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 Comply With DFARS, NIST SP 800-171, and CMMC

DoD prime contractors and subcontractors that process, store, or transmit Controlled Unclassified Information (CUI) must comply with the minimum DFARS 252.204-7012 standards if they provide products or services to the Department of Defense (DoD), whether directly or indirectly. To achieve these standards, DFARS 7012 states that organizations must follow and implement the control requirements within NIST SP 800-171 Rev 2.

A common misconception that many companies have is that even though they are ISO 9001, AS9100, ITAR Registered, or NADCAP Accredited, they are still obligated by the DoD and DFARS 7012 to achieve NIST SP 800-171 compliance and CMMC certification as soon as possible. However, they most definitely are!! Failure to do so could result in the risk of losing both current and future contracts.

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 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. Many organizations are somewhere on the path to compliance, and if your organization is not actively working towards compliance, you are way behind your competitors. But…it's not too late.

WHAT What Is NIST SP 800-171 Rev 2?

NIST SP 800-171 is a contractual requirement for the information systems of any non-federal organization that handles CUI in any way, whether digitally, physically or otherwise.

NIST SP 800-171 is a NIST (National Institute of Standards and Technology) Special Publication that provides recommended requirements for protecting the confidentiality of CUI.

Defense contractors, subcontractors, vendors & suppliers must be able to demonstrate their provision of "adequate security" to protect CUI included as part of their defense contracts, as required by DFARS 7012. If a downstream organization is part of a DoD, General Services Administration (GSA), National Aeronautics and Space Administration (NASA) or other federal or state agencies' supply chain, the implementation of the security requirements included in NIST SP 800-171 is a must.

NIST SP 800-171 outlines five (5) core cybersecurity areas; Identify, Protect, Detect, Respond, and Recover. These core areas serve as a core framework for developing an information security program that protects CUI and mitigates cyber risks.

NIST SP 800-171 requirements consist of 110 security controls corresponding to 14 control families, ranging from 3.1 Access Control to 3.14 System & Information Integrity. Within the 110 controls, there are 320 control/assessment objectives that need to be met in order to be considered compliant.

WHAT What Is The DFARS Interim Rule?

The DoD released the DFARS Interim Rule in September 2020, which went into effect on November 30, 2020. Its primary objectives are to clarify that CMMC will be the new framework for DoD contracts and inform contractors they are responsible for reporting their compliance with NIST SP 800-171.

The dual mandates (NIST and DFARS) allow the Interim Rule to address defense contractors' security and compliance gaps in preparation for the CMMC rollout.

The Interim Rule's primary changes are adding three new clauses, including 252.204-7019, -7020, and -7021.

- DFARS clause 252.204-7019 notifies the contractor that they are required to maintain a record of their NIST 800-171 compliance within the Supplier Performance Risk System (SPRS). This means that each contractor will need to have a Basic, Medium, or High assessment completed at least every three years and ensure it is properly reported to the SPRS.
- DFARS clause 252.204-7020 requires contractors to provide the Government access to its facilities, systems, and personnel any time the DoD is renewing or conducting a Medium or High assessment.
- DFARS clause 252.204-7021 requires DoD contractors to maintain the appropriate CMMC level with respect to each contract, while also ensuring any subcontractors are compliant to the same CMMC level for the duration of the contract.

WHAT What Is CMMC 2.0?

The Cybersecurity Maturation Model Certification (CMMC) is the DoD’s newest verification mechanism designed to ensure that cybersecurity controls and processes adequately protect CUI that resides on nonfederal organizations’ systems and networks which are considered part of the Defense Industrial Base (DIB), which would include all downstream service suppliers that have CUI.

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

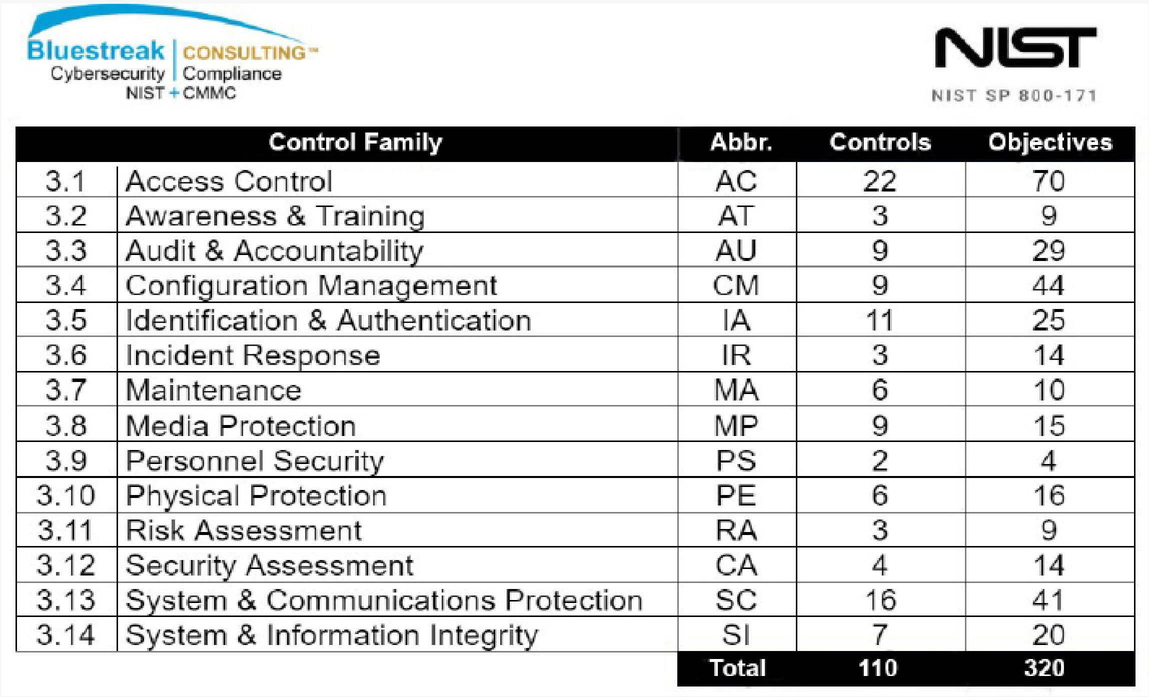
CMMC 2.0 consists of 3 levels:

- **Level 1 – Foundational:** Includes basic cybersecurity appropriate for small companies utilizing a subset of universally accepted common practices. This level includes the same 17 controls outlined in the original CMMC framework, but now only requires an annual self-assessment and affirmation by company leadership. This level is appropriate for companies who handle Federal Contract Information (FCI) and do not handle CUI.

- **Level 2 – Advanced:** Includes coverage of all 110 of NIST SP 800-171 Rev. 2 controls. Level 2 Advanced requires certification by a CMMC Third Party Assessment Organization (C3PAO) and recertification on a 3-year basis by an outside C3PAO versus an annual self-assessment. This is the minimum level for companies who handle CUI in any way.

- **Level 3 – Expert:** This level includes highly advanced cybersecurity practices. The processes involved at this level include using the tools available for continuous improvement across the organization's security practices, both digital and physical, in order to protect CUI. Details of this level are still being defined. It is expected that this level will incorporate a subset of controls from NIST SP 800-172 where a company will have an existing Level 2 certification, and the Level 3 controls will be assessed by DoD and not by a C3PAO.

This table delineates the 14 Control Families, the 110 Controls within those Families, and the 320 Control/Assessment Objectives associated with those Controls. All of these elements must be assessed and met to achieve compliance.



Bluestreak | CONSULTING™
Cybersecurity | Compliance
NIST + CMMC

NIST
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 Why Is DFARS, NIST SP 800-171, and CMMC Compliance So Important?

Compliance is a requirement, not an option. If you’re not already compliant with DFARS 252.204-7012, NIST SP 800-171 Rev 2., and CMMC 2.0, NOW IS THE TIME. The combined importance of these three security frameworks lies in the fact that they establish a comprehensive security framework for companies involved in the defense contracts. Meeting these requirements not only ensures compliance with regulations but also helps safeguard sensitive data, strengthens national security, and maintains the integrity of defense operations. Noncompliance can result in the loss of current and future contracts, reputation damage, and potential legal and financial consequences. So, being DFARS, NIST SP 800-171 compliant, and CMMC certified is crucial for any company operating in the defense industrial base (DIB) to demonstrate its commitment to security and its eligibility for DoD contracts.

Even if the company does not fall within the DIB or doesn’t handle CUI at all, NIST SP 800-171 is a great cybersecurity best practice for protecting both your data and your customer’s data.

6 Essential Steps Towards Compliance

STEP 1:
Ask for Help

During the implementation process, a company might encounter various obstacles, including issues related to time, finances, and expertise. Hiring the services of a proficient consultant can lead to a notable time and cost savings. Relying on their specialized knowledge will efficiently navigate you through the process or possibly even serve as project manager of the compliance effort, delegating certain tasks as needed.

Key considerations when selecting a consultant:

- Choose a consulting firm that provides comprehensive guidance to your team throughout this complex journey, have already made.
- Opt for a qualified consultant who provides guidance or complete leadership at a more affordable hourly rate compared to an MSP (Managed Service Provider) that handles all IT and cybersecurity tasks, potentially leading to conflicts of interest or short cut assumptions.
- Ensure that the consultant can train one or more of your team members to become adept in-house compliance expert(s).
- Give preference to a firm with a track record of success fully implementing DFARS, NIST SP 800-171 and CMMC frameworks within small/mid-size businesses (SMBs).

STEP 2:
NIST SP 800-171 Security Basic Assessment

As per requirement 3.12.1 of NIST SP 800-171, companies are obligated to conduct periodic or annual assessments of the security controls within their organizational systems to ascertain their effectiveness. This assessment must encompass all 14 Control Families, all 110 Controls, and all 320 Control/Assessment Objectives.

To execute this Basic Assessment, you can engage an internal team in conjunction with a consultant. This collaborative effort will guide you through the assessment process. Adhere to the NIST SP 800-171 Assessment Methodology, NIST SP 800-171A, and NIST HB-162 (Self-Assessment Handbook) to fulfill the minimum requirements outlined in DFARS clauses 252.204-7012, 7019, and 7020. Once complete, submit the resulting score to the SPRS (Supplier Performance Risk System).

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

Requirement control 3.12.2 mandates the creation of a POA&M. In the event that deficiencies are identified during the assessment or noncompliance with the relevant control is detected, companies are obligated to formulate and execute a POA&M. This plan is designed to rectify these deficiencies and eradicate vulnerabilities within the appropriate systems. As part of the SPRS submission, it is imperative to incorporate the timeline for your remediation and implementation strategy.

STEP 4:
Create a System Security Plan (SSP)

In accordance with NIST SP 800-171 control 3.12.4, companies are obligated to create, record, and regularly revise their SSP’s (System Security Plans). This plan needs to outline the boundaries of your system(s), operation contexts, security measures, and interactions with or linkages to other systems. It must also precisely depict how each of the 110 controls and 320 control/assessment objectives are executed. A successful submission of your assessment score to the SPRS will be rejected without a completed SSP.

STEP 5:
Submit the Assessment Score to SPRS

In order to secure a DoD contract, a current assessment score in SPRS is a prerequisite. Your submission should encompass the following details:

- The name(s) of the System Security Plan(s)
- The CAGE code linked to the contract(s)
- A brief description of system(s) assessed
- The projected date for the completion of all POA&M remediation tasks and implementation efforts.

STEP 6:
Implement Controls and Execute the POA&M

Companies are required to address and rectify the issues identified during the assessment to achieve NIST SP 800-171 compliance. This phase often demands a substantial investment of cost, time and effort, so plan your timeline and expectations carefully. The completion date you submitted to SPRS is a firm and committed to date by your company.

The chosen consultant or external MSP should possess a history of implementing NIST SP 800-171 controls within companies similar to yours (e.g., in terms of size and industry vertical). They should also demonstrate a proven ability to address the distinct challenges associated with achieving NIST SP 800-171 compliance in the DIB. Another focal point should be their preparing you for CMMC audits.

Also, they must exhibit the capacity to handle intricate controls across manufacturing, laboratory, and engineering environments. Their expertise should include ensuring that your SSP is meticulously updated to mirror the final implementation.

BUDGETING For DFARS & NIST Compliance

A contract with the federal government can offer substantial profit potential. However, if you are constrained by a fixed budget and narrow profit margins, it is advisable to engage a qualified consultant. They can conduct a basic assessment of your existing infrastructure, ensuring you are well prepared and positioned to optimize profitability.

While a significant portion of CUI might not require classification as sensitive enough to necessitate a high level of security clearance, this does not imply that it should be accessible by the public. As outlined by NIST SP 800-171, contractors are obligated to thoroughly review all information systems containing, processing, storing, or transmitting CUI. This review should encompass evaluating the efficacy of existing security measures in place to safeguard this information.

COST SHARING Financial Assistance May Be Available for Compliance Efforts

Cost Sharing is an option that may be available. Numerous companies across different states have implemented cost-savings strategies that include a portion, if not the entirety, of the expenses linked to this important project. Consequently, there are no valid reasons for noncompliance.

Reach out to Bluestreak Consulting™ to obtain further insights into potential 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 assist small to mid-sized businesses (SMBs) in achieving DFARS/NIST SP 800-171 compliance and preparing them for CMMC audits at a reduced hourly consulting rate. Bluestreak Consulting™ specializes in helping businesses like yours achieve compliance affordably and efficiently.

Bluestreak Consulting™ can support your business in meeting all requirements by aiding your team or leading the project in conducting the necessary security and risk assessments outlined in NIST SP 800-171. We will identify any security gaps in your systems or processes that may not meet DFARS regulations and collaborate with your team to create a remediation plan. Our team of qualified consultants will either guide your team through the comprehensive security requirements and solutions, or lead the entire project, required to obtain and maintain DFARS compliance.

If your business needs to achieve DFARS, NIST SP 800-171, or CMMC compliance and meet other regulatory requirements, please contact us to arrange a free consultation.

SERVICES Bluestreak Consulting™

Bluestreak Consulting™ employs established methodologies to ensure the success of your implementation process. Bluestreak Consulting™ can either lead your project or provide guidance across the following implementation domains to attain compliance:

- A high-level evaluation of your existing IT and general security environment
- Performing a complete assessment of all Control Families, Controls, and Control/Assessment Objectives
- Providing a detailed post-assessment report with recommendations
- Identification and safeguarding of CUI
- Conducting a Risk Assessment (person, process, device, etc.)
- Development of System Security Plan(s) - (SSP)
- Creating a Plan of Action & Milestones (POA&M)
- Strategizing Remediation and Implementation plan
- Formulation of Policies, Procedures, and Processes for all controls and other required documentation
- Creation of a comprehensive compliance plan
- Conducting a Basic Self Assessment/Attestation
- Submission of your assessment score to SPRS

Bluestreak Consulting™ Will Also Assist in the Following Areas for Continued Compliance Status:

- Conducting a reassessment of your environment when changes or updates occur
- Implementing changes in response to evolving needs and technologies
- Ensuring the updating of your SSP, POA&Ms, and score to SPRS
- Operating and maintaining a secure and compliant IT environment
- Conducting routine internal system audits across multiple areas

Bluestreak Consulting™ Also Offers:

- A Comprehensive project plan detailing all tasks, activities, and deliverables
- A Complete set of templates for Policies, Procedures, and necessary documents
- Essencial DFARS, NIST SP 800-171, and CMMC training for your implementation team.
- Tracking tools and regular updates to ensure adherence to schedule and budget constraints

Your Complimentary Consultation Includes:

- Discussing your requirements and gaining insight into your company's processes
- Providing a comprehensive overview of DFARS, NIST SP 800-171, and CMMC
- Addressing and answering any questions you may have
- Proposing Next Steps

Bluestreak | CONSULTING™
Cybersecurity | Compliance
NIST + CMMC

go-bluestreak.com

joe.coleman@go-throughput.com

513-900-7934