A CMMC Application Analysis Example

By: Gerald Rigdon - 2023

As an electrical contractor providing services to the Quantico military base, Neighbor Electric Services (NES), has been notified that the Department of Defense (DoD) has determined NES to be a cybersecurity risk. Since 2020, the DoD has used the Cybersecurity Maturity Model Certification, or CMMC, to qualify contractors providing services to operations under the authority of the DoD. Under the current revision, or CMMC Revision 2.0 (*About CMMC*, 2023), the DoD has specified a tiered approach to certification defined by three levels of maturity as follows:

1. Level1 – 15 basic cyber hygiene practices
2. Level2 – Demonstration of compliance with 110 requirements from NIST SP 800-171 in addition to Level1
3. Level3 – Demonstration of compliance with a subset of NIST SP 800-172 in addition to Level1 and Level2

For NES, the first step in this compliance journey will require company alignment with the basic cybersecurity practices of Level1 (*CMMC Self-Assessment Guide*, 2021) considering the following computer system discoveries of NES digital operations:

- The existence of the server in Lorton which stores sensitive Quantico military base information consisting of blueprints, clearance paperwork, employee information, and project data including timesheets and tracking status.
- Remote access to Lorton computer systems enabling employees to work from home.
- Network and computer system administration by personnel lacking cybersecurity training.

As stated in the CMMC documentation, (*CMMC Self-Assessment Guide*, 2021), this self-assessment process will include interviews with NES staff, reviews of company documents, policies, and testing to generate the findings for evaluation. Given the initial discoveries outlined above, your Access Control policies, and their associated enforcement mechanisms, will be a critical input to this assessment process. Moreover, NES will need to demonstrate its capabilities to identify, authenticate, and remediate when necessary to ensure the confidentiality, integrity, availability, and safety of digital information.

Compliance with Level1 demonstrates cybersecurity awareness and an understanding of the importance of Risk Management. While a degree of uncertainty will always exist, the identification, analysis, and execution of mitigation strategies are necessary for effective security outcomes. Part of the risk management process is understanding residual risk that remains post-mitigation and an analysis of why it is acceptable. Excellent guides to risk management including both general and cybersecurity specific frameworks are available through the National Institute of Standards and Technology (*Risk Management*, 2023).

Following industry best practices, NES should perform a threat modelling exercise (Shostack, 2021) to examine existing operations while considering the following questions:

- What can go wrong? What are we going to do about it? How did we do?

This important exercise makes use of both visual and textual techniques that facilitate a better understanding of existing data flows and where vulnerabilities may exist. This will give rise to more specific questions as NES contemplates basic concerns such as:

- Is a Virtual Private Network used when remotely connecting to the Lorton server?
- What is the password strength, are passwords rotated, and is multifactor authentication employed? Is the principle of least privilege followed?
- Do we have an incident response plan? What is our employee training program for cybersecurity awareness? What training has our network administrator received?

Following the completion of the Level1 self-assessment, there will be a re-evaluation of NES services to determine whether compliance with Level2 or Level3 requirements are to be implemented given the contracted services performed for the Quantico military base and upcoming bids for future contracts. Considering the nature of existing services, NES can anticipate the necessity for at least Level2 per (*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, 2020).

Given the small size of your company (approximately sixty employees), the streamlined CMMC framework is intended to provide clearly defined actionable items to achieve and maintain higher levels of certification as needed. With a Plan of Actions and Milestones it may be possible for NES to be awarded a future contract while actively working toward full Level2 compliance (*CMMC Implementation*, 2023). Please review the references provided below to begin the process toward certification.

References:

About CMMC. (2023, September). Dodcio.defense.gov. https://dodcio.defense.gov/CMMC/about/

CMMC Implementation. (2023, September). Dodcio.defense.gov. https://dodcio.defense.gov/CMMC/Implementation/

CMMC Self-Assessment Guide. (2021, December). Dodcio.defense.gov. https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (2020, February). Dodcio.defense.gov. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Risk Management (n.d.). nist.gov. https://www.nist.gov/risk-management

Shostack, A. (2021, September). *What can go wrong?* https://shostack.org/blog/what-can-go-wrong/