Welcome to CMMC 2.0!
February 2023

What Is the CMMC 2.0?

- The CMMC is the Cybersecurity Maturity Model Certification.
- This is the Department of Defense's (DoD) response to having the Defense Industrial Base (DIB) in the U.S. continuously hacked!
- In the past we could all self-attest to good cybersecurity practices but not any more! Now most of us have to get certified!

What Are the Changes in CMMC 2.0?

- First thing's first…. CMMC 2.0 is still not 100% ready but it's going live in May 2023 with two phases (aka some of this could be subject to change so make sure to check back)
- The Levels of CMMC attestation have changed. There are now 3 levels.
- Under "certain limited circumstances" you may now be able to become certified without having all controls in place (aka Plan of Action and Milestones also known as POA&Ms.)
- Waivers from the DoD can also be issued "under limited circumstances."
- There are now incentives for companies who voluntarily go through third party assessments though those incentives haven't been fully explained yet.
- Basically, CMMC 2.0 is a bit more flexible but still stringent.

Is The CMMC Required for My Business?

- Yes, if you wish to do business with the DoD or many of their contractors.
- Without a certification (or possibly self-attestation), most DoD Contracts will not be available to you thus limiting your potential revenue from these types of contracts.
- As most businesses are actually subcontractors in the DoD supply chain, this could also be potentially harmful to your existing relationships with DoD CMMC certified contractors who are required to use CMMC certified subcontractors for DoD work.

What Level of CMMC Certification is Right For My Business?

- As mentioned before, there are three levels of certification.
- As most businesses are subcontractors to Prime Contractors, the goal of your business is to be able to handle and secure the Controlled Unclassified Information (CUI) that is given to you by the prime.
- In order to handle CUI and be available for the majority of DoD contracts, as a subcontractor, the required CMMC certification is **Level 2** and should be the target of your business.
- Polling of the Defense Industrial Base shows that over 90% of businesses will achieve a Level 2 certification.

How Much Does a CMMC Implementation Cost?

- As each business is different there is no set cost but how we typically calculate an estimate takes into account the following factors (plus others):
    - The size of the organization (the more employees the more cost for hardware, software etc).
    - The current defensive posture of the organization. For example, if a company has 90% of the controls already in place their cost is much less than a company with only 20%.
- Costs can range from $20,000 to $200,000 or more depending on the above factors, as well as others. (This doesn't cover the official certification assessment or internal assessments prior to the official.)
- Expect this cost to be spread out between multiple fiscal quarters but no more than two years.
    - The heaviest costs tend to be in hardware and software as well as policy writing, which is a CMMC requirement. Also, labor for implementation as well can be costly.
- Outside of this cost would be the initial cybersecurity assessment to get your CMMC project started. Those can range from $15,000 - $40,000 or more for most businesses.

Given These Potential Costs, Should My Company Stop Working with The Dept. of Defense?

- There are multiple factors to consider when choosing to give up this source of revenue. Some things to consider:
    - The growth strategy of your company. If you were planning to expand into DoD work or grow other business with general or prime contractors, then a CMMC certification may be worth it.
    - You have the potential to lose "favored" status with your general or prime contractors. These large contractors will find it's easier to simply use a CMMC certified subcontractor for all kinds of work since they are flexible enough to do it.
    - A CMMC certification also gives you an edge in marketing and sales!
- Honestly, CMMC certification isn't for every company but giving up a revenue stream shouldn't be taken lightly!

My Company Works with Other Gov't Agencies but Not the DoD. Should We Care About The CMMC?

- Yes! While the CMMC was created for the DoD, it's now being adopted by other agencies such as the Department of Homeland Security.
- The Cybersecurity community predicts that the U.S. Government will actually accelerate the adoption of the CMMC into other agencies and departments within the next decade which would then make it a requirement for contractors and subcontractors outside of the DoD Supply Chain.
- State, county and municipal governments are also expected to adopt and force cybersecurity standards on their local contractors within the next decade as well. Small government is a serious and growing target that is being addressed.

I Partially Subcontract Out My DoD Work to Other Subcontractors. How Does This Affect Me?

- CMMC is required for any entity that will handle Controlled Unclassified Information (CUI) as part of their contract.
- Your subcontractors, if they are handling the CUI your business was issued by another contractor, also need a CMMC Level 2 certification as well.

- This affects the entire DoD Supply Chain so if your subcontractors decide to subcontract part of their work out, those sub-subcontractors need CMMC Level 2 certification.
- Any 1099 workers that will handle CUI need to go through your company's CMMC approved Cybersecurity Awareness Training too.

My Computer Network Is a Hybrid On-Premise and Cloud. What Do I Need to Know About for This Situation?

- The standards for handling Controlled Unclassified Information (CUI) are agnostic to the platforms you use, meaning all platforms in use must adhere to CMMC standards for your business to obtain certification.
- Example: The server(s) in your office must meet encryption, logging, threat detection and other standards before it can be certified for CMMC use.
- Example: Your company is using a third-party database provider into the cloud to store CUI. They must be able to prove they are a FedRAMP Moderate certified Cloud Service Provider (CSP) under their own corresponding standard (known as DFARS 252.204-7012.)
- Your cloud providers may have a "Government" option for your business to migrate to in order to make it easier to comply!

How Do I Start with the CMMC!?

- First things first, make sure to register yourself with the federal government as a DIB corporation via the Supplier Performance Risk System or SPRS.
- Go through a NIST 800-171 overview assessment to understand where you are in relation to achieving the Level 2 certification.
- Begin planning for those changes and upgrades. Remember, ideally keep this project under 8 fiscal quarters or 2 years.

On The Cybersecurity Side, What Are Some Things We Should Look Out For?

- Remember that no matter where your CUI data resides it has been secured to the CMMC standard which means implementing encryption, logging, permissions, monitoring and more!
- Your company will have to migrate to FedRAMP Moderate/DFARS 7012 compliant cloud solutions. (ex. Office 365 needs to move to Microsoft's GCC version of Azure)
- Due to cost and complexity, you can also consider creating an Enclave Solution, which segments off the CMMC compliant technology from the rest of your infrastructure.

Core CMMC Cybersecurity Tools

- Role Based Awareness Training for ALL employees
- Multiple types of backups!
- Next Generation Firewalls
- Endpoint Detection Response platforms
- Cloud based Spam Filtering
- Identity Management
- Digital Rights Management (DRM) / Data Loss Prevention (DLP)
- Good network control policies like passwords, PowerShell, access, MFA etc

- Live Security Monitoring, Remote Managed Monitoring, Mobile Device Management, Dark Web Monitoring
- Contingency Planning along with an Information Security Policy with supplemental policies and procedures
- Compliance Management Platform for organization of documentation and evidence of CMMC controls

About Nick Espinosa

Chief Security Fanatic at Security Fanatics

An expert in cybersecurity and network infrastructure, Nick Espinosa has consulted with clients ranging from small businesses up to the Fortune 100 level for decades. Nick founded Windy City Networks, Inc in 1998 at age 19 and was acquired in 2013. In 2015 Security Fanatics, a Cybersecurity/Cyberwarfare outfit dedicated to designing custom Cyberdefense strategies for medium to enterprise corporations, was launched. A internationally recognized speaker, member of the Forbes Technology Council, TEDx Speaker, strategic advisor to humanID, regular columnist for Forbes, award winning co-author of a bestselling book "Easy Prey", host of "The Deep Dive" nationally syndicated radio show, on the Board of Advisors for Roosevelt University's College of Arts and Sciences as well as their Center for Cyber and Information Security, the President of The Foundation for a Human Internet and is the Official Spokesperson for the COVID-19 Cyber Threat Coalition. Nick is known as an industry thought leader and sought after for his advice on the future of technology and how it will impact every day businesses and consumers.

Keep Up with the latest in Cybersecurity at:

https://twitter.com/NickAEsp
https://www.facebook.com/securityfanatics
https://www.linkedin.com/company/securityfanatics
http://www.securityfanatics.com