The Impact of NIST SP 800-171 and CMMC 2.0 on Small and Medium Businesses

Zoë Medina

Professor Templeton

CYBR 503- Cybersecurity Domain

Shiley-Marcos School of Engineering (SMSE), University of San Diego

Table of Contents

Introduction

Before deciding how to approach security for a company, it is important to understand the different frameworks associated with federal contracts. NIST SP 800-171 is a framework created by the National Institute of Standards and Technology that consists of security controls to help organizations evaluate their security posture and bolster it if needed. These security controls are divided into 17 different families that expand across a numerous amount of cybersecurity domains such as access controls, identity management, audits, and risk assessments. This framework was originally created for federal agencies to have standardized security requirements in order to protect the confidentiality of governmental data. It is also a way for the government to ensure that non-federal organizations that are involved with government affairs and data have the same standard of security to ensure confidentiality. Over time, many organizations began to use this framework as a starting point for their own security requirements and as a guideline for protecting their own data.

The Cybersecurity Maturity Model Certification 2.0 or CMMC 2.0 is a certification framework designed by the U.S. Department of Defense to determine the level of security of an organization. This framework is divided into three levels, which correlate to how many security controls that organization has met from the NIST SP 800-171 and from the CMMC 2.0. Level 1 of the CMMC 2.0 is the most basic tier that an organization can reach. This level requires that an organization meets 17 of the 110 security controls laid out by the NIST SP 800-171 and conducts self-assessments annually. In return, an organization may take contracts from the federal government that do not contain critical information. Level 2 of the CMMC 2.0 is the middle tier of the certification model. This level requires that an organization meets 110 of the 110 security controls published in the NIST SP 800-171 and has assessments conducted by a third-party every three years. In return, an organization may take contracts from the federal government that contains critical information. Level 3 of the CMMC 2.0 is the final tier that an organization can reach. This level requires that all security controls of the NIST SP 800-171 are met as well as 20+ additional security controls laid out by the CMMC 2.0 and that assessments are completed by the government every three years. In return, an organization may take contracts that contain national security level information. At the time of writing, this level is still being fleshed out by the US Department of Defense.

Compare and Contrast

From a surface level, the NIST SP 800-171 and the CMMC 2.0 are very similar. The main similarity between the two is their focus on protecting sensitive information by maintaining the confidentiality, integrity, and availability of data. Both frameworks are based on a set of security controls that professionals in the cybersecurity field have deemed best practice for each of the cybersecurity domains. They both require that organizations have some sort of assessment completed on their security posture in order to test the strength and thoroughness of their security controls. Furthermore, they both outline the security roles needed in a company that security personnel need to fill and how these roles collaborate with one another. Finally, both frameworks require that an organization establishes plans and procedures in the event of a security breach and for day-to-day monitoring.

When examining the two frameworks more carefully, there is much nuisance that makes them quite different. Firstly, while the frameworks are focused on increasing security to protect sensitive data, they were created for different demographics. The NIST SP 800-171 was created as a set of security controls to serve non-federal organizations while the CMMC 2.0 was meant to assess the maturity of an organization's security in order to determine if they are fit to work with the federal government. Therefore, the CMMC 2.0 is stricter when it comes to fulfilling the security controls and passing the security assessments. Secondly, the NIST SP 800-171 does not award an organization with a certification when a certain amount of security controls are meant like the CMMC 2.0 does. This is because the NIST SP 800-171 is more of a set of guidelines for companies to follow if they do not already have a cybersecurity plan in place while the CMMC 2.0 is a security program that companies must complete if they want to obtain federal contracts. Thirdly, because the NIST SP 800-171 is a non-formal framework, there is no requirement for a third-party security assessment. NIST SP 800-171 allows for an organization to complete a self-assessment to identify their security weaknesses while the CMMC 2.0 will require a third-party or government-led security requirement passed level 2 of the maturity model, which must be performed by a CMMC Third Party Assessor Organization or C3PAO. Finally, there is a difference when it comes to the allowance of Plan of Action and Milestones or POA&M, which is a plan for how an organization is going to remedy a vulnerability uncovered during an assessment. Typically, an organization must meet all necessary security requirements before they can be certificated. However, a POA&M allows an organization to submit a plan of action for meeting a security requirement and still receive their certification. Because the NIST SP 800-171 is a non-formal framework, it does not have a limitation on the number of POA&Ms that an organization can have active while the CMMC 2.0 does have a limitation.

Impact and Implications

The CMMC 2.0 is looking to be the main framework for obtaining federal contracts going forward. Therefore, it is important for organizations to start familiarizing themselves with the process of getting certified, especially small and medium sized businesses who rely on federal contracts. It is estimated that the process of being CMMC 2.0 certified can take up to several months, which will only take longer for smaller companies that have limited resources to put towards their security posture. Getting a jumpstart on obtaining level 1 of the maturity model would put a company in the best position to continue to work with federal contracts once the CMMC 2.0 certification becomes a requirement. The NIST SP 800-171 has less of an impact on organizations moving forward since many already rely on it for security guidance. Now, the NIST SP 800-171 security controls will be a requirement for anyone looking to obtain federal contracts since the CMMC 2.0 relies and builds upon those security controls. With the enforcement of the CMMC 2.0, the government can ensure that all organizations within its supply chain are being held to the same security standards and are actually maintaining compliance. In terms of the public, a uniform set of security standards and organizations being forced to meet them ensures that personal sensitive data remains confidential. In the long-term, these frameworks give the federal government more confidence in the organizations it is trusting its critical information to through its contracts. This will help bolster the overall security of our national cyber space and help keep government information safe. Over time, organizations will become more familiar with the certification process and it will become easier for smaller businesses to compete for those federal contracts. In addition, companies that are not involved with the government can still look to this framework to strengthen their own security to the level that is deemed appropriate for critical information.

Conclusion

In conclusion, the development of the CMMC 2.0 is important within the cybersecurity space. Its creation has established a standardized program for companies to base their compliance around, with the addition of a credible certification for reaching compliance. Its layed maturity model grants flexibility for small and medium companies to still obtain lower level federal contracts through the lowest level requirements while the company continues to bolster its security posture to meet those higher level requirements. This means that companies are punished for not having the same amount of resources and man-power to compete with larger companies. Periodic security assessments completed by certified third-parties reduces the chances of a company lying about their compliance status with the NIST SP 800-171 framework and instills confidence in the Department of Defense's supply chain. Due to the popularity and potential of the CMMC 2.0, it is unlikely that it will be replaced anytime soon and is therefore a framework worth investing in for companies both involved and not involved in federal contracts.

References

CMMC 2.0 and its impact on government contractors. iQuasar LLC. (2022, February 4). https://iquasar.com/blog/cmmc-2-0-and-its-impact-on-government-contractors/

CMMC vs NIST 800 171 compliance: What is the difference?. Hyper Vigilance. (2023, May 7). https://hypervigilance.com/types-of-compliance/cmmc-vs-nist-800-171/

Knight, A. (2023, May 15). *What are the implications of CMMC in 2023? I ciat.edu*. California Institute of Arts & Technology. https://www.ciat.edu/blog/implications-of-cmmc/

Mistry, A. (2023, August 17). *CMMC vs NIST 800-171: Key similarities and differences*. Cloud-Based File Transfer Software. https://www.sharetru.com/blog/cmmc-vs-nist-800-171-key-similarities-and-differences

Strategic direction for cybersecurity maturity model certification (CMMC) program. U.S. Department of Defense. (2021, November 4). https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/