GUIDANCE FOR THE CYBERSECURITY MATURITY MODEL CERTIFICATION

Learn about the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) and why it may be the key to securing our nation's critical systems and intellectual property.

OVERVIEW

In January 2020, the Department of Defense (DoD) unveiled version 1.0 of the Cybersecurity Maturity Model Certification (CMMC). The CMMC provides a consistent cyber framework for vendors doing business with the DoD, and it will require a attestation and certification by a third-party assessor.

In this guide, NCC Group, a global expert in cyber security and risk mitigation, provides insight into the CMMC and offers guidance for the nearly 300,000 companies that will need to demonstrate compliance in order to conduct business with the DoD.

THE DOD RESPONDS TO ITS MOST PERSISTENT THREAT

According to the Commission on the Theft of American Intellectual Property, the value of US trade secrets stolen by outside entities lies somewhere between $180 - $540 billion per year, amassing nearly 3% of the total economic output of the United States.[1]

“The theft of hundreds of billions of dollars of intellectual property (IP) due to malicious cyber activity threatens the U.S. economy and national security.” These words, used by the Department of Defense (DoD) in an early version of the Cybersecurity Maturity Model Certification, highlight the pervasive issue of data loss within the Federal Government and its many levels of supply chain partners.

But what is the CMMC, how can it put a stop to this tremendous loss, and how will it apply to the many contractors that do business with the DoD?

[1] http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

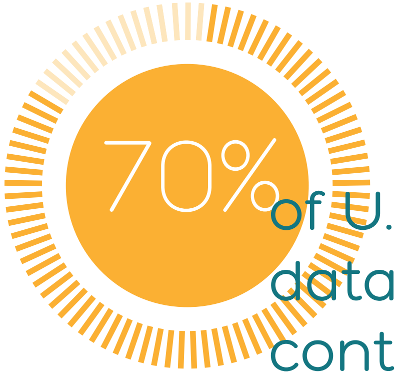
$180 - $540
billion dollars
per year value of U.S. trade secrets stolen by outside entities

WEAKNESSES IN THE GOVERNMENT'S SUPPLY CHAIN

Historically, Government networks have been protected by network segmentation and access control. However, new technologies enable information to be quickly and widely disseminated between the Government and its partners.

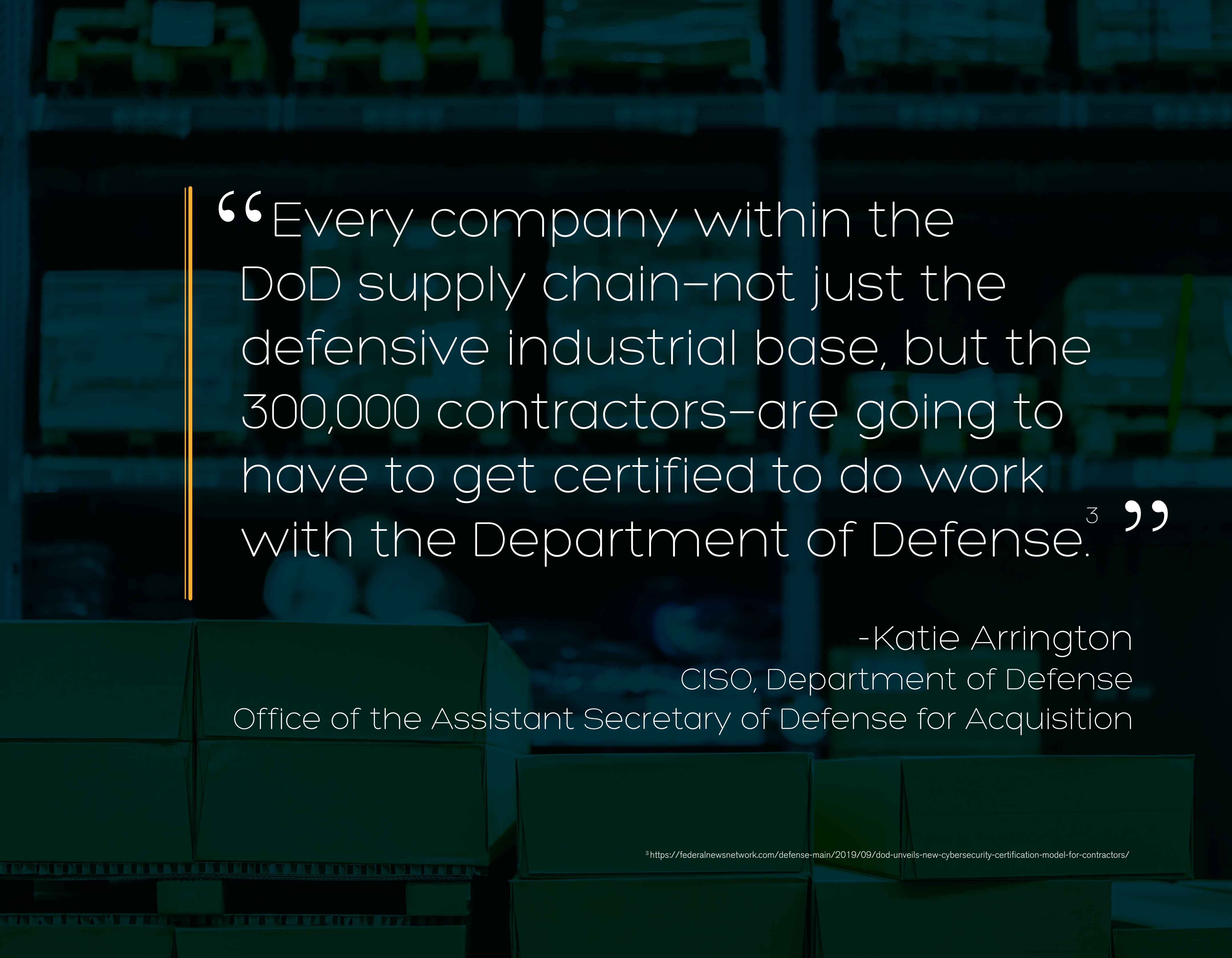
While the DoD has been held to the highest security standards, weaknesses exist within smaller organizations, much further down the supply chain, that connect to Agency environments and share and maintain critical information with the US Government. These contractors often do not have the necessary security maturity and infrastructure in place, and are a prime target for nation states and other threat actors.

To protect the government's sensitive, unclassified information against data exfiltration, new cyber risk standards were created and applied to contracts issued by the DoD, whose primary focus was to protect Controlled Unclassified Information (CUI), information not considered classified but that requires safeguarding or dissemination controls.



70% of U.S. Government data lives on contractor networks[2]

[2] https://www.nextgov.com/cybersecurity/2019/12/what-defense-departments-cyber-certification-will-mean-small-businesses/161838/



> “Every company within the DoD supply chain–not just the defensive industrial base, but the 300,000 contractors–are going to have to get certified to do work with the Department of Defense.[3] ”

-Katie Arrington
CISO, Department of Defense
Office of the Assistant Secretary of Defense for Acquisition

[3] https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors/

THE CASE FOR GOING BEYOND NIST 800-171

NIST 800-171 (also known as the Defense Federal Acquisition Regulation Supplement) requires contractors to demonstrate cybersecurity adherence for protection of Covered Defense Information (CDI) and CUI.

CUI is broad in scope, but can include:

- Legal material
- Technical drawings and blueprints
- Intellectual property

. . . precisely the kind of information most valuable to nation states and other threat actors.

Your organization likely creates & maintains CUI if it...

- Holds a Department of Defense contract
- Is a subcontractor to a DoD Contractor or supplier
- Does work for the Department of Defense

DFARS clause 252.204-7012 mandates that contractors provide “adequate security” on all of its unclassified information systems that process, store, or transmit CDI. This typically meant adherence with NIST 800-171, but the DoD has allowed companies that are still working to achieve full compliance with NIST standards to receive contracts and subcontracts. The contractor merely had to demonstrate they had in place an acceptable System Security Plan and Plan of Action and Milestones (POAM) that would eventually lead the company to full compliance.

Procurement example by Katie Arrington

CISO for the Department of Defense
Office of the Assistant Secretary of Defense for Acquisition

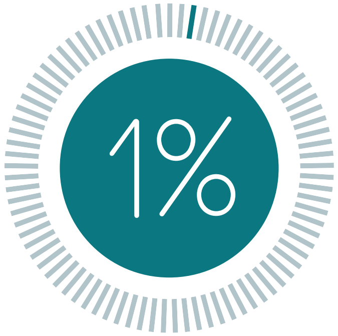
> “ In the true analysis, you haven’t been competitive.
>
> Here’s why: If I’m Small Business A, I have a contract with [controlled unclassified information]. DFAR clause 7012 applies to me. By the DFAR rule today, all you have to do is self-attest that you’re doing all 110 controls of NIST 171.
>
> I, Company A, attest I am doing 80 of the controls and I have a [plan of action] to implement the additional 30. I am technically acceptable on a contract.
>
> My rate is A.
>
> I’m Company B. I, too, am bidding on the same piece of work. I, too, have to be DFAR compliant. But I’m actually doing all 110 controls on NIST 171. My rate is B.
>
> Whose rate is higher? B.
>
> Who’s technically acceptable? A and B.
>
> Who’s going to get the work? A–every damn time.[4] ”

[4] https://www.nextgov.com/cybersecurity/2019/12/what-defense-departments-cyber-certification-will-mean-small-businesses/161838/

Why does "A" win every time?

Although contractors have been required to comply with NIST 800-171 since January 1, 2018, NIST 800-171 compliance across the Defense Industrial Base (DIB) has not been widespread enough to make an impact on cyber security within the DoD.

The CMMC's release marks the first time there will be a certification and accreditation (C&A) that will govern contractors' ability to work with the DoD or its supply chain.



of companies

in the Defense Industrial Base (DIB) have implemented all 110 NIST controls [5]

[5] https://www.nextgov.com/cybersecurity/2019/12/what-defense-departments-cyber-certification-will-mean-small-businesses/161838/

KEY POINTS OF THE CMMC

While NIST SP 800-171 Rev 1 is a foundational element to cyber security in the Government supply chain, it has three noted shortcomings effectively eliminated under CMMC: self-certification, applicability caveats, and flexibility for in-process compliance.

Interestingly enough, when NIST 800-171 was initially launched, the DoD would not accept any form of third-party audit for evidence of compliance. Yet, this is no longer the case with CMMC, which will require contractors to certify their internal cybersecurity technical practices and process maturity against published standards.

1 More than 300,000 defense DoD contractors and subcontractors must be certified at least at Level 1 in order to qualify for award. There is currently no waiver or deviation process for individual control gaps.

2 Contractors can no longer self-certify and instead will be certified by a CMMC 3rd-Party Assessment Organization (C3PAO). C3PAOs are limited to auditing work (cannot provide cybersecurity solutions), will undergo a background check, and will have received training by Mellon University's Software Engineering Institute (SEI) group.

3 The DoD will not retroactively inject CMMC into existing contracts. Selected RFIs (Requests for Information) will refer to CMMC requirements beginning in June 2020; selected RFPs (Requests for Proposals) will begin to include CMMC requirements in September 2020.

4 CMMC adds domains and process maturity to NIST 800-171. Asset management, recovery, and situational awareness are three domains that will be added to the current 14 NIST domains. CMMC will also add a process requirement starting at Level 2 suppliers.

5 Feasible adoption cost. Under CMMC, contractors will be able to roll any costs associated with security into their billable rate. Smaller contractors may take advantage of grants to assist with their initial certification.

6 CMMC requirements will align with the type of information handled by the organization. For example, under CMMC a company that handles nuclear fusion data would require a higher level of protections than one that handles building construction.

A DEEP DIVE INTO THE MATURITY LEVELS OF CMMC

DoD is increasingly concerned with the nature and speed of cyber threats targeting mission-critical government systems and data. The latest draft of the CMMC Model[6] categorizes contractor cyber security practice levels by Domains, Capabilities, Processes and Practices. You can view the graphics below that outline the 17 Capability Domains and the five levels of cyber security maturity.

As a result, CMMC has a number of practices that are focused on situational awareness, cyber threat alerts, and cyber threat intelligence. CMMC Levels 2 and 3 focus on more basic practices combined with cyber threat intelligence. Levels 4 and 5 focus include more advanced cyber threat intelligence (e.g., IOC's, threat hunting, cyber threat sharing)

[6] https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

The CMMC encompasses five maturity levels, from Level 1 comprising "Basic Cyber Hygiene" to Level 5 "Highly Advanced."

LEVEL 1: PERFORMED

Level 1 is for basic safeguarding of FCI (Federal Contract Information), and only addresses practices from the FAR Clause 52.204-21. There are no maturity processes assessed at Level 1. An organization performs Level 1 practices but does not have process institutionalization requirements.

LEVEL 2: DOCUMENTED

With 72 practices and 2 processes, Level 2 includes protecting CUI in addition to safeguarding FCI. In Level 2, the contractor will establish a policy that includes their identified domain. They will then document the CMMC practices to implement this policy.

LEVEL 3: MANAGED

Level 3 contains 130 practices including all 110 controls found in NIST 800-171 Rev.1, and is designed specifically around protecting CUI.

Note: All contractors that handle CUI will be required to certify at a CMMC Level 3. In Level 3, the contractor will establish, maintain, and resource a plan that includes their identified domain.

LEVEL 4: REVIEWED

Level 4 centers around reducing the risk from Advanced Persistent Threats (APTs). This level contains an additional 26 practices, sourced mostly from NIST 800-171 Draft RevB. In Level 4, the contractor will review and measure their identified domain activities for effectiveness.

LEVEL 5: OPTIMIZING

Level 5 centers around further reducing the risk from APTs This level contains an additional 15 practices. In Level 5, the contractor will standardize and optimize a documented approach for their identified domain across all applicable organization units.

CMMC MATURITY PROCESS PROGRESSION [7]

LEVEL 1

PERFORMED

0 PROCESSES

✓ Select practices are documented where required

LEVEL 2

DOCUMENTED

2 PROCESSES

✓ Each practice is documented, including Level 1 practices

✓ A policy exists that includes all activities

LEVEL 3

MANAGED

3 PROCESSES

✓ Each practice is documented, including lower levels

✓ A policy exists that cover all activities

✓ A plan exists, is maintained, and resourced that includes all activities*

LEVEL 4

REVIEWED

4 PROCESSES

✓ Each practice is documented, including lower levels

✓ A policy exists that covers all activities

✓ A plan exists that includes all activities*

✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management)

LEVEL 5

OPTIMIZING

5 PROCESSES

✓ Each practice is documented, including lower levels

✓ A policy exists that covers all activities

✓ A plan exists that includes all activities*

✓ Activities are reviewed and measured for effectiveness

✓ There is a standardized, documented approach across all applicable organizational units

[7] https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

17 CAPABILITY DOMAINS [8]

- Access Control **(AC)**
- Asset Management **(AM)**
- Audit & Accountability **(AA)**
- Awareness & Training **(AT)**
- Configuration Management **(CM)**
- Identification & Authentication **(IDA)**
- Incident Response **(IR)**
- Maintenance **(MA)**
- Media Protection **(MP)**
- Personnel Security **(PS)**
- Physical Protection **(PP)**
- Recover **(RE)**
- Risk Management **(RM)**
- Security Assessment **(SAS)**
- Situational Awareness **(SA)**
- System & Communications Protections **(SCP)**
- System & Information Integrity **(SII)**

[8] https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

FAQ AROUND THE CMMC

Will other Federal (non DoD) contracts use CMMC?

The initial implementation of the CMMC will only be within the DoD.

How will CMMC be different from NIST SP 800-171?

CMMC will implement multiple levels of cyber security, but will go a step further to assess the company's maturity/institutionalization of cyber security practices and processes.

How will my organization become certified?

Your organization will coordinate directly with an accredited, independent third party commercial certification organization to request and schedule your CMMC assessment.

You will be awarded certification at the appropriate CMMC level upon demonstrating the appropriate maturity in capabilities and organizational maturity to the satisfaction of the assessor and certifier.

Can I self-certify?

No. There will not be a self-certification.

How often will my organization need to be reassessed?

The duration of the certification is still under consideration.

If my organization is certified under the CMMC and I am compromised, will I lose my certification?

No, you will not lose your certification. However, depending on the circumstances of the compromise and the direction of the government program manager, you may be required to undergo recertification.

What if my organization cannot afford to be certified? Will I still be able to work on DoD contracts?

The cost of certification will be considered an allowable, reimbursable cost and should not be cost prohibitive. Contracts requiring CMMC will disqualify you from participating if your organization is not certified.

My organization is a subcontractor that does not handle CUI. Do I have to be certified anyway?

Yes. All companies conducting business with the DoD must be certified.

NCC GROUP:
YOUR CMMC GUIDE

NCC Group is an experienced FedRAMP 3PAO and has helped numerous organizations through other types of Federal Authorizations. Our team of consultants have direct experience as government operators, auditors, and information security officers (ISO).

We have the strategic and technical experience to help you implement a successful CMMC compliance program. Our tailored methodology will help you go from where you are today to the desired compliance level. Our experience across frameworks, standards, and regulations will help us build your CMMC compliance program to avoid over-engineering your processes and practices.

As your advisor, we will help you build an efficient, effective program that is easily manageable in the long term. We will also support your certification audit and continuous monitoring to ensure you remain in compliance with your requirements.

Whether your company has an experienced security team in-house (or if it lacks one entirely) we can help simplify CMMC for your business. We are focused on helping you secure your people, systems, and data on the way to successfully procuring new business.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face. To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

www.nccgroup.com

1 (800) 813 3523

uscons-info@nccgroup.com