Bluestreak | CONSULTING
Cybersecurity | Compliance
NIST + CMMC

DFARS/NIST SP 800-171 & CMMC

COMPLIANCE

WHO Needs To Be Compliant With DFARS NIST SP 800-171, And CMMC Certified

WHAT Steps You Need to Take Today!

WHEN Do You Need To Be Compliant/Certified

WHY The Importance of NIST 800-171 Compliance

WHO Needs To Be Compliant With DFARS/NIST SP 800-171 And CMMC

NIST SP 800-171 is a contractual requirement for the information systems of any non-federal entity (i.e., contractors, vendors, suppliers) that processes, stores, transmits, or protects Controlled Unclassified Information (CUI) for the Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA). Due to the sensitivity of and persistent security risks to CUI, all Government contractors who work with this type of information must follow the NIST SP 800-171 controls. Sub-contractors, vendors, and suppliers that may not contract directly with DoD or may not even handle CUI will be required, and many are already being required, by Prime contractors to meet compliance requirements.

WHAT What Is the DFARS 252.204-7012 Clause?

DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is a flow-down that obligates United States Department of Defense (DoD) prime contractors to ensure their operations and supply chains meet NIST SP 800-171 requirements. All covered contractor information systems not operated on behalf of the government were required to implement security requirements outlined in NIST SP 800-171 no later than December 31, 2017. But….it's not too late.

WHAT What Is the DFARS Interim Rule?

The DFARS Interim Rule went into effect on November 30, 2020. The DFARS Interim Rule and the three added clauses are an extension of the original DFARS 252.204-7012 clause that has been required in DoD contracts since 2018.

The DFARS Interim Rule implements the NIST 800-171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC). The three new clauses in the DFARS Interim Rule are:

- 252.204-7019 clause: Notice of NIST SP 800-171 DoD Assessment Requirements. DFARS 7019 mandates you perform a self-assessment of your networks and systems.
- 252.204-7020 clause: Lays out the actual requirements of your self-assessment.
- 252.204-7021 clause: Introduces the requirements you will need to become CMMC Certified.

WHAT What Is NIST SP 800-171?

Complying with NIST 800-171 is a requirement for all DoD contractors or anyone within their supply chain. Not adhering to NIST 800-171 doesn't just mean you're practicing poor cybersecurity methods; it also means you risk losing out on current and future business.

NIST 800-171 outlines five core cybersecurity areas; which are... Identify, Protect, Detect, Respond, and Recover. These core areas serve as a framework for developing an information security program that protects CUI and mitigates cyber risks. NIST 800-171 requirements consist of 110 security controls corresponding to 14 control families ranging from access control (AC) to system and information integrity (SI). Within the 110 security controls, there are 320 control/assessment objectives that are to be met in order to become fully compliant.

WHAT What Is CMMC? (Cybersecurity Maturity Model Certification)

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's (DoD) newest verification mechanism designed to ensure that cybersecurity controls and processes adequately protect Controlled Unclassified Information (CUI) that resides on Defense Industrial Base (DIB) systems and networks.

The security controls required to be implemented by the DFARS are defined within NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

There are 3 Levels of CMMC certification:

- **Level 1 – Foundational:** This level includes basic cybersecurity appropriate for small companies, that do NOT handle CUI, utilizing a subset of universally accepted common practices. This level also includes 17 controls from NIST 800-171.

- **Level 2 – Advanced:** This level includes coverage of all 110 NIST SP 800-171 Rev. 2 controls. Level 2 Advanced requires recertification on a 3-year basis by an outside C3POA (CMMC Third Party Assessment Organization) versus an annual self-assessment.

- **Level 3 – Expert:** This level includes highly advanced cybersecurity practices. Details of this level are still being defined. It is expected that this level will incorporate all of Level 2 requirements and additional controls from NIST SP 800-172. Level 3 will be rolled out in the coming months.

This table breaks down the 14 Control Families, the number of Controls (110) within those Control Families, and the number of Control/Assessment Objectives (320) within those Controls, all of which need to be assessed during your self-assessment.

Bluestreak CONSULTING™ Cybersecurity | Compliance NIST + CMMC

NIST SP 800-171

	Control Family	Abbr.	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
		Total	**110**	**320**

WHY The Importance of NIST SP 800-171 Compliance

If you're not already DFARS 252.204-7012 and NIST 800-171 compliant, NOW is the time to get started to avoid losing current and future business.

Many DoD contractors are seeing requirements on contracts stating "DFARS Compliant". This means all deliverables must meet the DFARS 252.204-7012 and NIST 800-171 Compliance requirements.

There are a lot of companies and downstream service providers that are either having current contracts canceled due to not being compliant or are eliminated from being awarded future contracts until compliance has been proven.

Even if your company does not fall within the DoD supply chain or doesn't handle CUI at all, NIST 800-171 is a great cybersecurity best practice to have for protecting both your data and your customer's data, and it sets you up to acquire future business. You don't need to have CUI to become NIST-800-171 compliant.

6 Essential Steps Towards Compliance

STEP 1:
Ask for Help

Through the process of implementation, a company may encounter several roadblocks such as: time, money and know-how. With the help of a qualified consultant, you can expect to save time and money. Relying on their expertise guides you through the process in the most efficient way.

What to look for in a consultant:

- A consulting firm that will guide your team through this complicated and confusing process from beginning to end, taking into account anything that you may have already done.

- A qualified consultant who guides you through the pro cess with a lower hourly rate versus a MSP (Managed Service Provider) who does everything for you, and may have a conflict of interest.

- Make sure the consultant is able to train one or more of your team members who will become your in-house compliance expert(s).

- Look for a firm with experience implementing DFARS/ NIST 800-171 and CMMC with SMBs (small and mid-size businesses).

STEP 2:
NIST 800-171 Security Self-Assessment

According to requirement 3.12.1 of NIST 800-171, companies must periodically assess the security controls in their organizational systems to determine their effectiveness. The assessment should cover all 14 Control Families, all 110 Controls, and all 320 Control/Assessment Objectives.

You can use an Internal team, along with a consultant to guide you through the process of conducting this Basic Self-Assessment. Follow the NIST 800-171 Assessment Methodology, NIST 800-171A, and NIST HB-162 (Self Assessment Handbook) to meet the minimum requirements of DFARS 252.204-7012, 7019, & 7020. Then submit the resulting score through the SPRS (Supplier Performance Risk System).

STEP 3:
Create a Plan of Action and Milestones (POA&M)

Requirement Control 3.12.2 requires a POA&M to be created. If shortcomings are uncovered during the assessment or you are not in compliance with the associated control, companies must develop and implement a POA&M to correct these deficiencies and eliminate vulnerabilities in their systems. You will need to include the timeline of your remediation and implementation plan as part of the SPRS submission.

STEP 4:
Create a System Security Plan (SSP)

Per NIST 800-171 requirement 3.12.4, companies must develop, document, and periodically update their SSPs. This plan should describe your system(s) boundaries, operating environments, security measures, and relationships with or connections to other systems. Also, it must accurately reflect how you implemented each of the 110 controls & 320 control/assessment objectives. You will not be able to successfully submit your assessment score to the SPRS without a SSP.

STEP 5:
Report the DoD Assessment Score to SPRS

To be awarded a DoD contract, you must have a current assessment in SPRS. Your submission will need to include:

- The name(s) of the System Security Plan(s) (SSP)
- CAGE code associated with the contract
- A brief description
- Date of the self-assessment
- Date when all remediations and implementations will be completed

STEP 6:
Implement Controls and Execute the POA&M

Companies must remediate the issues identified during the Basic SELF-Assessment to achieve NIST 800-171 compliance. This step often requires a significant amount of time and effort, so plan your timeline and expectations accordingly.

For many suppliers, this remedial step can be a strain on their internal resources. However, delays can cause you to miss out on opportunities and leave money on the table. That's why many defense contractors choose to work with a third-party cybersecurity consulting service to guide them through the process to help implement the controls and achieve compliance.

Your consultant or external MSP should have experience implementing NIST 800-171 controls for businesses similar to yours (e.g., size, vertical) and a track record in solving the unique challenges of achieving NIST 800-171 compliance in the defense industry. One of the goals should also be helping you become CMMC audit ready.

They should have the capabilities to execute complex controls in manufacturing, lab, and engineering environments and ensure that your SSP is updated to reflect the final implementation.

BUDGETING For DFARS & NIST Compliance

A contract with the federal government can be a lucrative opportunity, but if you're facing a fixed budget with small margins, it's in your best interest to hire a qualified consultant to help perform a full review of your existing infrastructure to help ensure you're fully equipped and positioned to maximize profitability.

Most CUI information doesn't need to be classified as sensitive enough to require a high level of security clearance, but that doesn't mean it should be visible or accessible by the public. As NIST 800-171 states, contractors need to make a complete review of all information systems where CUI is stored, processed, or transmitted and review security measures in place to protect this information.

COST SHARING Financial Assistance Available for Compliance

Cost sharing is an option that may be available. There are cost saving measures for many companies in various states, that cover a certain percentage of the cost, if not all the cost, associated with this critical project. So, there's no excuse to not being compliant. Contact Bluestreak Consulting™ for more details regarding financial assistance.

ABOUT Bluestreak Consulting™

Bluestreak Consulting™ is a division of Throughput Consulting, Inc.™, a sister company to Bluestreak | Bright AM™. Bluestreak Consulting™ was launched to help SMBs (Small to mid-sized businesses) achieve DFARS/NIST 800-171 compliance and help you become CMMC audit ready at a lower hourly consulting rate. Bluestreak Consulting™ specializes in helping businesses like yours achieve compliance in an affordable and efficient way.

Bluestreak Consulting™ can help your business meet all requirements by helping your team conduct the necessary security and risk assessments required as part of NIST SP 800-171. We'll help identify any security gaps in your systems or processes that may not meet the DFARS regulations, and work with your team to develop a remediation plan. Our team of qualified consultants will guide you through the many in-depth security requirements and solutions needed to obtain and maintain your DFARS compliance.

If your business needs to achieve DFARS compliance and fulfill other regulatory compliance policies such as ISO, ITAR, Nadcap, AS9100, etc., contact us to set up a free consultation.

SERVICES Bluestreak Consulting™ Provides Guidance:

Bluestreak Consulting™ utilizes proven methods to help ensure your implementation process is successful. Bluestreak Consulting™ will guide you through the following implementation areas to achieve compliance:

- Assessing your current environment
- Identifying and protecting CUI (Controlled Unclassified Information)
- Gap Analysis
- Remediation and Implementation Planning
- System Security Plan(s) (SSP)
- Plan of Action & Milestones (POA&M)
- Policies, Procedures, and Processes for all controls & other required documents
- Comprehensive compliance plan
- Self-Assessment/Attestation
- Submitting your Score to SPRS (Supplier Performance Risk System)

Bluestreak Consulting™ will also assist in the following areas for continued compliance status:

- Re-Assessing your environment when it changes or is updated
- Updating your SSP, POA&Ms, and SPRS Score
- Implementing changes as needs and technologies evolve
- Operating and maintaining a secure and compliant IT environment
- Conducting regular internal system audits in multiple areas

Bluestreak Consulting™ also offers:

- Detailed project plan including all tasks, activities, and deliverables
- Full set of templates for Policies, Procedures, and required documents
- Basic DFARS/NIST and CMMC training for your implementation team
- Tracking tools to keep you both on schedule and on budget

Your complimentary consultation includes:

- Discussing your needs and understanding your company processes
- A high-level overview of DFARS, NIST SP 800-171, and CMMC
- Discussing and answering any questions you may have

Bluestreak | CONSULTING™
Cybersecurity | Compliance
NIST + CMMC

CYBER AB CMMC CERTIFICATION
REGISTERED PRACTITIONER

Joe Coleman
Certified CMMC RP,
Registered Practitioner
(Cyber AB)

go-bluestreak.com
joe.coleman@go-throughput.com
513-900-7934