NORTH CAROLINA MILITARY BUSINESS CENTER

NEW DFARS INTERIM RULE

Definitions

- Defense Federal Acquisition Regulation Supplement (DFARS) – supplement to the Federal Acquisition Regulation that is specific to DoD contracts.
- DFARS 252.204-7012 – cybersecurity regulation requiring that defense contractors self-attest to compliance with NIST SP 800-171 ***if you touch CUI.***
- NIST SP 800-171: National Institute of Standards and Technology Special Publication that contains 110 cybersecurity controls.
- DFARS Interim Rule Case 2019-D-041 – amends the DFARS to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification to enhance the protection of unclassified information in the DoD supply chain. Effective Date: 30 Nov 2020

DFARS Interim Rule

- Amends DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting to implement the NIST SP 800-171 DoD Assessment Methodology
- Directs contracting officers to verify in the Supplier Performance Risk System (SPRS) that a company has a current assessment on record prior to contract award (for companies that have DFARS 252.204-7012 in their contract(s).
- Adds DFARS 252.204-7019 and DFARS 252.204-7020 - directs contracting officers to add these 2 new clauses to contracts.
- Adds DFARS 252.204-7021 - CMMC
- Does NOT apply to strictly COTS items or contracts below the micro-purchase threshold.

New DFARS Clauses

DFARS 252.204-7019

- Requires contractors to perform a self-assessment to NIST SP 800-171 using the DoD Assessment Methodology
- Results of the self-assessment must be uploaded to the SPRS
- Must have a current (not older than 3 years) Assessment on record in order to be considered for an award

DFARS 252.204-7020

- Requires contractors to provide the Government with access to its facilities, systems and personnel when it is necessary to conduct or renew a high-level assessment
- Requires contractors to ensure that applicable subcontractors also have the results of a current Assessment posted in SPRS prior to awarding a subcontract

DFARS 252.204-7021 - CMMC

- DFARS 252.204-7021 establishes the Cybersecurity Maturity Model Certification requirements. (discussed in a separate presentation)

DoD Assessment Methodology

- Enables strategic assessments at the entity (corporate) level – not by contract
- Provides a standard methodology for contractors to do a self-assessment (Basic Assessment) to NIST SP 800-171
- Provides a way to transition from DFARS 252.204-7012 to CMMC
- "***The requirement for the Basic Assessment would be imposed through incorporation of the new solicitation provision and the contract clause in new contracts and orders. As such, the requirement to have completed a Basic Assessment is expected to phase-in over a three-year period…***"

DoD Assessment Methodology

Assessments

Basic Assessment

- Self-assessment to 110 NIST controls
- Uploaded to SPRS prior to award
- Valid for 3 years
- Confidence level - low

Medium Assessment

- Performed by (DCMA)
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- Confidence level – medium
- DoD uploads results to SPRS

High Assessment

- Performed by (DCMA)
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- Confidence level – high
- DoD uploads results to SPRS

DoD Assessment Methodology - Scoring

- How to Score the Self-Assessment – a perfect score is 110, meaning the contractor has all 110 NIST controls in place.
- For every control that is not in place, subtract its value from 110 – see below

***NIST SP 800-171 DoD Assessment* Scoring Template**

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

Example: If my company is not compliant with controls 3.1.1 and 3.1.5, subtract 8 points from 110.

DoD Assessment Methodology - Scoring

Remember the contracting officer only sees your total score, not how you scored on each control.

So how does the DoD know if you're compliant with the controls that have more impact on the security of your network – the ones rated a "5" – without doing a Medium or High assessment?

DoD Assessment Methodology - Results

- Assessment results posted in SPRS are available to DoD personnel only and are protected. (Method for primes to check score of potential subs has not yet been established)
- The information below must be posted to SPRS

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

DoD Assessment Methodology - POAMS

- If any of the 110 controls are not in place, a Plan of Action and Milestones must be developed to show how you plan to implement the control and when the control will be in place.
- The date that a score of 110 will be achieved (uploaded to SPRS) should be the latest date on your POAMS.
- There has been no guidance on how long POAMS can be open.
- There has been no guidance regarding how many times scores can be uploaded to SPRS. Ideally companies would upload each time a POAM is closed and the score increased.

Assessment Costs

- Since the DFARS Interim Rule is based on the NIST controls in DFARS 252.204-7012, which is already in most contracts, the DoD is only considering the cost of the assessments to be allowable. In other words, any labor and equipment expenses incurred to achieve compliance to the 110 NIST controls is not considered an allowable cost and may not be billed to the customer.
- Contractors do not have to pay the assessors for Medium and High assessments; the expenses are all internal to the contractor.
- Because the assessments are valid for three years, the estimated costs are shown as yearly (amortized over the 3-year period).

Assessment Costs

Assessment	Cost/ Assessment	Annual Cost/ Entity	Total Unique Entities	Annual Cost All Entities
Basic	$75	$25	26,469	$655,637
Medium	$909	$303	444	$134,467
High	$50,676	$16,892	243	$4,104,756

Assessment Costs and CUI

- The DFARS Interim Rule amends DFARS 252.204-7012, which requires protection for CUI
- While assessments using the DoD Assessment Methodology aren't quite as expensive as CMMC assessments, ***the best way to avoid the expense is to not touch CUI. With less CUI being transmitted, the risk to national security is reduced.***
- Work with your contracting officer or prime to discuss ways of eliminating the need to process, store or transmit CUI.
- Primes should not flow down these requirements unless it is absolutely necessary for the subs/suppliers to touch CUI.

Post-Assessment

- Contractors have 14 days after a Medium or High Assessment to file a rebuttal or fix any issues found during the assessment.
- If you have open POAMS, work toward getting them closed out. Start with implementing the easiest and least expensive controls.
- If the system allows it, upload your score to SPRS each time your score improves.
- Remember – CMMC compliance is coming, so consider beginning to work toward CMMC Level 3 compliance. Fifteen contracts in 2021 will have CMMC requirements in them, and it is anticipated that 1500 companies in the supply chain will be affected.

Transitioning to CMMC

- Contractors that process, store, transmit or create CUI will be required to comply with CMMC Level 3 requirements at some point in the future - unless your company receives advanced persistent threats and needs to comply with a higher CMMC level.
- CMMC is a quality management system and maturity model for cybersecurity, so it involves much more than simply implementing controls. CMMC requires processes and procedures as well as a plan for continuous improvement – in other words it is a program.
- The next slide shows the additional 20 controls in CMMC Level 3 – over and above the 110 controls in NIST SP 800-171.

Transitioning to CMMC – 20 Additional Controls

AM.3.036	Define procedures for the handling of CUI data.
AU.3.048	Collect audit information (e.g. logs) into one or more central repositories.
AU.2.044	Review audit logs.
IR.2.093	Detect & report events.
IR.2.094	Analyze & triage events to support event resolution & incident declaration.
IR.2.096	Develop & implement responses to declared incidents according to pre-defined procedures.
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.
RE.2.137	Regularly perform & test data back-ups.
RE.3.139	Regularly perform complete, comprehensive & resilient data backups as organizationally defined.
RM.3.144	Periodically perform risk assessments to identify & prioritize risks according to the defined risk categories, risk sources & risk measurement criteria.
RM3.146	Develop & implement risk mitigation plans.
RM.3.147	Manage non-vendor supported products (e.g. end of life) separately & restrict as necessary to reduce risk.
CA.3.162	Employ a security assessment of enterprise software that has been developed internally, for internal use, & that has been organizationally defined as an area of risk.
SA.3.169	Receive & respond to cyber threat intelligence from information sharing forums/sources & communicate to stakeholders.
SC.2.179	Use encrypted sessions for the management of network devices.
SC.3.192	Implement Domain Name System (DNS) filtering services.
SC.3.193	Implement a policy restricting the publication of CUI on externally-owned, publicly accessible websites (FB, LinkedIn, Twitter, etc.)
SI.3.218	Employ spam protection mechanisms at information system access & entry points.
SI.3.219	Implement email forgery protections.
SI.3.220	Utilize email sandboxing to detect or block potentially malicious email

Recommendations

1. Review your current contract(s) to see if DFARS 252.204-7012 is referenced. Remember – just because the DFARS clause is referenced that doesn't mean you touch CUI. If you don't touch CUI, the clause is not applicable.
2. If you are unsure about CUI, review the CUI Registry Categories . If you're still unsure, work with your contracting officer. Your KO can send an email to the CUI Executive Agent for the DoD if they need help with CUI - osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil
3. If there is any doubt about CUI in your contract(s), get something in writing from your contracting officer. **CUI = $$ and Risk**
4. Perform a gap analysis. NC State University- Industry Expansion Solutions has developed a gap analysis tool for NIST SP 800-171. Link . Project Spectrum and CISA also have gap analysis tools.

Recommendations

4. Determine your score using the DoD Assessment Methodology.
5. Put a Plan of Action and Milestones in place for each control you have not implemented. (See links on last slide)
6. Upload your score to the Supplier Performance Risk System

- Most small and many medium-sized companies will need to find a consultant to assist with compliance. Keep in mind that IT and cybersecurity are two different disciplines, so your IT person/staff may not have the necessary expertise to implement all the controls. Several cybersecurity consulting companies have signed up on the NCMBC website. **These companies will not be vetted by the NCMBC, so it is important to take the time to vet these companies yourself.** Link

Recommendations

- Be wary of consulting companies that over-sell, advertise false and/or misleading information about the DFARS Interim Rule, and/or try to scare you into using their services
- Using a Cloud Service Provider (CSP) will not provide 100% compliance – it is NOT possible – particularly for CMMC. If a company promises 100% compliance, they do not understand the regulations. The defense contractor is responsible for compliance – which means you must thoroughly understand how the services the CSP provides helps maintain compliance and be able to prove it. CSPs that are FedRamp certified are very expensive.
- Contact Laura Rodgers at the NCMBC for questions about the DFARS clauses or compliance- rodgersl@ncmbc.us

DFARS Interim Rule – Important Links

- DFARS Interim Rule – Federal Register
- CUI Registry Categories – more information about CUI. Check each category, not just Defense.
- System Security Plan and POAM Templates – (templates are downloadable) NIST requires a System Security Plan (SSP) and Plans of Action and Milestones.

NORTH CAROLINA MILITARY BUSINESS CENTER

NEW DFARS INTERIM RULE