DFARS, NIST SP 800-171, AND CMMC 2.0 COMPLIANCE

With the escalating threat of cyberattacks, the DoD has prioritized addressing cybersecurity threats and protecting sensitive information, including controlled unclassified information (CUI) and federal contract information (FCI). (Courtesy: Shutterstock)

As a heat treater, complying with these Department of Defense certifications can be critical to your company's future.

By **JOE COLEMAN**

As a heat treater, if you are providing services or products to a Department of Defense (DoD) contractor, a downstream supplier, or fall anywhere within the DoD supply chain, you are most likely affected by certain DoD mandates.

Discussions around DFARS compliance, NIST SP 800-171 implementation, and cybersecurity within the federal defense contracting space is becoming increasingly prevalent. Although it seems like the conversation has just recently gained steam, the DFARS mandate has been around longer than most people realize.

In this article, you will be provided the answers to the most common questions regarding how heat treaters can position themselves for additional business by becoming compliant, remaining compliant, and improving overall cybersecurity health.

WHO NEEDS TO BE COMPLIANT

With the escalating threat of cyberattacks, the DoD has prioritized addressing cybersecurity threats and protecting sensitive information, including controlled unclassified information (CUI) and federal contract information (FCI). The DoD is requiring all contractors, subcontractors, and suppliers to comply with DFARS 252.204-7012. Don't take a chance at losing your current DoD contracts and losing future business because you're not compliant. Compliance is not an option if you fall within the DoD supply chain and the Defense Industrial Base (DIB).

If you have or are pursuing any contracts that include DFARS Clause 252.204-7012 requirements, you are already required to be compliant with NIST SP 800-171, including the major provisions of what is required in CMMC 2.0.

SOME CYBERSECURITY STATISTICS

Heat treaters implementing effective cybersecurity practices are particularly challenged today because there are more devices (including mobile devices) than people, and attackers are becoming more innovative. Cybersecurity is the practice of protecting systems, data, networks, and programs from digital attacks (web/cloud-based). These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes and procedures. This is why the government is pushing for enhanced cybersecurity more than ever before. You need to be sure you and your customers' critical data and systems are protected and secured.

Here are some statistics from 2022 on how cybercrime affects SMBs (small to mid-sized businesses):

» Less than 50 percent of SMBs have a cybersecurity plan in place.

» Cyberattacks have increased by nearly 600 percent since the beginning of the pandemic in 2020.

» 58 percent of cyberattack victims are small and mid-sized businesses.

» Major data breaches cost businesses an average of $4.35 million in 2022 … each.

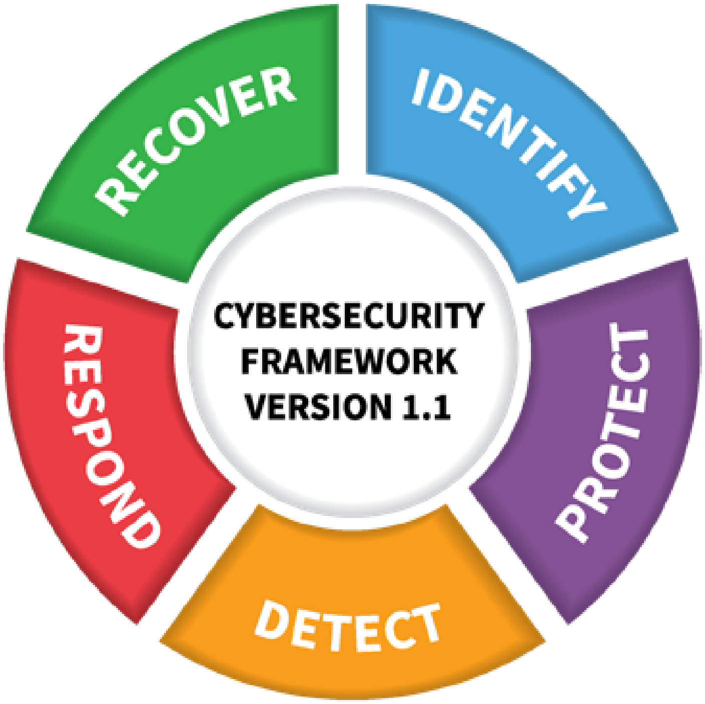
» 60 percent of small companies close their business within six months after a major security breach.

» 55 percent of ransomware attacks involve companies with fewer than 100 employees.

» 95 percent of cybersecurity breaches are a result of human error (the weakest link).

» About 236 million ransomware attacks occurred globally in the first half of 2022.

Cyberattacks continue to increase day by day, minute by minute. For your business to survive, you need to implement the NIST security control requirements and "harden" your security position now — before something goes wrong.



The DoD is requiring all contractors, subcontractors, and suppliers to comply with DFARS 252.204-7012. (Courtesy: Bluestreak Consulting)

WHAT IS DFARS 252.204-7012?

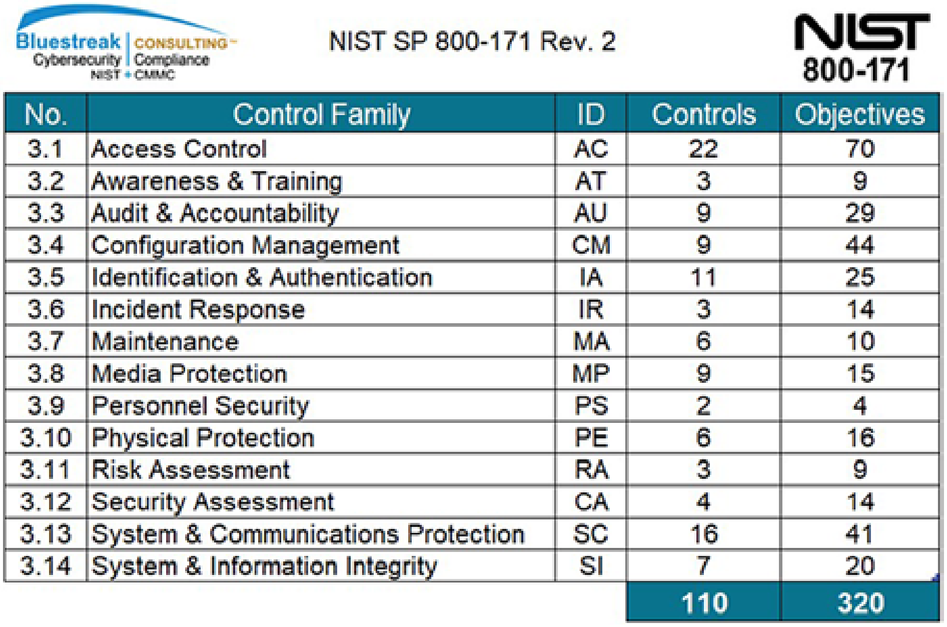
What are the DoD compliance requirements for members of the DIB? The Defense Federal Acquisition Regulation Supplement or DFARS is a set of cybersecurity regulations that defense contractors must follow to be awarded new DoD contracts and to keep current contracts.

Originally implemented in 2016, DFARS 252.204-7012 requires safeguarding and "adequate security" of covered defense information (CDI), which also includes CUI, by implementing the guidelines found in NIST SP 800-171.

DFARS 252.204-7012 further requires contractors, subcontractors, and suppliers to follow certain procedures in the event of a cyber incident, including reporting the incident to the government and providing access to systems. Lack of DFARS compliance will result in the loss of current and future contracts. As a result, this can also hurt the organization's reputation. And, as you already know, bad news travels faster than good news.

WHAT IS NIST SP 800-171?

NIST SP 800-171 is a National Institute of Standards and Technology Special Publication that provides recommended requirements for protecting the confidentiality of CUI in non-federal organizations or businesses. Defense contractors, subcontractors, and downstream suppliers must implement the recommended 110 controls contained in NIST SP 800-171 to demonstrate their provision of adequate security to protect the sensitive information and CUI included in their defense contracts, as required by DFARS 252.204-7012. If a manufacturer is part of a DoD, General Services Administration (GSA), NASA, or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must.


Bluestreak | CONSULTING
Cybersecurity | Compliance
NIST + CMMC
NIST
800-171

NIST SP 800-171 Rev. 2

No.	Control Family	ID	Controls	Objectives
3.1	Access Control	AC	22	70
3.2	Awareness & Training	AT	3	9
3.3	Audit & Accountability	AU	9	29
3.4	Configuration Management	CM	9	44
3.5	Identification & Authentication	IA	11	25
3.6	Incident Response	IR	3	14
3.7	Maintenance	MA	6	10
3.8	Media Protection	MP	9	15
3.9	Personnel Security	PS	2	4
3.10	Physical Protection	PE	6	16
3.11	Risk Assessment	RA	3	9
3.12	Security Assessment	CA	4	14
3.13	System & Communications Protection	SC	16	41
3.14	System & Information Integrity	SI	7	20
			110	320

NIST SP 800-171 is a National Institute of Standards and Technology Special Publication that provides recommended requirements for protecting the confidentiality of CUI in non-federal organizations or businesses. (Courtesy: Bluestreak Consulting)

NIST SP 800-171 requirements consist of 14 specific security control families. Within the 14 security control families, there are 110 separate controls and, within those controls, there are 320 individual control/assessment objectives, all of which need to be met to become 100 percent compliant.

WHAT IS CMMC 2.0?

CMMC stands for Cybersecurity Maturity Model Certification. It combines the controls from NIST SP 800-171 and from other sources, depending on the level of certification. This is a new model that will replace NIST SP 800-171 and will be enforced by the DoD. What is the difference? The new CMMC 2.0 contains three levels of certification, which will give the contractor a score that will determine their ability to bid on certain contracts.

CMMC Level 1: Foundational Cyber Hygiene

The most basic level of security, Level 1, requires the implementation of basic cybersecurity hygiene practices such as password management and keeping systems up-to-date with security patches. This level is intended for small businesses with minimal risk to their data.

There are 17 Controls in Level 1, and they are based on what is found in the Federal Acquisition Regulation FAR 52.204-21. This is a good starting point for organizations just beginning to implement cybersecurity measures, or who have limited resources.

Level 1 certification is required for companies that handle Federal Contract Information (FCI) but aren't considered part of the critical infrastructure, which includes most businesses and government agencies.

Level 1 is NOT for any business that processes, stores, or transmits CUI in any way. If you handle CUI, a Level 2 certification is a minimum requirement.

CMMC Level 2: Advanced Cyber Hygiene

Level 2 builds on the cybersecurity hygiene practices of Level 1 and requires additional measures to be put in place.

Level 2 is similar to NIST SP 800-171 and includes 110 practices. Some of the practices focus on access control, incident response, risk management, physical security, and system and information integrity. If you have any doubt about whether you handle CUI (or will in the future), Level 2 certification is recommended.

CMMC Level 3: Expert Cyber Hygiene

Level 3 is the highest level of CMMC certification and requires the most stringent security measures. Level 3 is based on NIST SP 800-171 and adds additional practices from NIST SP 800-172. The extra practices focus on more sophisticated detection and response capabilities, information protection, and system-hardening requirements.

Level 3 certification is required for the same types of companies that need Level 2 certification, but who also handle CUI in the most sensitive or higher security assurance of DoD contracts. Organizations required to comply with CMMC Level 3 certification are assessed by the federal government's Defense Contract Management Agency. Assessment process details for Level 3 are still being developed at this time.

THE DFARS INTERIM RULE

On September 29, 2020, the DoD published the DFARS interim rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, effective November 30, 2020. These new clauses are an extension of the original DFARS 252.204-7012 clause that has been required in DoD contracts since 2018.

The interim rule consisting of DFARS Clauses 252.204-7019, 252.204-7020, and 252.204-7021 implements the NIST SP 800-171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The interim rule requires contracting officers to take specific action before awarding contracts, tasks, or delivery orders, or exercising an option period of extending the period of performance on existing contracts, on or after November 30, 2020.

DFARS 252.204-7019 CLAUSE: NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

All DoD contractors in the DIB and their supply chain must complete a self-assessment using the DoD's NIST 800-171A Assessment

Heat treaters implementing effective cybersecurity practices are particularly challenged today because there are more devices (including mobile devices) than people, and attackers are becoming more innovative. Courtesy: Shutterstock)

Methodology and generate a points-based score. If the self-assessment score falls below 110, contractors are required to create a POAM (plan of action with milestones) and indicate by which date the security gaps will be remediated and a score of 110 will be achieved as part of the Supplier Performance Risk System (SPRS). At the time of contract award for a DoD contract containing the new 7019 clause, a DoD contracting officer will verify that a score has been uploaded to the SPRS.

DFARS 252.204-7020 CLAUSE: NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

Along with the 252.204-7012 and 252.204-7019 clauses, the 252.204-7020 clause is approved for use in all DoD contracts. This new clause requires contractors provide the government with access to its facilities, systems, and personnel when it's necessary for the DoD to conduct or renew a higher-level assessment. The higher-level assessments are the medium and high assessments. The self-assessment conducted as part of the 252.204-7019 clause is called a basic assessment.

A medium assessment is conducted by DoD personnel and will include a review of your system security plan (SSP) and how each of the requirements is met to identify any language that may not adequately address the security requirements.

A high assessment is conducted by DoD personnel onsite at the contractor's location and will leverage the full NIST 800-171A to determine if the implementations meet the requirements by reviewing evidence and demonstration such as recent scanning results, system inventories, baseline configurations, and demonstration of multifactor authentication and/or two-factor authentication.

Along with that, this rule also requires contractors flow down their requirements from 252.204-7019 to their subcontractors and suppliers. Just as the DoD may choose not to award a contract due to noncompliance, you may not be able to use a subcontractor or supplier in your downstream due to their noncompliance.

DFARS 252.204-7021 CLAUSE: CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) REQUIREMENTS

This DFARS clause establishes CMMC into the federal regulatory framework. This requires CMMC is to be included in all contracts, tasks or orders, and solicitations, with very few exceptions.

The level of CMMC required will be determined by the DoD and added to the request for proposal (RFP/RFQ). Contractors must maintain the appropriate CMMC level for the duration of any contract, and the requirements must be flowed down to their subcontractors and suppliers. The CMMC certification is required at the time of contract award.

CONSEQUENCES OF FAILING TO COMPLY WITH DFARS 7012 & NIST SP 800-171

Heat treaters willing to move forward with these cybersecurity initiatives by the DoD will have an overwhelming impact on the DoD supply chain and their business. Many heat treaters within the U.S. who will not embrace the mandatory requirements will result in the few who do become compliant being awarded the contracts by the DoD or their contractors.

Poor cybersecurity practices can result in hacking, potentially losing your data and your customers' critical data, being attacked by malware, viruses, and ransomware resulting in significant damage to your business, and you losing customers, not to mention being liable for all losses and paying significant fines.

This is neither a fast nor inexpensive process. NIST SP 800-171 compliance can take from between nine to 12 months. Achieving CMMC 2.0 certification can take between 12 to 18 months. So, starting now is very important.

CAN YOU AFFORD COMPLIANCE?

With the huge push for cybersecurity by the government, certain cost-sharing and funding sources have been identified who may cover a large percentage of the costs associated with these critical cybersecurity projects. Bluestreak Consulting™ can provide more information during the free consultation meeting, if interested.

ABOUT THE AUTHOR

Joe Coleman is the cyber security officer at Bluestreak Consulting™ and Bluestreak | Bright AM™. Coleman is also CMMC RP (Registered Practitioner) certified. He has more than 35 years of diverse manufacturing and engineering experience. His background includes extensive training in cybersecurity, a career as a machinist, a machining manager, a lead manufacturing engineer, and an early additive manufacturing (AM) pioneer. For more information, contact Coleman at joe.coleman@go-throughput.com or 513-900-7934.