, assess, and mitigate risks
(CA) Security Assessment	Assess and monitor security controls
(SA) Situational Awareness	Maintain awareness of cybersecurity threats
(SC) System & Communications Protection	Control and protect communications
(SI) System & Information Integrity	Protect against malicious code

Table 3.2: The 17 CMMC 2.0 Level 2 Practice Domains

Details on how to implement each of the 110 practices can be found within both the CMMC Assessment Guide and the NIST SP 800-171 documentation, additionally the 320 Assessment Objectives (AO) are found in NIST SP 800-171A. These documents provide valuable insights on what an assessor would be checking to confirm controls are adequately met when evaluating the system. Each practice is addressed by first presenting a short summary, then assessment objectives are listed in a lettered list, followed by some discussion points, examples, and considerations to provide additional background information and assistance with understanding the practice.

System Security Plan (SSP)

As each practice is addressed through the adherence to the controls and the implementation of policies, procedures, and technical solutions to meet the requirements, the details should be added to the SSP. The intent of this document is to provide a description of an information system, its cybersecurity stance, and even physical security. It should make clear what may be potential problems, and provide a record over time to help track and reference as updates and changes are made. When completed, the SSP could be anywhere from 50-100 or even up to 200 pages long, and should contain references to: computers, networking, software, people, support, and the physical facility. The *System* in this sense is not an *IT System* but the entire environment which allows the organization to function.

3.5 Perform Assessment

This stage might be considered more as *mock assessment* since its four phases mimic those performed by an assessor during an official assessment. The principle behind conducting this self assessment is to try to visualize the system landscape from an assessor's perspective in order to suss out any gaps in implementation before the official assessment. Aiming to detect as many issues as possible during this stage will increase confidence leading up to the final assessment.

Phase 1: Plan & Prepare

This phase involves establishing the scope and objectives of the assessment just as an assessor would. During this phase, relevant documentation is gathered, and the assessment scope is confirmed. Time should be taken to understand the environment and plan the assessment schedule with the organization seeking certification. All necessary resources should be in place and functioning as they would during an official assessment. Proper planning and preparation will be the foundation for a thorough and effective assessment whether a self assessment or the real thing.

Phase 2: Conduct Assessment

Conducting an assessment involves evaluating cybersecurity controls against the CMMC criteria. Tools such as the free Cybersecurity Evaluation Tool (CSET) (section 4.1) created by the Cybersecurity and Infrastructure Security Agency (CISA), *FutureFeed* (section 4.2), and many other applications can be extremely helpful when performing a self assessment. This phase is crucial for checking the evidence of compliance with each practice required by the targeted CMMC level. Detailed and systematic assessment activities help in identifying strengths and areas needing improvement.

Phase 3: Report Results

The findings of the assessment are next documented comprehensively by compiling the assessment results into a report that highlights strengths, weaknesses, and areas of non-compliance. The report provides detailed findings and observations, along with recommendations for improvement. Clear and precise reporting ensures that the organization understands the assessment outcomes and areas that require attention. Many tools also provide the capability to automatically generate detailed reports and presentations to assist with this phase.

Phase 4: Create POA&M

The final step of creating the Plan of Action and Milestones (POA&M) involves developing a plan to address gaps identified in the previous phases to achieve compliance. Based on the assessment findings, a POA&M is developed which outlines the specific actions, timelines, and responsible parties for addressing deficiencies. This document serves as a final roadmap for remediation efforts, ensuring that all necessary improvements are made before the final certification review. A well-structured POA&M facilitates systematic remediation and boosts confidence during the final spot check of the CMMC Readiness roadmap.

3.6 Update SPRS

The SPRS score is a metric used by the DoD to assess the cybersecurity posture of DIB contractors. This score helps the DoD evaluate the cybersecurity risk associated with working with various contractors and suppliers. It is based on an assessment of how well controls are implemented through an evaluation of the contractor's practices, policies, and procedures. Each of the 110 controls for CMMC Level 2 has a different value associated with it based on its importance — either 1, 3, or 5, with 1-point items being the least critical and 5-point items being the most critical. The scoring does not start at zero; instead, it begins with a negative value of -203 and increases to 110 as each control is implemented.

A number of tools can assist with evaluating the SPRS score, again including CSET (section 4.1) and *FutureFeed* (section 4.2) which are discussed in more detail later. The SPRS score is then uploaded and managed on the official SPRS website, which is part of the DISA Cyber Exchange website. Contractors and vendors who are part of the DIB can access and update their SPRS scores through this platform.

3.7 Engage C3PAO

The final step in the CMMC Certification Roadmap is to engage a Certified Third-Party Assessor Organization (C3PAO) to conduct the official assessment. This phase is critical, as it involves a comprehensive evaluation of the OSC's cybersecurity practices against the CMMC requirements. C3PAOs are entities accredited by the CMMC Accreditation Body (Cyber AB) to conduct official assessments of OSC. Cyber AB is responsible for both accreditation and oversight of C3PAOs, ensuring that they maintain the highest levels of quality, integrity, and professionalism. They also establish the guidelines and criteria that C3PAOs must follow, including rigorous training and certification processes for individual assessors. The critical role C3PAOs play in evaluating an organization's adherence to CMMC requirements ensures that the OSC's cybersecurity practices meet the necessary standards.

Before the final audit, it is recommended to conduct a 20-control *spot check* to gauge readiness. The spot check involves an evaluation on 20 key controls that provide a representative snapshot of the overall cybersecurity posture. This pre-assessment is designed to identify any remaining gaps and ensure preparedness for the full assessment. During this step, the C3PAO will assess the organization based on these 20 controls without providing guidance on how to pass, maintaining the integrity and objectivity of the assessment process. The spot check is typically about 25% of the cost of the final assessment, making it a cost-effective strategy to confirm readiness and mitigate the risk of being unprepared for the full assessment.

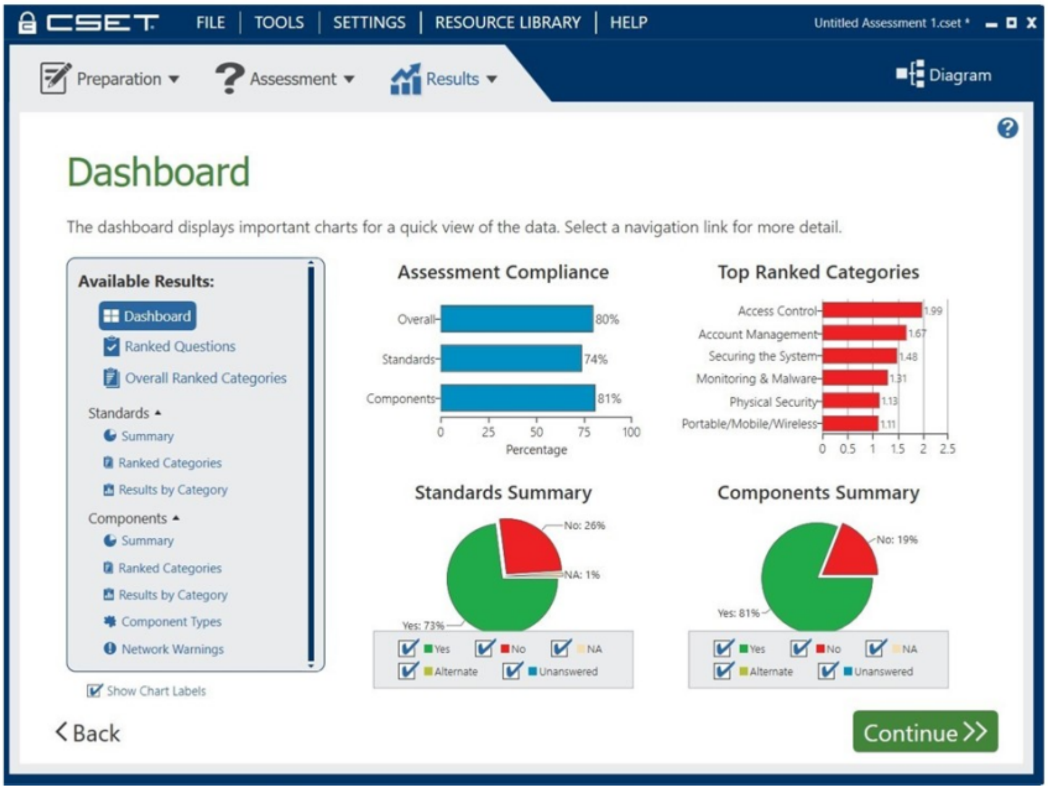
Following the spot check, the C3PAO will proceed with the comprehensive assessment, utilizing the same four phases discussed in the *Perform Assessment* section: Plan and Prepare, Conduct Assessment, Report Results, and Create POA&M. This final assessment is thorough and may evaluate any of the required controls to determine compliance. The assessors will conduct interviews, review documentation, and observe processes to ensure the organization's cybersecurity practices meet the stringent CMMC standards. The outcome of this assessment will determine if the standards have been met to convey certification, and if allowed, identify any areas needing improvement which can be assigned to a final POA&M.

Chapter 4

CMMC TOOLS

Due to the massiveness of the CMMC certification process, numerous tools have become available which aim to assist with the organization of records, policies, processes, and control objectives. There are even third-parties offering entire certified operating environments referred to as *enclaves*. As can often be seen when governments mandate new regulations, an entire ancillary economy springs up around it providing third-party tools to support and cater to the affected companies.

4.1 Cybersecurity Evaluation Tool (CSET)



The dashboard displays important charts for a quick view of the data. Select a navigation link for more detail.

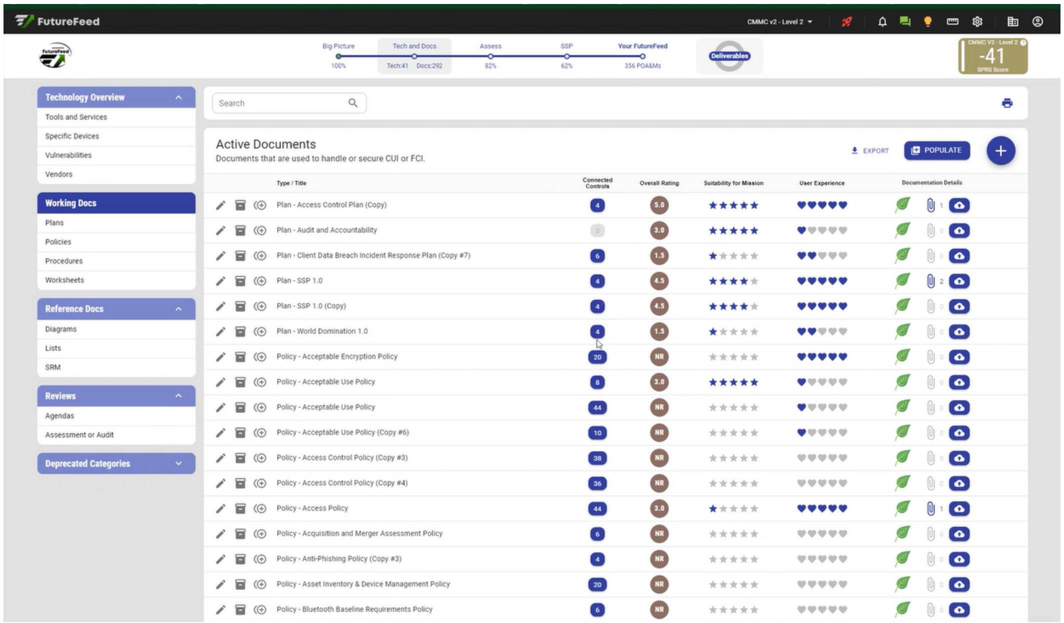
Figure 4.1: CSET Results Dashboard

CSET is a free software application provided by CISA which assists with the evaluation of an organization's cybersecurity posture according to various frameworks. In our case, we utilized the tool to perform an evaluation using its questionnaire to assess against all 110 NIST SP 800-171 controls. When assessing each control, it can be marked as either *met*, *not met*, or *not applicable*, along with an additional field to add notes.

The tool then allows for the computation of the SPRS score so it can be reported to DoD. While not as fully featured as other tools like *FutureFeed*, which will be discussed next, this free tool should not be overlooked when making an initial assessment. It can provide valuable insights into an organization's cybersecurity posture by generating reports that highlight strengths and weaknesses and offer prioritized recommendations.

4.2 FutureFeed

Before officially starting with the project I was able to join a video call concerning *FutureFeed*, a tool intended to help manage the CMMC certification process. You begin by entering all the information concerning the Organization Seeking Certification and answering an assessment based on NIST SP 800-171 similarly to CSET. It will then automatically generate a gap assessment and SPRS score, and provides additional tools to help close the gaps and track progress in a collaborative environment.



Active Documents
Documents that are used to handle or secure CUI or FCI.

Type / Title	Connected Controls	Overall Rating	Suitability for Mission	User Experience	Documentation Details
Plan - Access Control Plan (Copy)	4	5.0	★★★★★	♥♥♥♥♥	1
Plan - Audit and Accountability	0	3.0	★★★★★	♥♡♡♡♡	0
Plan - Client Data Breach Incident Response Plan (Copy #7)	6	1.5	★☆☆☆☆	♥♥♡♡♡	0
Plan - SSP 1.0	4	4.5	★★★★☆	♥♥♥♥♥	2
Plan - SSP 1.0 (Copy)	4	4.5	★★★★☆	♥♥♥♥♥	0
Plan - World Domination 1.0	4	1.5	★☆☆☆☆	♥♥♡♡♡	0
Policy - Acceptable Encryption Policy	20	NR	☆☆☆☆☆	♥♥♥♥♥	0
Policy - Acceptable Use Policy	8	3.0	★★★★★	♥♡♡♡♡	0
Policy - Acceptable Use Policy	44	NR	☆☆☆☆☆	♥♡♡♡♡	0
Policy - Acceptable Use Policy (Copy #6)	10	NR	☆☆☆☆☆	♥♡♡♡♡	0
Policy - Access Control Policy (Copy #3)	38	NR	☆☆☆☆☆	♡♡♡♡♡	0
Policy - Access Control Policy (Copy #4)	36	NR	☆☆☆☆☆	♡♡♡♡♡	0
Policy - Access Policy	44	3.0	★☆☆☆☆	♥♥♥♥♥	1
Policy - Acquisition and Merger Assessment Policy	6	NR	☆☆☆☆☆	♡♡♡♡♡	0
Policy - Anti-Phishing Policy (Copy #3)	4	NR	☆☆☆☆☆	♡♡♡♡♡	0
Policy - Asset Inventory & Device Management Policy	20	NR	☆☆☆☆☆	♡♡♡♡♡	0
Policy - Bluetooth Baseline Requirements Policy	6	NR	☆☆☆☆☆	♡♡♡♡♡	0

Figure 4.2: FutureFeed Control Panel

As we were discussing the application, the representative made a poignant observation concerning the difficulties of compliance:

> *The big thing about compliance is not the technical part, or writing policies and procedures... that's easy. The hard thing is organizing the records which the policy says they should do.*

It allows for policies to be connected to controls via tagging, and then connect to different documents such as network maps, data flow diagrams, or onboarding information. Evidence can then be collected to show that the policy is actually being followed should an assessor ask for confirmation. Additionally, reports and presentations can be automatically generated to prove the current compliance level.

4.3 CUIck Trac Enclave

We had another online meeting with a company offering a product called *CUIck Trac*[1] which is essentially a self-contained virtual environment which has been pre-configured to meet all the technical practices of NIST SP 800-171. This virtual environment is also known as an *enclave* because it operates distinctly from the rest of an organization's IT operations, and has been isolated to contain systems, applications, and data in a high security zone.

An example use case for the DIB is the utilization of an enclave to handle all CUI-related activities. This enclave would be isolated from the rest of the corporate network, with strict access controls and enhanced security measures in place. The organization only needs to focus its CMMC compliance efforts on the enclave, ensuring that all necessary controls and practices are implemented and maintained. When using the CUIck Trac enclave however, all the work to ensure compliance has already been done, thus freeing the organization to focus its time elsewhere.

In our client's case however, this off-the-shelf solution may not be as practical as proposed, since the CUI in their environment will need to operate outside the bounds of the enclave. The solution was also considered for our own purposes, as it may be more practical to use a certified enclave environment to perform IT support duties with the client rather than attempt to re-tool the entire business to meet CMMC guidelines.

[1] CUIck Trac Homepage [https://www.cuicktrac.com/]

4.4 FortiGate Firewall

Though not a tool specific to evaluating CMMC, a firewall is a principle Security Protection Asset (SPA) intricately involved in protecting an organization's network, and serves as the primary gateway to allow and deny access to the company's infrastructure. Not only does it contain the policies which determine which traffic will be allowed and which will be rejected, but it also performs certificate validation, packet inspection, web filtering, application control, and endpoint monitoring. Being an industry partner with Fortinet, we exclusively utilize their FortiGate Next-Generation Firewall (NGFW) solutions, and they have proved to be an extremely beneficial SPA for addressing numerous CMMC/NIST controls.[2]

In addition to the advanced data inspection capabilities of the firewall, it allows segmentation of the network into multiple vLANs in order to keep traffic from less secure endpoints such as IoT, tablets, and guest devices on isolated subnets. When remote users need to access the corporate network, the device's SSL VPN feature is used to provide a secure tunnel into the LAN. These remote devices can be additionally secured through the use of Zero Trust Network Access (ZTNA) clients which perform device health checks to ensure adherence to OS patching, antivirus, encryption, and Multi-Factor Authentication (MFA) requirements which will be discussed in detail in section 5.4.

During my time working on this project, I was able to earn two industry certifications from Fortinet: the Fortinet Certified Fundamentals (FCF)[B.2] and Fortinet Certified Associate (FCA)[B.3]. Upon completing these initial certifications, I received a complimentary firewall device from our representative to aid in my ongoing training for the Fortinet Certified Professional (FCP) in Network Security certification.

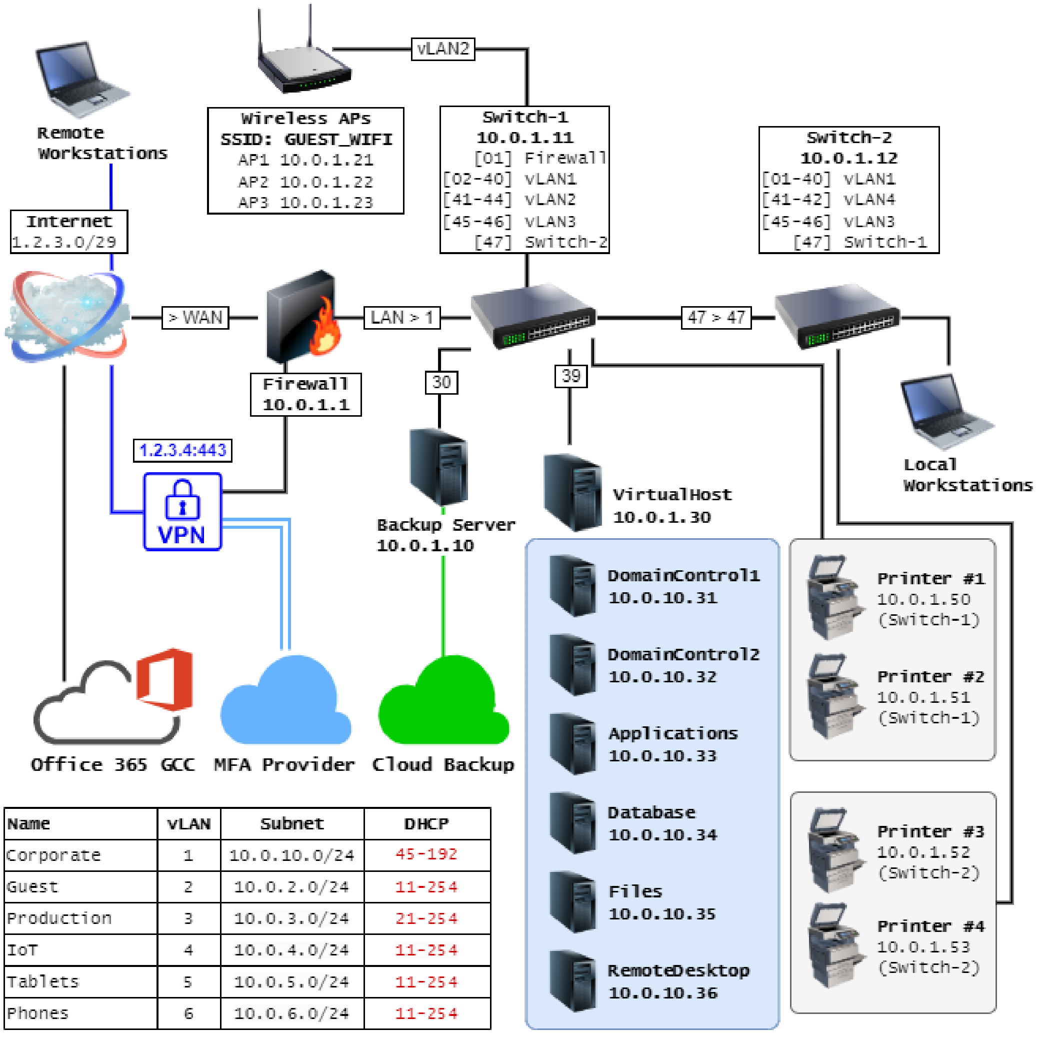
I also started a side project using MicroPython on a Raspberry Pi Pico.[B.4, B.5] This involved exploring serial UART communication and converting the Pico's TTL to RS-232 to interface with the firewall's console port. A touchscreen TFT display will allow users to interact with the device via a GUI, executing scripts loaded via the SD card. The goal is to enable those unfamiliar with FortiGate to provision new devices with standard options. The device will run on LiPo batteries and require a standard DB9 console cable and null modem. Additionally, a 3D-printed case is being designed to house all components compactly and securely.

[2] Fortinet Solutions for CMMC [https://www.fortinet.com/content/dam/fortinet/assets/certifications/comparison-matrix-cmmc-assets.pdf]

Chapter 5

CONTRIBUTIONS

5.1 Scoping: Network Topology



Name	vLAN	Subnet	DHCP
Corporate	1	10.0.10.0/24	45-192
Guest	2	10.0.2.0/24	11-254
Production	3	10.0.3.0/24	21-254
IoT	4	10.0.4.0/24	11-254
Tablets	5	10.0.5.0/24	11-254
Phones	6	10.0.6.0/24	11-254

Figure 5.1: Network Topology Example (Altered and Redacted)

In order to begin to determine which assets may possibly store, process, or transmit FCI or CUI, it was necessary to construct a proper network topology. Though the client did not currently have an existing network diagram, there was detailed documentation available within Top Dog's information management system. Where this did not suffice, or did not contain the sought information, a variety of other tools were used to confirm "the lay of the LAN".

The primary tool employed for creating the diagram was *draw.io*, a commonly used web application chosen for its simple but extensive user interface and helpful feature set. The most obvious place to begin the diagram was to start with the Internet cloud, and then proceed by adding additional network components by confirming their connection to the prior.

Other techniques used included analyzing the Remote Monitoring and Management (RMM) software's device reports to verify the IP addresses of user workstations and servers. Scans performed using `nmap` or similar tools to catalog an entire IP range were also utilized to sniff out devices which may not be monitored by the RMM agents. Additionally, the firewall and switches provided information in the form of DHCP device listings and port mappings referencing MAC address.

5.2 Scoping: Asset Listing

While building the network topology diagram, a correlating asset list was begun using a spreadsheet to create a concise listing of all network devices. Additional spreadsheets will also be created to list software applications, cloud services, and miscellaneous resources. A corresponding device inventory may look similar to the following:

Asset	**Host**	**IP Address**	**Scope**	**Notes**
Firewall	FW01	10.0.10.1	SPA	Main firewall for network
Switch	SW01	10.0.10.2	SPA	Core switch for LAN
Domain Controller	DC01	10.0.10.10	CRMA	Primary domain controller
File Server	FS01	10.0.10.20	CUI	Main file storage
WiFi AP	AP01	10.0.10.30	SPA	SSID: CorporateWifi
WiFi AP	AP02	10.0.10.31	SPA	SSID: GuestWifi
WiFi AP	AP03	10.0.10.32	SPA	SSID: ConfRoom
Printer	PR01	10.0.10.50	CUI	Printer for CUI documents
CNC Machine	CNC01	10.0.10.60	CUI	Uses CUI CAD files
Workstation	WS01	10.0.10.100	CUI	Windows 10 Pro
Workstation	WS02	10.0.10.101	CUI	Linux Ubuntu 20.04
Workstation	WS03	10.0.10.102	CUI	Windows 11 Home

Table 5.1: Example Network Asset Inventory

5.3 Practice: AC.L2-3.1.12 - Control Remote Access

The objective of this practice is to monitor and control remote access sessions, meeting all assessment objectives by determining whether:

[a] remote access sessions are permitted;

[b] the types of permitted remote access are identified;

[c] remote access sessions are controlled; and

[d] remote access sessions are monitored.

My assignment was to investigate solutions for performing a Device Health Check (DHC) on remote devices wishing to connect to the network via the VPN. The investigation primarily addresses assessment objective [c]. Additionally, some advice ascertained from the assessment guide informs us:

> *During session establishment, the message "Verifying Compliance" means software like a Device Health Check (DHC) application is checking the remote device to ensure it meets the established requirements to connect [c].*

(Department of Defense, 2023, p. 38–40, NIST, 2021, p. 13–14, NIST, 2018, p. 14)

This task required that I verify whether the current FortiClient endpoint solution used for making VPN connections supports DHC with the licensed version. My recent training with Fortinet introduced me to their Zero Trust Network Access (ZTNA) and Network Access Control (NAC) solutions for providing DHC capabilities. Motivated by this knowledge, I dug deeper into both technologies to determine which, if any, would meet the practice requirements. After thorough research, it appears that the ZTNA option is the best fit for meeting the assessment objectives.

Zero Trust Network Access (ZTNA)

I was able to confirm the licensed FortiClicent ZTNA edition provides a number of features beyond the unlicensed version, enabled via the FortiClient Enterprise Management Server (EMS). EMS allows for the centralized endpoint management, deployment, configuration, and monitoring. It can be installed either on-premesis, or in the cloud provided the CSP is FedRAMP certified.

Some of the advanced security features enabled through the use of EMS include policy enforcement, Advanced Threat Protection (ATP) including anti-exploit, antivirus, and web filtering, and Endpoint Detection and Response (EDR). Device posture check functions ensure that endpoints meet security compliance controls such as having up-to-date antivirus, patches, and encryption before granting network access to the remote device. While continuous trust verification provides ongoing monitoring of identity and security posture of the endpoint, which can adjust access permissions in real-time.[1]

Network Access Control (NAC)

Since the NAC solution I researched is part of the Fortinet ecosystem, it is naturally called *FortiNAC*. Unlike FortiClient ZTNA, which focuses on zero-trust access for remote applications, FortiNAC is primarily a network access control solution. Its capabilities include device inventory management and onboarding, dynamic network segmentation, SIEM orchestration, and continuous device monitoring. One key difference is that FortiNAC is deployed either as a hardware appliance or a virtual machine on the LAN network, rather than as a software application running on a client device. Even if an unrecognized device plugs into a local LAN port, FortiNAC can sandbox the device using least-privilege access restrictions until it can be verified. Being primarily focused on internal enterprise networks, FortiNAC encompasses much more than is required to meet the assessment objectives concerning remote access monitoring and would not be the best choice for this use case.

5.4 Practice: AC.L2-3.1.13 - Remote Access Confidentiality

This practice concerns the employment of cryptographic mechanisms used to protect the confidentiality of remote access sessions. The assessment objectives seek to determine if:

> **[a]** cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and
>
> **[b]** cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

[1] EMS Administration Guide [`https://docs.fortinet.com/document/forticlient/7.0.4/ems-administration-guide/24450/introduction`]

The assessment considerations also explain:

> *Are cryptographic mechanisms used for remote access sessions (e.g., Transport Layer Security (TLS) and Internet Protocol Security (IPSec) using FIPS-validated encryption algorithms) defined and implemented [a,b]? Note that simply using an approved algorithm is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140.*

(Department of Defense, 2023, p. 41–42, NIST, 2021, p. 14, NIST, 2018, p. 14)

Federal Information Processing Standards

Federal Information Processing Standards (FIPS) is a standard for validating the cryptographic modules used by the US federal government and regulated industries to secure sensitive information. Modules referencing FIPS 140 validation means they have been assessed by a NIST-accredited Cryptographic Module Validation Program (CMVP) laboratory against the requirements found in FIPS Publication 140-2. (NIST, 2002)

Application of Controls

When assigned to address the fulfillment of this practice, I learned that both the firewall VPN and the cloud-based Outlook 365 email service would fall under the umbrella of the practice. This necessitated a review of current configurations and settings to identify any gaps in compliance. I needed to verify that both items either were or could be FIPS validated and document the steps required to ensure they complied.

Outlook 365

My research on the validation of Outlook 365 was very expedient, and I was able to find a suitable reference confirming it would suffice as-is, without requiring any additional updates or changes to how it was already utilized in the client's environment. A relevant Microsoft document confirmed *"All Microsoft Entra customer-facing web services are secured with the Transport Layer Security (TLS) protocol and are implemented using FIPS-validated cryptography."* [2]

[2] Configure CMMC Level 2 Access Control (AC) controls [`https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-access-control`]

Virtual Private Network

Validating the VPN proved to be a bit more difficult, not due to a lack of technical capability, but because of questions regarding the requirements of the FIPS validation itself. I learned that the firewall did have the capability of operating in a specialized "FIPS-CC" (Common Criteria) mode, which was documented on the Fortinet community forum.[3] The FIPS firmware version (FortiOS 7.0.12) was slightly older than the current release (FortiOS 7.4), but it remained within the current 7.0 branch and should retain a common feature set. Although this version was validated on the NIST website, Fortinet's firmware archive also included a patched version addressing recent CVEs affecting it.[4] Since the unpatched version of the firmware was the one validated by NIST, it raised questions about the compliance of the patched version.

I also had questions concerning an *entropy token* device which I had read about on the webpage explaining FIPS-CC mode activation. It seemed that the FortiGate 50E device required a USB-based entropy device to assist with true random number generation, which led me to assume that the 60E device I was working with might also need one. After contacting a Fortinet engineer about the entropy token, I learned that it wasn't necessary for the 60E. The engineer explained that "the 60E has SOC3 ASIC which includes CP9lite" and directed me to a technical document mentioning a "Ring OSC entropy source" used for random number generation.[5]

Concerning the validated firmware build, the engineer also reported to me that "FIPS-CC-70-6 is an old firmware with known vulnerabilities, and you should not operate on that firmware unless there are no other options." It certainly makes sense to use the patched version, but *technically*, it was not the NIST-validated option. I am realizing government regulations can seem to hinder security efforts due to the time and resources required for reassessing patched software after mitigating a new vulnerability. I am still awaiting a final response on this matter from someone in the compliance department.

Finally, the firewall VPN uses a default factory certificate which is not certified by a trusted Certificate Authority (CA) and will prompt the client to accept a certificate

[3] Technical Tip: How to enable FIPS-CC mode [https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-enable-FIPS-CC-mode/ta-p/196629]

[4] Cryptographic Module Validation Program Certificate #4443 [https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4443]

[5] CP9 Capabilities [https://docs.fortinet.com/index.php/document/fortigate/7.4.4/hardware-acceleration/340357/cp9-capabilities]

with an invalid CA when connecting. Fixing this error is not a difficult matter, and is typically handled through the creation of a new DNS A record and subdomain name which points to the VPN's IP address. Usually this looks like *vpn.domain.com* or *remote.domain.com* and not only provides a reference name for the SSL certificate, but is also an easy to remember name for configuring the VPN client. Should the VPN IP change, it is a trivial matter to update the DNS A record a single time rather than update every user's VPN client. An SSL certificate confirming the domain can then be purchased from a respected CA and installed on the firewall.

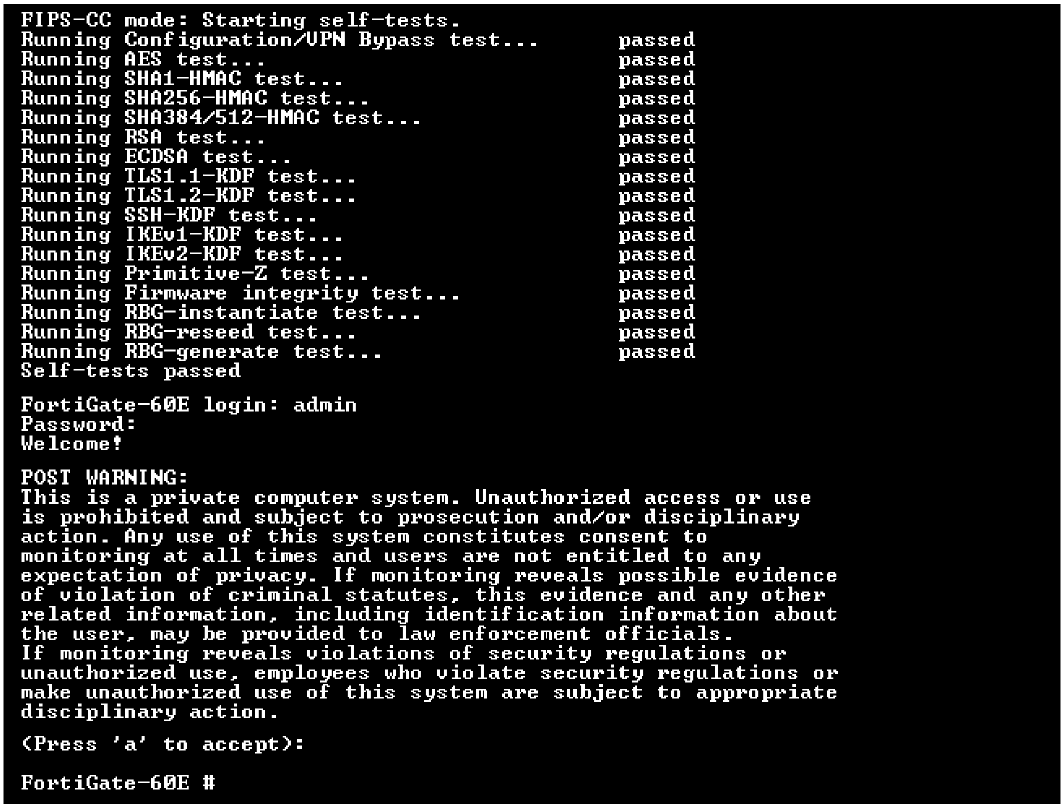
Project Proposal

In addition to my research, I was asked to compile my findings into a short report that would also serve as a project proposal to implement the control. My report was to include the project goals, my assessment, implementation steps, a time estimate, and any potential impacts of the changes to be made. Since the proposal was written before I received a response on the entropy token, it was still referenced, though later verbally confirmed that it would not be an issue. I also assumed that the patched version of the firmware would be used, despite not having a finalized answer on the subject. I suspected this will simply be a detail noted in the SSP rather than leave the system vulnerable. My two-page project proposal can be found in the appendix (see Figures B.6 and B.7).

Project Implementation

The project proposal was reviewed with the client during our weekly Friday Teams call. Due to the absence of key individuals during the final week of the six-week project period, I would primarily focus on assessing the steps required to update the firmware and enable FIPS-CC mode on a clone of the actual device on-site. Using a phased approach would allow for addressing any potential issues with the firmware update before scheduling on-site time, as the update would necessitate downtime for the entire network, likely during after-hours. The registration of a new SSL certificate would also require additional purchase authorization, but the A record was added easily only requiring 10-15 minutes.

In the time available before writing this report, I backed up the client's firewall settings and replicated them onto another device with identical specifications. After completing this step, I proceeded to update the firmware to the FIPS (pseudo) validated version, which included CVE patches, and enabled FIPS-CC mode. Enabling FIPS-CC mode necessitated connecting to the console port using a serial cable and accessing the CLI via a terminal program (PuTTY). This step alone made any potential remote update of the client's device impossible. Additionally, during the process of enabling FIPS-CC mode, I encountered a warning message that most of the device settings would be wiped, effectively negating my efforts to clone the current device settings. After updating the device it now performed additional self-checks upon boot, and presented a warning message upon login (Figure 5.2).



```
FIPS-CC mode: Starting self-tests.
Running Configuration/VPN Bypass test...      passed
Running AES test...                           passed
Running SHA1-HMAC test...                     passed
Running SHA256-HMAC test...                   passed
Running SHA384/512-HMAC test...               passed
Running RSA test...                           passed
Running ECDSA test...                         passed
Running TLS1.1-KDF test...                    passed
Running TLS1.2-KDF test...                    passed
Running SSH-KDF test...                       passed
Running IKEv1-KDF test...                     passed
Running IKEv2-KDF test...                     passed
Running Primitive-Z test...                   passed
Running Firmware integrity test...            passed
Running RBG-instantiate test...               passed
Running RBG-reseed test...                    passed
Running RBG-generate test...                  passed
Self-tests passed

FortiGate-60E login: admin
Password:
Welcome!

POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.

(Press 'a' to accept):

FortiGate-60E #
```

Figure 5.2: FortiGate FIPS-CC Mode Console

Although I was able to perform the updates to my cloned device, I did not have enough time to finalize the project before the submission of this report. My plan moving forward is to assess what settings may still remain - if any - and make note of the steps required to rebuild the configuration including interface settings, firewall policies, VPN configuration, and the advanced NGFW features. It should then be possible to bring this clone device on-site and do a direct replacement to quickly verify its functionality within the LAN. If everything appears to continue to function as normal, the client's firewall can then be upgraded and the same settings applied. It may also be prudent to have a second cloned device on-hand with all the original non-FIPS settings and configurations should there be any issues.

Chapter 6

CONCLUSIONS

After spending six weeks intensely involved with the CMMC process, I can honestly say that it is an incredibly large body of knowledge to digest in such a short period of time. Additionally, not being able to begin the project from its onset hampered my ability to gain a clear understanding of the initial steps. Since I was unable to attain an holistic view of the process from the start, I was sometimes confused when attempting to implement certain practices that seemed to require artifacts which seemed to not exist.

I believe this confusion was due to the fact that this was my company's first attempt to assist with a CMMC evaluation. With no prior assessments of this sort under our belt, I was learning along with the project leaders. However, part of my role was to identify our shortcomings and suggest improvements. My recommendation is that such a project should have a dedicated resource who has participated in *at least* one previous evaluation so they can provide insight into some of the areas we are having difficulty navigating.

I believe one of these areas in particular is the scoping process, and I suggest we spend time reviewing official and third-party scoping resources to ensure that every asset is cataloged and system boundaries are clearly defined. Properly scoping the environment makes it easier to address potential issues and helps avoid the possibility for fundamental changes occurring later in the process. Additionally, many practices apply to every in-scope asset, and will need to be reassessed if something is missing. Having a better method for determining where we are in the process, better organization of artifacts, and guidelines on how the project is being implemented is another suggestion. Investing in a tool such as *FutureFeed* to help organize and direct the process may be a solution to address these items.

Overall, this project has certainly been more difficult than I originally expected and has shown me another side of cybersecurity which is of great importance. As we approach the deadline for the final CMMC implementation, more and more organizations will be seeking help from those who have previously navigated the process to avoid common pitfalls. Having the process refined will allow us to best assist them in their CMMC journey.

Appendix A

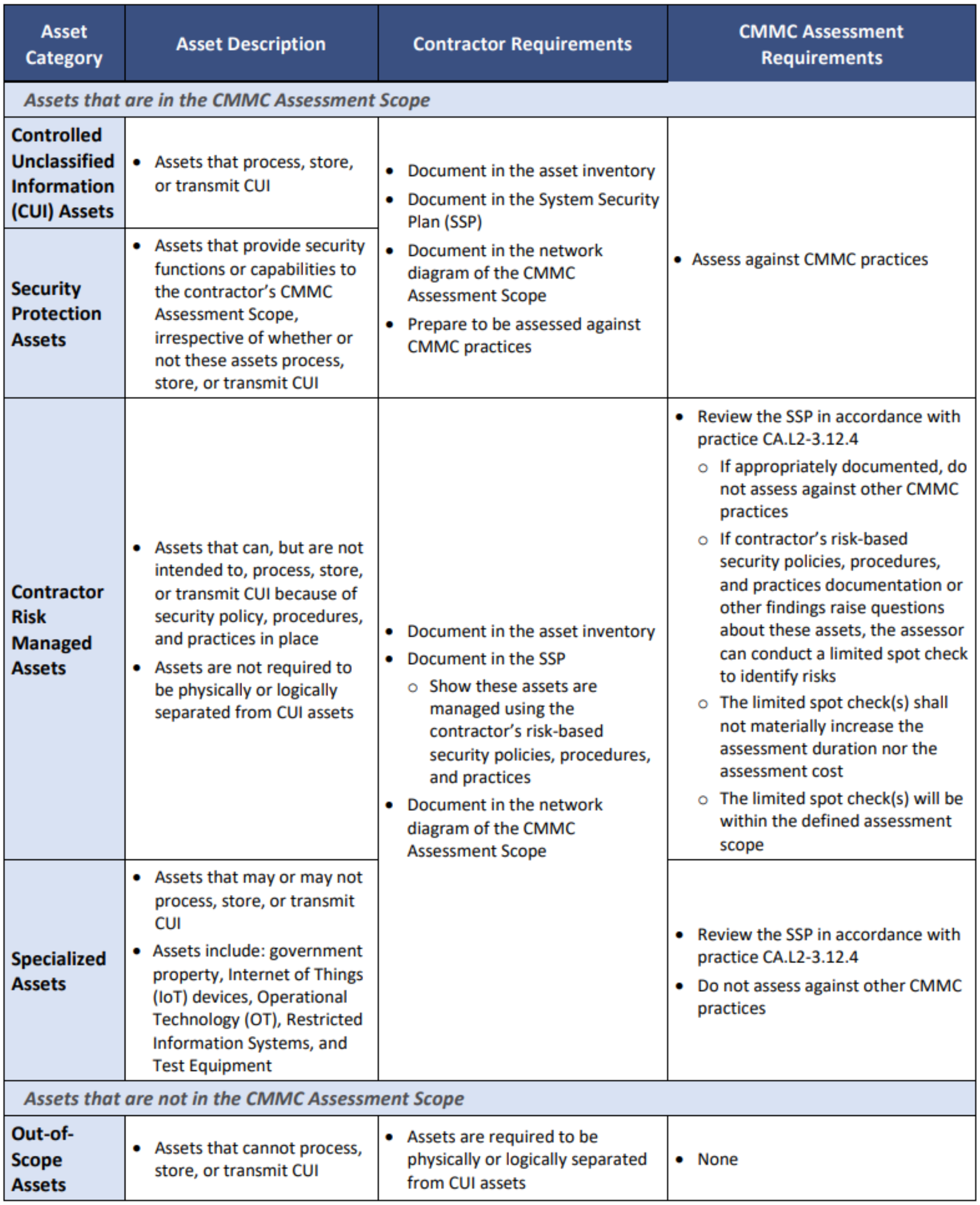
ACRONYMS

Acronym	Definition
AO	Assessment Objectives
APT	Advanced Persistent Threats
ATP	Advanced Threat Protection
C3PAO	Certified Third-Party Assessor Organization
CA	Certificate Authority
CDI	Covered Defense Information
CFR	Code of Federal Regulations
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CMVP	Cryptographic Module Validation Program
CRMA	Contractor Risk Managed Asset
CSET	Cybersecurity Evaluation Tool
CSP	Cloud Service Providers
CUI	Controlled Unclassified Information
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DFD	Data Flow Diagram
DHC	Device Health Check
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoD	US Department of Defense
EDR	Endpoint Detection and Response
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
MFA	Multi-Factor Authentication
MSP	Managed Service Provider

NAC	Network Access Control
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
OSC	Organization Seeking Certification
POA&M	Plan of Action and Milestones
RMM	Remote Monitoring and Management
SA	Specialized Asset
SPA	Security Protection Asset
SPRS	Supplier Performance Risk System
SSP	System Security Plan
ZTNA	Zero Trust Network Access

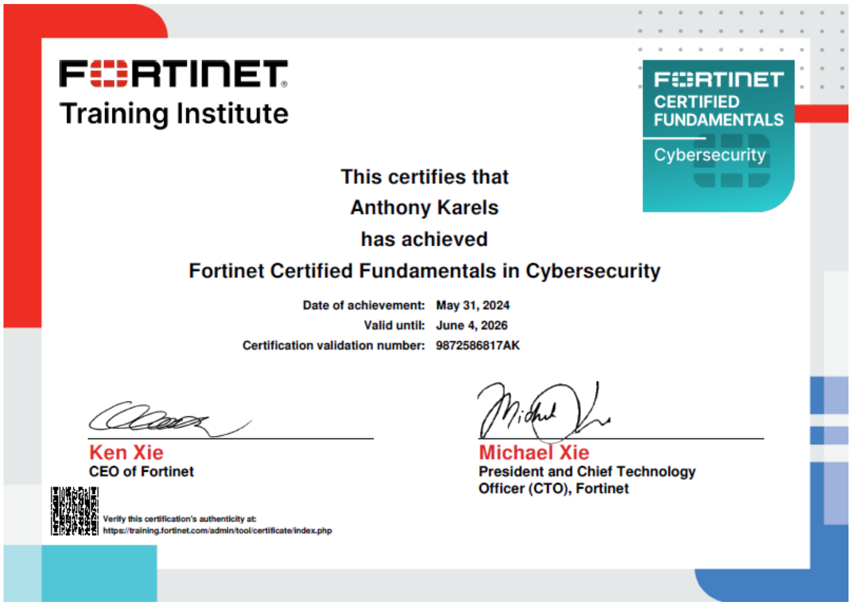
Appendix B

ADDITIONAL FIGURES



Asset Category	Asset Description	Contractor Requirements	CMMC Assessment Requirements
Assets that are in the CMMC Assessment Scope			
Controlled Unclassified Information (CUI) Assets	• Assets that process, store, or transmit CUI	• Document in the asset inventory • Document in the System Security Plan (SSP) • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC practices	• Assess against CMMC practices
Security Protection Assets	• Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI		
Contractor Risk Managed Assets	• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place • Assets are not required to be physically or logically separated from CUI assets	• Document in the asset inventory • Document in the SSP ○ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices • Document in the network diagram of the CMMC Assessment Scope	• Review the SSP in accordance with practice CA.L2-3.12.4 ○ If appropriately documented, do not assess against other CMMC practices ○ If contractor's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited spot check to identify risks ○ The limited spot check(s) shall not materially increase the assessment duration nor the assessment cost ○ The limited spot check(s) will be within the defined assessment scope
Specialized Assets	• Assets that may or may not process, store, or transmit CUI • Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment		• Review the SSP in accordance with practice CA.L2-3.12.4 • Do not assess against other CMMC practices
Assets that are not in the CMMC Assessment Scope			
Out-of-Scope Assets	• Assets that cannot process, store, or transmit CUI	• Assets are required to be physically or logically separated from CUI assets	• None

Figure B.1: CMMC Asset Categories [Department of Defense, 2021, p. 2]



FORTINET
Training Institute

FORTINET
CERTIFIED
FUNDAMENTALS
Cybersecurity

This certifies that
Anthony Karels
has achieved
Fortinet Certified Fundamentals in Cybersecurity

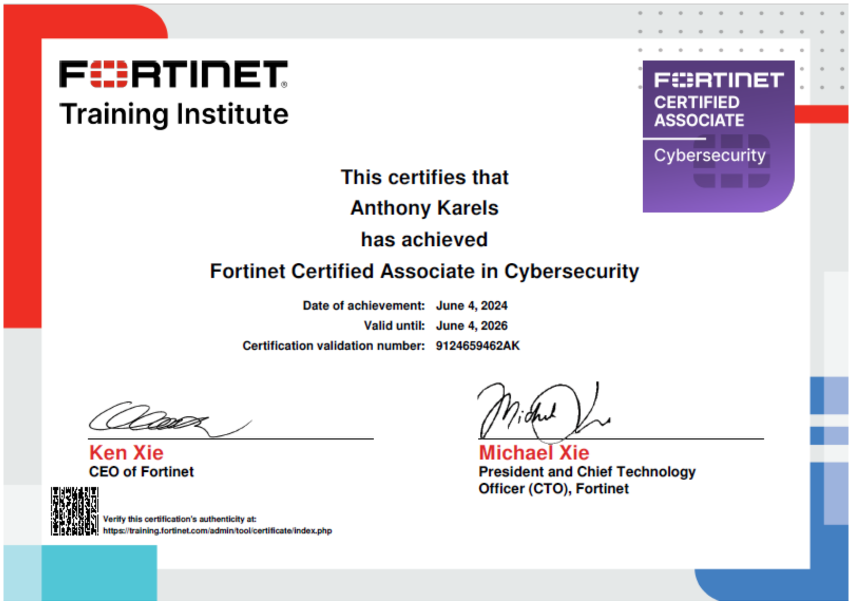
Date of achievement:	May 31, 2024
Valid until:	June 4, 2026
Certification validation number:	9872586817AK

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

Figure B.2: Fortinet Certified Fundamentals (FCF) Certificate



FORTINET
Training Institute

FORTINET
CERTIFIED
ASSOCIATE
Cybersecurity

This certifies that
Anthony Karels
has achieved
Fortinet Certified Associate in Cybersecurity

Date of achievement:	June 4, 2024
Valid until:	June 4, 2026
Certification validation number:	9124659462AK

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet

Verify this certification's authenticity at:
https://training.fortinet.com/admin/tool/certificate/index.php

Figure B.3: Fortinet Certified Associate (FCA) Certificate

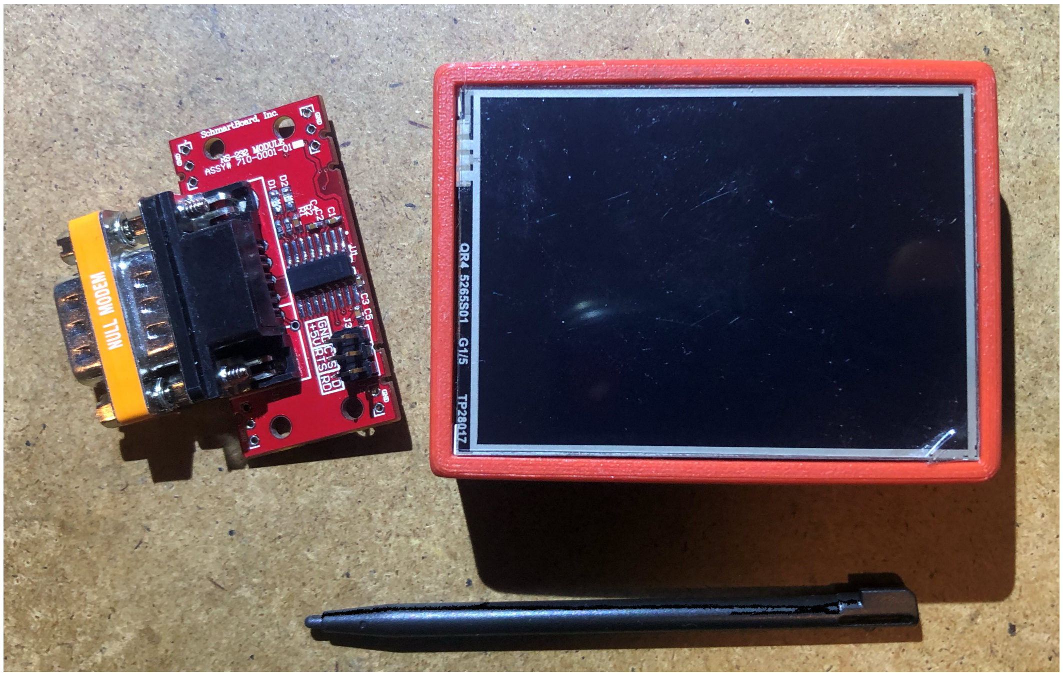


Figure B.4: Raspberry Pi Pico Based "FortiProgrammer" Device

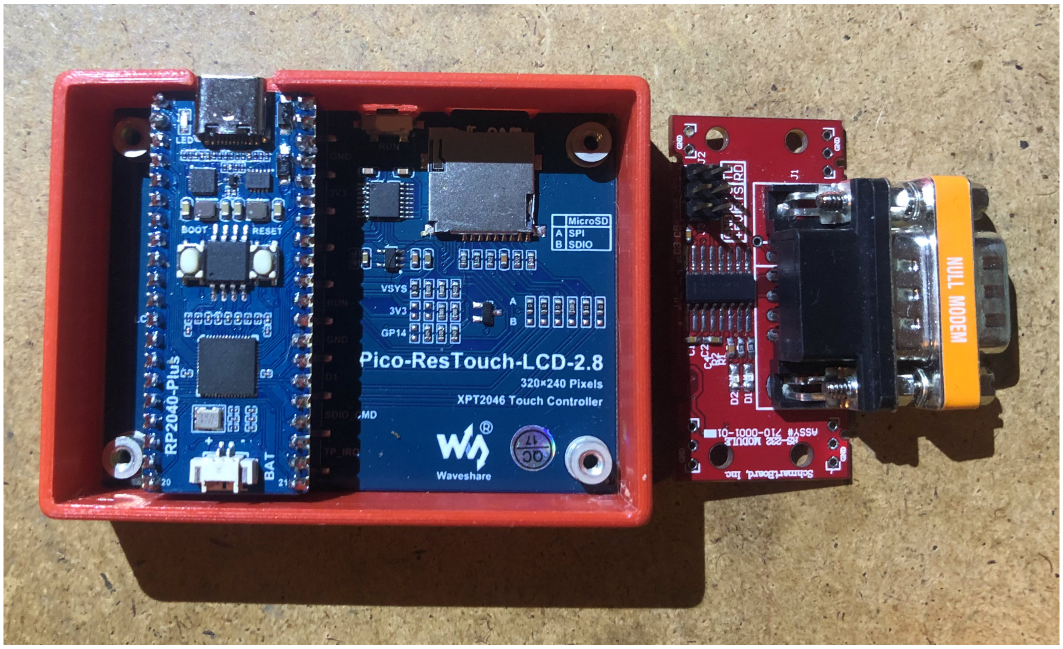
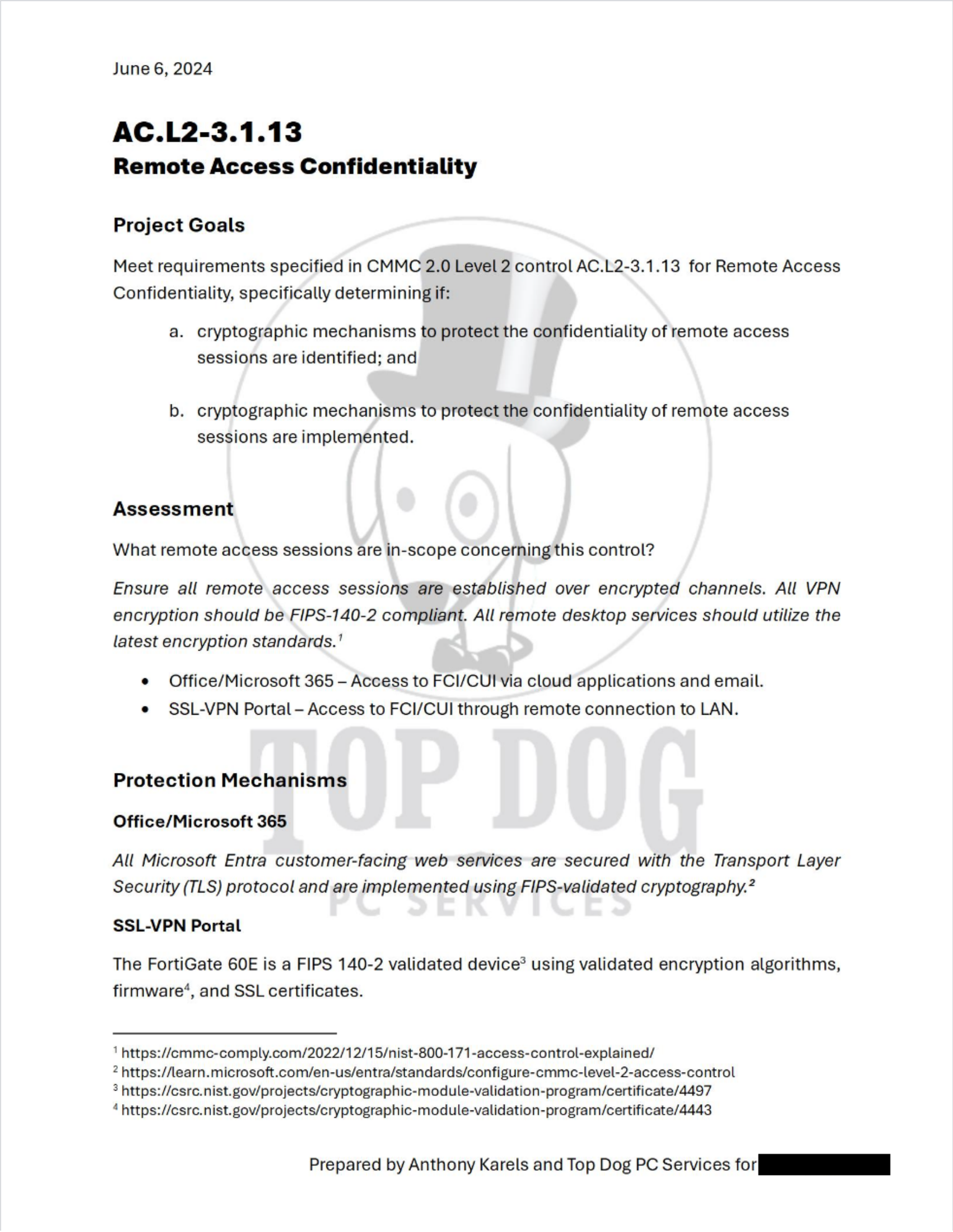


Figure B.5: Component View of "FortiProgrammer" Device



June 6, 2024

AC.L2-3.1.13
Remote Access Confidentiality

Project Goals

Meet requirements specified in CMMC 2.0 Level 2 control AC.L2-3.1.13 for Remote Access Confidentiality, specifically determining if:

a. cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and

b. cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

Assessment

What remote access sessions are in-scope concerning this control?

Ensure all remote access sessions are established over encrypted channels. All VPN encryption should be FIPS-140-2 compliant. All remote desktop services should utilize the latest encryption standards.[1]

- Office/Microsoft 365 – Access to FCI/CUI via cloud applications and email.
- SSL-VPN Portal – Access to FCI/CUI through remote connection to LAN.

Protection Mechanisms

Office/Microsoft 365

All Microsoft Entra customer-facing web services are secured with the Transport Layer Security (TLS) protocol and are implemented using FIPS-validated cryptography.[2]

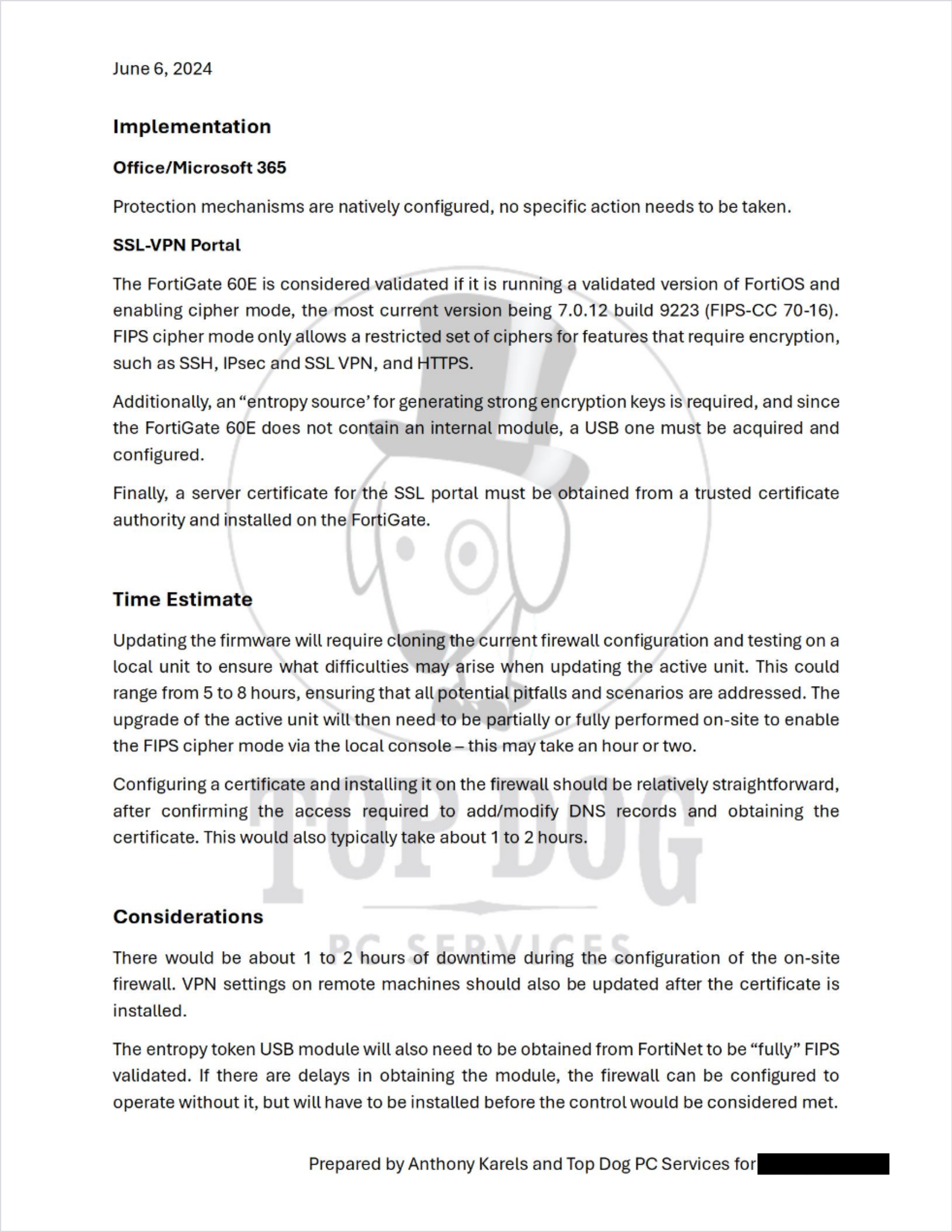
SSL-VPN Portal

The FortiGate 60E is a FIPS 140-2 validated device[3] using validated encryption algorithms, firmware[4], and SSL certificates.

[1] https://cmmc-comply.com/2022/12/15/nist-800-171-access-control-explained/
[2] https://learn.microsoft.com/en-us/entra/standards/configure-cmmc-level-2-access-control
[3] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4497
[4] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4443

Prepared by Anthony Karels and Top Dog PC Services for [redacted]

Figure B.6: AC.L2.3.1.13 Project Proposal (pg.1)



June 6, 2024

Implementation

Office/Microsoft 365

Protection mechanisms are natively configured, no specific action needs to be taken.

SSL-VPN Portal

The FortiGate 60E is considered validated if it is running a validated version of FortiOS and enabling cipher mode, the most current version being 7.0.12 build 9223 (FIPS-CC 70-16). FIPS cipher mode only allows a restricted set of ciphers for features that require encryption, such as SSH, IPsec and SSL VPN, and HTTPS.

Additionally, an “entropy source’ for generating strong encryption keys is required, and since the FortiGate 60E does not contain an internal module, a USB one must be acquired and configured.

Finally, a server certificate for the SSL portal must be obtained from a trusted certificate authority and installed on the FortiGate.

Time Estimate

Updating the firmware will require cloning the current firewall configuration and testing on a local unit to ensure what difficulties may arise when updating the active unit. This could range from 5 to 8 hours, ensuring that all potential pitfalls and scenarios are addressed. The upgrade of the active unit will then need to be partially or fully performed on-site to enable the FIPS cipher mode via the local console – this may take an hour or two.

Configuring a certificate and installing it on the firewall should be relatively straightforward, after confirming the access required to add/modify DNS records and obtaining the certificate. This would also typically take about 1 to 2 hours.

Considerations

There would be about 1 to 2 hours of downtime during the configuration of the on-site firewall. VPN settings on remote machines should also be updated after the certificate is installed.

The entropy token USB module will also need to be obtained from FortiNet to be “fully” FIPS validated. If there are delays in obtaining the module, the firewall can be configured to operate without it, but will have to be installed before the control would be considered met.

Prepared by Anthony Karels and Top Dog PC Services for [redacted]

Figure B.7: AC.L2.3.1.13 Project Proposal (pg.2)

BIBLIOGRAPHY

32 CFR § 2002.4 (Sept. 2016). *Controlled Unclassified Information*. URL: https://www.govinfo.gov/content/pkg/CFR-2023-title32-vol6/pdf/CFR-2023-title32-vol6-sec2002-4.pdf.

48 CFR § 52.204-21 (May 2016). *Basic Safeguarding of Covered Contractor Information Systems*. as amended at 86 FR 61032, Nov. 4, 2021. URL: https://www.govinfo.gov/content/pkg/CFR-2023-title48-vol2/pdf/CFR-2023-title48-vol2-sec52-204-21.pdf.

Army Multimedia and Visual Information Division (Feb. 2024). *Cybersecurity Maturity Model Certification (CMMC) Proposed Rule Overview*. Video. Duration: 40:40. URL: https://www.defense.gov/Multimedia/Videos/videoid/912871/.

Department of Defense (Dec. 2021). *DoD CMMC Assessment Scope Level 2 Version 2.0*. URL: https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf.

– (Nov. 2023). *DoD CMMC Assessment Guide Level 2 Version 2.11 - DRAFT*. DoD-CIO-00003 (ZRIN 0790-ZA19). URL: https://www.regulations.gov/document/DOD-2023-OS-0096-0005.

DoD, US (2021). *Key Features of CMMC 2.0*. Figure. URL: https://dodcio.defense.gov/CMMC/About/.

HITECH Secure, Inc. (2023). *A Guide to CMMC Readiness*. Figure. URL: https://topdogpc.com/getting-started-with-cmmc-certification/.

Hive Systems (2024). *The Race to CMMC Compliance*. Figure. URL: https://www.hivesystems.com/blog/racetocmmccompliance.

NIST (2002). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*. Updated Version 2.0.1, December 3, 2002. URL: https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

– (June 2018). *NIST Special Publication 800-171A*. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf.

– (Jan. 2021). *NIST Special Publication 800-171 Revision 2*. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

Obama, Barack (Nov. 2010). *Executive Order 13556: Controlled Unclassified Information*. Federal Register. Signed November 4, 2010. URL: https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information.

Peak InfoSec (2022). *Debunking CMMC Assessment Scope Myths*. Figure. URL: https://peakinfosec.com/whitepapers/white-paper-debunking-cmmc-assessment-scope-myths/.