SUPPLIER CYBERSECURITY

WHERE TO START

The Defense Industrial Base is facing new threats every day. The Deparement of Defense needs its supply chain to enhance its security and resiliency in the cybersecurity space. Bell Flight will provide information and tools to our supply base to help prepare for the cybersecurity requirements in efforts to secure the supply chain.

TOOLS

UNDERSTANDING THE REQUIREMENTS

Use resources provided by Bell, such as the CMMC FAQ and Helpful Links, in conjunction with public resources, such as Project Spectrum, to educate your business about CMMC.

SSP AND POAM TEMPLATE

Use the templates provided as a guide to track and measure your progress with NIST SP 800-171 Rev. 1 and CMMC implementation .

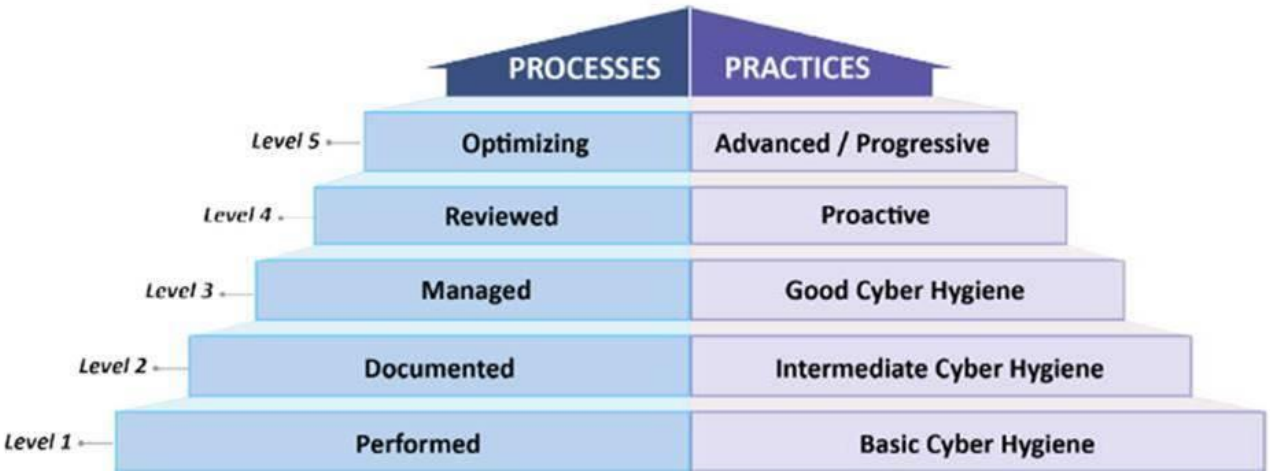
FOCUS GROUPS

Small and Medium Businesses are invited to collaborate with the prime through discussions on their CMMC implementation progress.

PROVIDED BY

SCM CYBER RISK TEAM

STEP 1:
UNDERSTANDING THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



Short Answer:

The CMMC framework verifies the implementation of processes and practices associated with the achievement of a required cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level that corresponds with the risk.

Long Answer:

CMMC accounts for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references. The CMMC levels and the associated sets of processes and practices are cumulative and build upon each other. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and the increased security requirements for CUI specified in NIST SP 800-171 Rev. 1 per DFARS clause 252.204-7012. Furthermore, the CMMC model includes an additional five processes and 61 practices across Levels 2-5 that demonstrate a progression of cybersecurity maturity.

STEP 2:
EVALUATING THE NEED FOR YOUR BUSINESS TO BE CMMC COMPLIANT

Ask yourself the following questions:

1. Do I anticipate bidding for military work in the future?
    a. If Yes, you should anticipate being CMMC compliant in future contracts.
    b. If No, you are exempt from CMMC per DFARS 252.204-7021.

2. Do I exclusively supply COTS (commercial off-the-shelf) items to Bell?
    a. If Yes, you are exempt from CMMC per DFARS 252.204-7021.
    b. If No, you should anticipate being CMMC compliant in future contracts.

3. Do my departments that support part build (i.e. sales, engineering and design, quality) access ENOVIA or other Bell technical data?

Starting 2021, if you anticipate being awarded a contract that supports a military program, you will need at least a CMMC Level 1. By 2025, the CMMC requirement will be on all DoD Contracts. This certification is an entry to market requirement. Whether your business is a machine shop or a large OEM, you'll need a cybersecurity certification. The level varies by what kind of data you access from the prime contractor.

Think of CMMC like a quality certification, and view the parallels below:

	AS9100 Rev D	CMMC
Certification to do businesses with the DoD	Yes	Yes
Individual auditors	Yes	Yes
Renewable Certification	Yes	Yes
Goal of the Certification	**Create a standard** for Quality Management Systems in the Aviation, Space and Defense (AS&D) industry	**Create a standard** for cybersecurity practices and hygiene in the Defense Industrial Base (DIB).

We've made physical safety and quality a foundation in how we do business. Now it's time to do the same with our supply base by adopting and standardizing cybersecurity practices to protect the information in the DIB. CMMC builds upon DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting), which appears as a flow down in past DoD contracts.

I don't do business directly with the DoD, why does this apply to me?

Since CMMC is a DFARS requirement, it is mandated to be flowed down to the supply chain. Whether you're a 1st or 7th tier subcontractor, a CMMC level must be awarded for you in order to do business with the DoD at any level. The goal of CMMC is to mitigate risk of information theft at ***all*** levels.

STEP 3:
ACCESSING CMMC RESOURCES

Bell has created a Cybersecurity Toolkit with resources to help our suppliers begin to understand CMMC. These resources can be found in the “Cybersecurity Toolkit” folder in your Sell2Bell Portal.

- CMMC FAQs
- Helpful Links
- Requirements Interim Rule DFARS Case 2019-D041
- NIST SP 800-171 Rev 1 Methodology and Assessment

These documents were created with information from several DoD resources and designed to be a one-stop shop for questions your organization may have regarding the NIST assessment and the CMMC certification.

Here are other free resources provided by different government agencies dedicated to cybersecurity education:

Project Spectrum : Created by the Office of Small Business Programs of the Department of Defense. The goal of Project Spectrum is to educate businesses about CMMC and how to be compliant. It includes training videos, webinars from DoD officials, online course, NIST Self-Assessment Tool, and more.

NIST Small Business Cybersecurity Corner: Created by the U.S. Department of Commerce. This site provides cybersecurity basics, guidance, solutions, and training to protect your information and manage your risks. Look into The National Initiative for Cybersecurity Education (NICE) framework to access provides free and low-cost online cybersecurity training.

ND-IASC CyberAssist: The DIB SCC Industry Task Force is identifying and posting links to helpful publicly available cybersecurity resources. The resources were selected both to help companies (i) meet DoD and other U.S. cybersecurity standards applicable to U.S. federal contractors (e.g., FAR Basic Safeguarding clause, DFARS Safeguarding CDI clause, CMMC); and (ii) otherwise improve their current cybersecurity protections.

BEWARE OF SCAMS: CMMC Accrediting Body (AB) is the only organization that can assign a CMMC Level to your business. As of February 2021, the CMMC AB has approved provisional assessors, but have not started the audits. A portal to sign up for your certification has not been released. Be vigilant and do not be misled by third-party entities who are publicly representing themselves as capable of providing a CMMC certification that will be accepted by the DoD. Bell Flight will release communication and instructions on how to sign up for your CMMC certification when available.

STEP 4:
PERFORM A NIST SP 800-171 R1 ASSESSMENT

Before you get a CMMC certification by the CMMC Accrediting Body, you need to complete the NIST SP 800-171 Rev. 1 basic assessment and submit your results into the Supplier Performance Risk System (SPRS). The assessment is called out in the interim rule specified in DFARS Case 2019-D041:

DFARS 252.204-7019	DFARS 252.204-7020
Requires offerors to ensure the results of any applicable current Assessments are posted in SPRS.	Requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment.

The clauses above do not duplicate, overlap, or conflict with any other Federal rules. Rather these rules validate and verify contractor compliance with the existing cybersecurity requirements in FAR clause 52.204-21 and DFARS clause 252.204-7012 and ensures that the entire DIB sector has the appropriate cybersecurity processes and practices in place to properly protect FCI and CUI during performance of DoD contracts.

As the NIST framework has matured, there are free resources for your business to complete the audit:

- ***Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 rev 1 Security Requirements:*** Review the step-by-step guide to assessing a small manufacturer's information systems against the security requirements in NIST SP 800-171 Rev 1. Click here to access or see the Bell Cyber Toolkit.
- ***NIST SP 800-171 rev 1 DoD Assessment Methodology Version 1.2.1****:* Provides a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171 Rev 1. Click here to access or see the Bell Cyber Toolkit.

NOTE: Performing the basic assessment does not make your company compliant. This assessment methodology measures a company's compliance to the 110 controls of NIST SP 800-171 Rev 1. A NIST compliance score could be zero, a negative score, or a perfect score being 110.

STEP 5:
CRAFTING A CMMC GAME PLAN

1. *Identify your stakeholders*
    a. Who will lead the CMMC initiative for the business?
    b. Who will be affected by this new requirement?
    c. Who will help interpret and implement changes that this requirement will bring in the business?
    d. Who will approve additional personnel/equipment needed to be CMMC compliant?
    e. Ex: Legal, Compliance, IT, Cybersecurity, Engineering, Procurement, Contracts

2. *Quantify Resources and Personal:*
    a. Should the business hire consultants or does the business have the resources and expertise to do a self-evaluation and implementation?
    b. How many man hours will be needed to be compliant?
    c. How much will I spend on software, hardware, or firmware purchases and upgrades to be compliant?

3. *Determining the Right CMMC Level for your Business*
    a. Who should help gauge my data sharing environment?
    b. Do I handle CUI or do I anticipate handling CUI in the future?
    c. How much data and what type of data from the prime do I access?
    d. How much data from the prime am I flowing down?

NOTE:

The CMMC framework requires contractors to flow down the appropriate certification requirements to subcontractors throughout the entire supply chain. DIB companies that do not process, store, or transmit CUI, must obtain a CMMC Level 1 certification. DIB companies that process, store, or transmit CUI must achieve a CMMC Level 3 or higher, depending on the sensitivity of the information associated with a program or technology being developed. The DoD will specify the required CMMC level in Requests For Information (RFIs) and Requests for Proposals (RFPs). Bell suggests that suppliers proactively create CMMC goals and gap analysis between their possible target levels.

Focus Groups

Implementing and complying to growing cybersecurity regulation is a challenge. If you would like to sign up for a cybersecurity focus group to share your experience and questions, please email scmcyberrisk@bellflight.com.

Topics of Discussion include:

- NIST SP 800-171 Rev 1 and SPRS
- CMMC goal and timeline for your business
- Roadblocks/Hurdles
- Data Marking

FREQUENTLY ASKED QUESTIONS (FAQS)

1. **What does each CMMC Level consist of?**

Level	Description
1	Consists of the 15 basic safeguarding requirements from FAR clause 52.204-21.
2	Consists of 65 security requirements from NIST SP 800-171 implemented via DFARS clause 252.204-7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3.
3	Consists of all 110 security requirements from NIST SP 800-171, 20 CMMC practices, and 3 CMMC processes.
4	Consists of all 110 security requirements from NIST SP 800-171, 46 CMMC practices, and 4 CMMC processes.
5	Consists of all 110 security requirements from NIST SP 800-171, 61 CMMC practices, and 5 CMMC processes.

2. **What is Controlled Unclassified Information (CUI)?**

   CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

   A CUI Registry provides information on the specific categories and subcategories of information that the Executive branch protects. The CUI Registry can be found at: https://www.archives.gov/cui . Resources, including online training to better understand CUI, can be found on National Archives' website at https://www.archives.gov/cui/training.html.

   For guidance on how to mark CUI data in your business, please review the training publication provided by the Department of Defense here or at https://www.dodcui.mil/Home/Desktop-Aids/.

3. **Who is exempt?**

   DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, ***except for acquisitions solely for commercially available off- the-shelf (COTS) items.***

4. **When should I be CMMC certified? How often does my organization need to be reassessed?**

   Prior to awarding a contract to a subcontractor, the prime contractor must ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the appropriate level for the information that is being flowed down to the subcontractor. The subcontractor must be reassessed every 3 years.

5. Will there be new DFARS clauses added to future contracts?

Per the Interim Rule DFARS Case 2019-D041, here are 3 new clauses regarding NIST SP 800-171 and CMMC:

New Provision: DFARS 252.204-7019

- Notice of NIST SP 800-171 DoD Assessment Requirements.
- Requires offerors to ensure the results of any applicable current Assessments are posted in SPRS

New clause: DFARS 252.204-7020

- NIST SP 800-171 DoD Assessment Requirements.
- Requires a contractor to provide the Government with access to its facilities, systems, and personnel when it is necessary for DoD to conduct or renew a higher-level Assessment.

New clause: DFARS 252.204-7021

- Cybersecurity Maturity Model Certification Requirements
- Requires a contractor to: Maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments.

6. What is the difference between NIST SP 800-171 Rev. 1 and CMMC?

NIST SP 800-171 Rev. 1 is a self-assessment performed by the contractor in accordance to the NIST SP 800-171 DoD Assessment Methodology. The framework consists of three levels of assessments (Basic, Medium, High). These three types of assessments reflect the depth of the assessment, and the associated level of confidence in the assessment results.

Unlike NIST SP 800-171, the CMMC model possesses five levels. Each level consists of practices and processes as well as those specified in lower levels. In addition to assessing a company's implementation of cybersecurity practices, the CMMC will also assess the company's institutionalization of cybersecurity processes.

CMMC Levels 1-3 encompass the 110 security requirements specified in NIST SP 800-171 Rev 1. CMMC incorporates additional practices and processes from other standards, references, and/or sources such as NIST SP 800-53, Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 "Critical Security Controls for Effective Capability in Cyber Defense", and Computer Emergency Response Team (CERT) Resilience Management Model (RMM) v1.2.

7. **How do I enter my NIST SP 800-171 Rev. 1 Basic Assessment into SPRS?**

   To create a SPRS account, go to the Procurement Integrated Enterprise Environment (PIEE) Getting Started Page. To troubleshoot problems you may encounter when creating a PIEE account, please contact the PIEE Help Desk. Per the new provision DFARS 252.204-7019, offerors must ensure the results of any applicable current Assessments are posted in Supplier Performance Risk System (SPRS). Please review the Quick Entry Guide for step by step instructions to log your assessment into the Assessment Database. To troubleshoot problems you may encounter when entering your assessment, please review the FAQs or contact customer support.

8. **How will my organization become certified?**

   The CMMC Accreditation Body (AB), a non-profit, independent organization, will accredit CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors. The CMMC AB will provide the requisite information and updates on its website (www.cmmcab.org).

   Only CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors that have been accredited by the CMMC AB will perform CMMC assessments. The CMMC AB plans to establish a CMMC Marketplace that will include a list of approved C3PAOs as well as other information. After the CMMC Marketplace is established, DIB companies will be able to select one of the approved C3PAOs and schedule a CMMC assessment for a specific level.

9. **What is the cost of a CMMC certification per level?**

   Per interim rule DFARS Case 2019-D041, here is the cost breakdown per CMMC Level below. To review the engineering and certification costs associated with the assessment in depth, please review the interim rule DFARS Case 2019-D041, D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule, section 2. CMMC Framework.

CMMC cert	Annual Assessment Cost	Cost to Certify (Every 3 years)
Level 1	$1,000	$3,000
Level 2	28,050	84,150
Level 3	60,009	180,027
Level 4	371,786	1,115,358
Level 5	482,874	1,448,622

HELPFUL LINKS

1. **Cybersecurity Maturity Model Certification (CMMC)**
   - Homepage: https://www.acq.osd.mil/cmmc/index.html
   - CMMC Updates: https://www.acq.osd.mil/cmmc/updates.html
   - FAQs: https://www.acq.osd.mil/cmmc/faq.html
   - CMMC Model and Assessment Guides: https://www.acq.osd.mil/cmmc/draft.html
     - This section includes PDFs, excel files, and assessment guides for CMMC Level 1 and 3.

2. **CMMC Level Model Matrix**
   - To see all domains covered by CMMC and how each practice references other cybersecurity frameworks:
     - CMMC Model Matrix: pg. 5-40
     - Source Mapping: pg. 325-332

3. **Controlled Unclassified Information (CUI)**
   - CUI Registry: https://www.archives.gov/cui
   - CUI Training and resources: https://www.archives.gov/cui/training.html

4. **Regulation and clauses related to NIST SP 800-171 Rev. 1 and CMMC:**
   - FAR 52.204-21
   - DFARS 252.204-7012
   - DFARS 252.204-7019
   - DFARS 252.204-7020
   - DFARS 252.204-7021

5. **Procurement Integrated Enterprise Environment (PIEE):**
   - Home page: https://piee.eb.mil/piee-landing/
   - Creating an account: piee.eb.mil
   - Help Desk:
     - Phone: 866-618-5988
     - Email: disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil
     - Fax: 801-605-7453
     - Website:https://piee.eb.mil/xhtml/unauth/web/homepage/vendorCustomerSupport.xhtml#helpdesk

6. **Supplier Performance Risk System (SPRS)**
   - Home page**:** https://www.sprs.csd.disa.mil/
   - Instructions to enter your NIST SP 800-171 r1 basic assessment into SPRS: Quick Entry Guide
   - Review the NIST SP 800-171 Rev. 1 FAQs to help troubleshoot your assessment upload: FAQs
   - Customer Support Desk:
     - Phone: Commercial: (207) 438-1690 or DSN: 684-1690
     - Email: webptsmh@navy.mil
     - Website: https://www.sprs.csd.disa.mil/contacts.htm

7. **CMMC Accreditation Body (AB)**
   - For updates regarding CMMC Third Party Assessment Organizations (C3PAOs) and individual assessors: www.cmmcab.org

8. **Helpful Readings and Articles**
   - *CMMC—Securing the DIB Supply Chain with the Cybersecurity Maturity Model Certification Process*. Carnegie Mellon University Software Engineering Institute, 2020, https://resources.sei.cmu.edu/asset_files/FactSheet/2020_010_001_638407.pdf

   - *Your Best Cyber Defense Isn't a '60s Super Spy. It's You*. Smart Manufacturing Experience, 2020, https://www.sme.org/technologies/articles/2020/october/your-best-cyber-defense-isnt-a-60s-super-spy.-its-you/