EXOSTAR®
We build trust.

SUPPLIERS GUIDE TO THE

CYBERSECURITY MATURITY MODEL CERTIFICATION

How to Get on the Road to CMMC Compliance at Speed, and With Confidence

The Cybersecurity Maturity Model Certification (CMMC) is a new requirement for existing Department of Defense (DoD) contractors, subcontractors and suppliers that comprise the Defense Industrial Base (DIB). The certification will be built on existing requirements—such as NIST SP 800-171, NIST SP 800-53, private sector contributions and input from academia—and reinforces the self-attestation model with a mandatory third-party certification regime. The CMMC certification is intended to tighten cybersecurity within the DIB, and consists of five levels to measure the cybersecurity practices of contractors.

HOW DID WE GET HERE? *FAILURE*

The major reason the CMMC was introduced was that the DoD's existing compliance programs were not working as planned. The DOD estimates over $600 billion is lost every year to data exfiltration carried out by adversaries—cybercriminals and threat actors as well as nation-state actors. That number represents the value of Controlled Unclassified Information (CUI) lost annually. CUI is government parlance for information developed by the government itself or by U.S. defense sector manufacturers, universities and technology companies that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

Aside from the staggering dollar amount, the DoD rightly perceives the massive loss of highly sensitive defense technology data as a direct threat the United States' technological advantage and military superiority. The scale of the problem alarmed defense officials to the point where the CMMC program was announced in January 2019, and the initial CMMC Model version 1.0 was released to the public on January 31, 2020. Industry observers point to two main reasons why existing DoD compliance didn't work as designed:

1. LACK OF ENFORCEMENT

Prior to CMMC, DoD took a self-policing model to cybersecurity. The largest prime contractors were expected to be able to demonstrate compliance to the government, but on a self-attestation model. Additionally, primes were expected in turn to vouch for the compliance of the subcontractors and suppliers who fulfilled important aspects of procurement contracts.

Again, the method prescribed for primes to monitor their subcontractors' and suppliers' compliance was self-attestation – asking each company to self-assess and self-report its state of compliance, specifically with respect to SP 800-171's 110 security controls. Each was responsible for having a System Security Plan (SSP) and a Plan of Actions & Milestones (POA&M) that described how and when non-compliant systems or processes would be corrected. But with lack of enforcement, many subcontractors and suppliers adopted a lowest common denominator approach, implementing the least expensive security solutions available and calling it a day. Other organizations just didn't bother.

2. LACK OF AWARENESS

In the summer of 2019, the Defense Contract Management Agency undertook security audits of 10 prime contractors, each with DoD contracts worth at least $1 million, to evaluate the security controls they had implemented to protect CUI. Industry observers would have expected all 10 of these companies to have passed an audit. Nine of them failed, however, and each was found deficient in as many as 8 of the 10 basic security controls. The auditors found that the most common security shortcomings were:

- Weak passwords
- Lack of multifactor authentication
- Failure to mitigate vulnerabilities identified on networks and systems
- Placement of CUI on unprotected removable media

IMPLICATIONS FOR SUPPLIERS

If large DoD contractors, all presumably having dedicated security and IT resources, fared so poorly with respect to basic security hygiene, what should be the expectations for smaller companies with fewer resources? The DoD has consistently stated it doesn't want to place undue fiscal burden on the DIB, particularly on smaller businesses that may only seek a Level 1 certification (see sidebar for overview of the five levels in the CMMC model structure). For this level, the DoD selected cybersecurity practices that represent basic protection that most organizations should already have in place as required by the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS).

The DoD also recognizes that stepping up to CMMC presents ongoing resource challenges for all members of the DIB. For this reason, security will be an allowable cost that contractors and suppliers can claim for programs that require CMMC certification, based on contract type and required CMMC levels. Prime contractors may also offer assistance to their subcontractors to help them successfully achieve the necessary levels of certification.

WHEN WILL CMMC AFFECT US?

DoD began to roll out CMMC in early 2020, a process that will continue until fully implemented by 2026. Both 800-171 and CMMC will be requirements for all contracts that deal with CUI. There will also be mandatory reporting of DoD Basic Assessment Score for 171 for all new contracts actions. However, CMMC will not be inserted retroactively into ongoing programs. Only new DoD programs and those up for renewal will be subject to it. **Beginning in late 2020, RFIs and RFPs published by DoD may contain CMMC language, and suppliers planning to participate in new contracts from that date will need to be actively preparing for the certification process in order to participate in new programs.** For individual companies, they would need to obtain CMMC certification depending on the lifecycles of their current contracts and any future bids.

WHERE DO WE START?

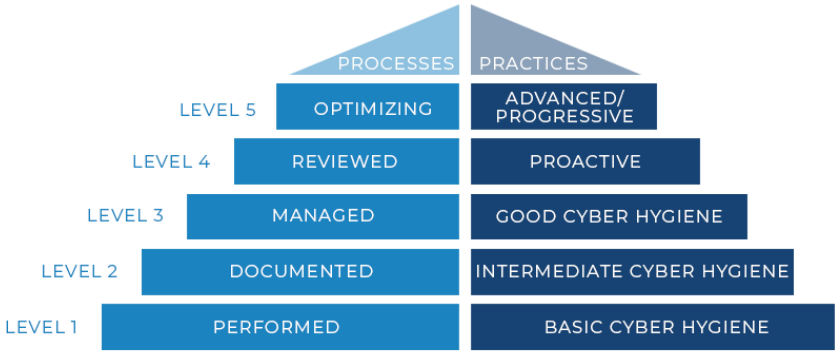
DO WE STILL NEED TO COMPLY WITH NIST 800-171, OR SHOULD WE JUMP RIGHT TO CMMC?

NIST 800-171 will remain relevant, and a contractors security posture (as scored with the DoD Assessment Methodology) will provide the government stronger insight into a companies progress as CMMC slowly ramps up over the next couple of years before accelerating. Organizations that store or handle CUI need to conduct and score a basic assessment based on DoD assessment methodology and submit the scores to DoD SPRS. DoD will review the organizations' DoD SPRS scores for new contracts. **If an organization doesn't have basic scores in SPRS, they are not going to be considered for new contracts.** Additionally, DoD will select organizations for audits, and conduct medium and high assessment audits.

Even though self-attestation is allowed, these businesses now need to shared their self assessment scores, based on the DoD Assessment Methodology, and should expect increased scrutiny in the form of audits conducted by DCMA. Inconsistencies between self-assessments and audits could put companies in jeopardy of adverse contract impacts or penalties under the False Claims Act.

On an important note, Plans of Action and Milestones (POA&Ms) that may have been accepted as part of NIST 800-171 compliance likely will not be allowed to successfully achieve CMMC certification. So, contractors subject to 800-171 compliance should be prioritizing implementation (and thus elimination) of their POA&Ms.

CMMC Model Structure: Cybersecurity Maturity Across Five Levels



LEVEL 1 - PERFORMED

0 Processes

- Select processes 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 covers 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 are 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 (results of the review are shared with higher level management)
- There is a standardized, documented approach across all applicable organizational units

17 CAPABILITY DOMAINS FOR CMMC LEVEL 3 CERTIFICATION

In order for suppliers to pass the audit process for CMMC Level 3 certification, they will need to demonstrate that they have adopted best practices and put in place security technologies and measures in the following areas:

- Access Control (AC)
- Incident Response (IR)
- Media Protection (MP)
- Risk Management (RM)
- Asset Management (AM)
- Maintenance (MA)
- Security Assessment (CA)
- Awareness and Training (AT)
- Situational Awareness (SA)
- Audit and Accountability (AU)
- Personnel Security (PS)
- System and Communications Protection (SC)
- Configuration Management (CM)
- Physical Protection (PE)
- System and Information Integrity (SI)
- Identification and Authentication (IA)
- Recovery (RE)

NEXT STEP FOR SUPPLIERS

Fundamentally, the NIST 800 provisions and now CMMC are all about data security. As such, raising your awareness of what kinds of data your organization holds, where it's stored and who has access to it should be the first order of business in preparing for CMMC certification. Keep in mind that NIST 800-171 addresses mainly confidentiality and integrity of the CIA triad (Confidentiality, Integrity and Availability). CMMC addresses availability and resilience additionally, while CMMC level 4 and 5 address advanced persistent threats (APT). The following is a framework for initiating such a review:

SCOPING

Data classification is natively defined and guided by DoD CUI and DoDI 5200.48

- Inventory your data (What do you have? How much?).
- Identify where the data resides and processes that utilize it.
- Work to reduce the data and its footprint.
- Inventory any 3rd party involvement.
- Establish clear expectations of shared responsibilities of 3rd parties.
- Identify FCIs or CUIs delivered by DoD and its contractors or created for DoD and its contractors.
- Scope, design, and implement the system and processes where FCI or CUI data resides and processes.
- Follow DODI 5200.48 for marketing and distribution control in case you deal with CUI.
- Place and maintain appropriate security controls, practices, and processes rqeuired by NIST 800-171/CMMC.
- Monitor and update those security measures whenever new changes occur.
- Report any incidents that may have impact on FCI/CUI.
- Report basic assessment score to SPRS every three years.

EXOSTAR®
We build trust.

SECURITY CONTROLS FOR CMMC

- Level 1: address items from 48 CFR § 52.204-21
- Level 2+: follow guidance in NIST SP 800-171A and integrate NIST SP 800-171 Appendix E
- CMMC practices and processes in NIST 800-171: Follow guidance in CMMC documentation and NIST 800-171A
- CMMC practices processes NOT in NIST 800-171: Follow guidance in CMMC documentation
- You can also work with third party consultants for readiness assessment.

MANAGE YOUR RELATIONSHIPS

- Seek to minimize receipt of CUI
- Ensure that you know if you need to flow requirements to any of your relationships

Controlled Unclassified Information (CUI)

What is CUI?

- Government created or owned UNCLASSIFIED information that must be safeguarded from unauthorized disclosure.
- An overarching term representing many difference categories, each authorized by one or more law, regulation, or Government-wide policy.
- Information requiring specific security measures indexed under one system across the Federal Government.

Why is CUI important?

- The establishment of CUI was watershed moment in the Department's information security program, formally acknowledging that certain types of UNCLASSIFIED information are extremely sensitive, valuable to the United States, sought after by strategic competitors and adversaries, and often have legal safeguarding requirements.
- Unlike with classified national security information, DoD personnel at all levels of responsibility and across all mission areas receive, handle, create, and disseminate CUI.
- CUI policy provides a uniform marking system across the Federal Government that replaces a variety of agency-specific markings, such as FOUO, LES, SBU, etc.

WHAT TO EXPECT FROM YOUR PRIME & MID-TIER PARTNERS

The current version of DFARS includes a flowdown provision that places the onus on primes to ensure that their entire supply chain is in compliance with NIST 800-171 if they are to receive CUI. This provision will remain valid for all current DoD programs until contract completion or renewal. Meanwhile, the DoD plans to update DFARS to account for the introduction of CMMC. CMMC mandates all participants on a bid team to possess certain levels of certification, with the minimum being a CMMC Level 1 for any first-tier subcontractors.

So, even though these flowdown provisions potentially increase compliance pressures on suppliers by requiring all companies in the DoD supply chain to obtain their own certification, prime contractors must still maintain visibility into the CUI capabilities and certifications of all of their subcontractors and suppliers. This will allow them to confidently bid on contracts at all five CMMC levels, particularly those at Level 3 and above when CUI is a factor, as well as protect their own sensitive data and intellectual property. As such, suppliers need to be aware that they are likely to come under increased scrutiny from primes and subcontractor partners in the years ahead. In addition, suppliers can expect their DIB partners will be applying evaluation criteria frameworks that mandate inquiries such as:

SUPPLIER CYBER RISK

- What kinds of cybersecurity technologies have suppliers put in place, and of what quality?
- Have they submitted, or have plans to submit, their DoD Assessment Methodology Basic score to the SPRS?
- Do they have a valid System Security Plan, and associated IT Policies, that align with their DoD Assessment Methodology Basic score?
- Do they have funding and a project plan associated with POAMS (plans of actions and milestones) for any deficiencies?
- Do they have an understanding of what CUI is, and if they create or receive CUI?
- If using cloud services, such as email, as part of the processing of CUI, are they working with a vendor and service offering that contractually commits to providing 171 fully compliant services, with no POAMs?
- Are suppliers upgrading their performance capabilities to align with the new mandates?
- Can suppliers accomodate innovative & non-conventional methods to accept support from upstream partners?

EXOSTAR®
We build trust.

CERTIFICATION ASSISTANT FROM EXOSTAR

THE SINGLE, SECURE SYSTEM FOR ALL NIST 800-171 AND CMMC MATERIALS & OPERATIONS

Demonstrating command of cybersecurity best practices and investment in high quality CMMC compliance tools and technologies will be basic business qualifiers for suppliers in the new regulatory environment. Certification Assistant from Exostar is the single solution from a proven, long-time technology provider to the DIB that will enable you to face the CMMC challenge with confidence. Certification Assistant delivers a comprehensive platform for streamlining the implementation of controls and policies necessary to complete an accurate NIST 800-171 self-assessment and to prepare for CMMC certification success.

For suppliers and subcontractors who've struggled to track NIST compliance via spreadsheets, file shares and email threads, Certification Assistant will be a very welcome new solution indeed. Through an intuitive SaaS-based user interface, Certification Assistant provides comprehensive workflows that empower self-guided, step-by-step progress to NIST 800-171 and CMMC compliance. It's your secure online platform that centralizes all documents, communications and processes needed to achieve certification at your required Level.

EXOSTAR®
We build trust.

CERTIFICATION ASSISTANT FEATURES

- Dashboard enables quick, close tracking of overall assessment and compliance status.
- Easy-to-understand reports illustrate compliance status and gaps, and identify essential next steps and activities.
- With no limit on number of users, your appropriate staff can own their part of the process, and collaborate internally to accomplish tasks.
- Task Assignment and Status Tracking by user provides insight into the full range of action items.
- Information guides provide clarification on all controls and practices.
- Storage for policy documents, control/practice implementation responses, and associated evidence eliminates sprawl, and prepares you to collect information that certification assessors are certain to ask about.
- Support for security controls, processes, and practices, along with the establishment of system security plans (SSPs) and plans of action and milestones (POA&Ms), simplifies interactions with third-party service providers.
- Reporting for risk and compliance attributes prepares suppliers for successful audits.
- Secure access control and content protection are provided through Exostar's Managed Access Gateway (MAG).

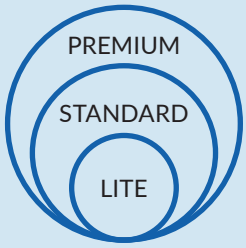
AVAILABLE IN 3 TIERS

PAY ONLY FOR WHAT YOU NEED

Certification Assistant offers the flexibility of tiered options to accommodate different CMMC compliance levels. Each tier includes a dashboard and reporting for risk and compliance attributes and accommodates evidence and artifact uploading. You can upgrade to Certification Assistant Standard or Premium at any time.

Flexible Tiers for Every Level in the CMMC

If you're a supplier that never or rarely handles CUI, it's likely you'll never need to get certified beyond Level 2 certification. By tailoring Certification Assistant to the progressive levels of the CMMC model, and making it available in a convenient Software-as-as-Service (SaaS) basis, we ensure you can progress toward the Certification Level you need, and do so without the exorbitant costs associated with enterprise software platforms.



EXOSTAR®
We build trust.

	LITE	STANDARD	PREMIUM
CMMC assessment	Level 1	Level 1 - 3	Level 1 - 5
NIST 800-171 assessment		✓	✓
CMMC level explanation and guidance	✓	✓	✓
Storage for documents, evidence, and evaluation criteria	✓	✓	✓
Managing the system description, environment, asset inventory, and policy documents	✓	✓	✓
All attachments encrypted in FIPS 140-2 validated module	✓	✓	✓
Assigning and tracking multiple action items per Practice/Process	✓	✓	✓
Status of compliance and identification of security gaps	✓	✓	✓
Compliance reporting	✓	✓	✓
Dashboard – Overall assessment status	✓	✓	✓
Dashboard – Individual domain level asessment status for CMMC and NIST 800-171		✓	✓
Dashboard – DoD Basic Assessment Score		✓	✓
DoD Basic Assessment Score and report for SPRS submission		✓	✓
30 day free trial	✓	✓	
Partner engagement for external assessment	✓	✓	
Risk management		✓	✓
Generating SSP/POAM for CMMC and NIST 800-171		✓	✓
Importing asessment data of Exostar Partner Information Manager		✓	✓

Try CA Free!
You can sign up for a 30-day free trial on our **Registration Portal**

EXOSTAR®
We build trust.

A PROVEN DOD TECHNOLOGY LEADER

Since 2000, Exostar has been helping organizations in highly-regulated industries mitigate risk, solve identity and access challenges, and collaborate securely across their supply chain ecosystem. The company was originally founded through a consortium of some of the largest DoD prime contractors serving the DIB: BAE SYSTEMS, The Boeing Company, Lockheed Martin Corporation and Raytheon Company. Providing tools and resources to help subcontractors and suppliers to conduct DIB business securely and compliantly was key to the joint, business-improvement vision at Exostar's founding and remains core to the solutions we provide today.

Exostar's cloud-based platforms create exclusive communities within highly-regulated industries where organizations securely collaborate, share information, and operate compliantly. Within these communities, we build trust. More than 135,000 aerospace and defense organizations and agencies in over 150 countries trust Exostar to strengthen security, reduce expenditures, raise productivity, and help them achieve their missions. Exostar is a Gartner Cool Vendor.

WANT TO LEARN MORE?

Visit us at www.exostar.com

ADDRESS

2325 Dulles Corner
Blvd. Suite 600
Herndon, VA 20171

CONTACT

info@exostar.com
(703) 561 - 0500

CONNECT

LinkedIn
Twitter