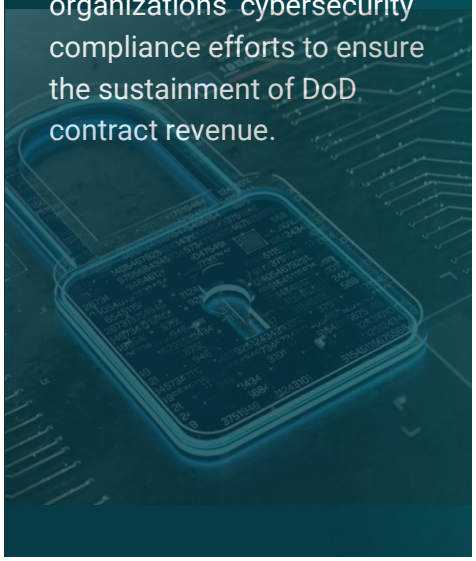
ankura

KEY TAKEAWAY

While the DoD charts a path forward on CMMC, the USG is emphasizing the need to comply with existing cyber obligations in government contracts and taking steps to enforce compliance with those obligations.

The June 16 Memo comes amid increased False Claims Act scrutiny pursuant to the DoJ's Civil Cyber-Fraud Initiative, the impending rulemaking enhancing CISA's role to oversee cyber incident reporting in critical infrastructure, and new requirements for federal contractors to demonstrate they securely develop software which will be used by federal agencies.

When read together, these developments should hasten organizations' cybersecurity compliance efforts to ensure the sustainment of DoD contract revenue.



DoD Re-Emphasizes Commitment to Holding Contractors Accountable on Cybersecurity

As the Defense Industrial Base ("DIB") awaits the final rule implementing the Cybersecurity Maturity Model Certification ("CMMC"), the US Government ("USG") is using other means at its disposal to ensure that DIB companies comply with existing contractual requirements to implement cybersecurity protections for Controlled Unclassified Information ("CUI"). The US Department of Defense ("DoD") recently reminded DIB contractors and subcontractors that compliance with DFARS 252.204-7012 and 252.204-7020 clauses is not optional.

In a memo released on June 16, 2022 (the "June 16 Memo"), the Office of the Under Secretary of Defense DoD for Acquisition & Sustainment ("OUSD A&S") outlined the applicability of these clauses and the consequence of non-compliance. Non-compliant contractors subject to 7012 or 7020 clauses can face "withholding progress payments; foregoing remaining contract options; and potentially terminating the contract in part or in whole." The June 16 Memo also directs the agency's contracting officers to verify that contractors have submitted scores under the proper assessment before awarding a new contract if there is a 252.204-7019 clause in the contract. Additionally, contracting officers, in consultation with the DIB Cyber Assessment Center ("DIBCAC"), may renegotiate a 252.204-7020 clause into contracts where one does not yet exist. Thus, even contractors not presently subject to a 252.204-7020 clause should understand potential compliance requirements to make informed decisions in such negotiations.

ankura

DFARS 252.204-7012 and 7020 Crash Course

DFARS 252.204-7012 sets forth the basic requirements for securing government information, requiring government contractors to provide “adequate security on all covered contractor information systems” operated by or for a contractor that process, store, or transmit covered defense information.

“Adequate security” is governed by the National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-171 (see side bar for more information). Exceptions must be requested by “writing to the Contracting Officer, for consideration by the DoD CIO.” Additionally, in DFARS 252.204-7012(c), there are cyber-incident reporting requirements. Finally, and importantly, DFARS 252.204-7012(m) has a flow down requirement such that subcontractors also must agree to comply with these cybersecurity requirements.

DFARS 252.204-7019 and -7020 define the assessment standards for compliance with DFARS 252.204-7012(b) (“Adequate Security”). There are three assessment levels: high, medium, and basic. A high assessment is conducted by government representatives using the DoD Assessment Methodology (including the assessment procedures of NIST SP 800-171A) and involves tasks such as document review, verification exercises, demonstrations, and interviews. A medium assessment requires a basic-level self-assessment and a high-level verification by government representatives. Basic assessments require contractors to conduct a self-assessment using NIST SP 800-171 DoD Assessment Methodology and to submit a summary score in the Supplier Performance Risk System (“SPRS”).

SPRS scores are posted by emailing the score through encrypted email to DoD. If the 252.204-7020 clause is not in a contract, contractors are not required to complete a High or Medium assessment. However, the contracting officer is required to ensure a SPRS score is posted before the award of any new contract. Contractors are required to flowdown 252.204-7019 and -7020 clauses and cannot grant work to a subcontractor with a SPRS score older than three years.

What is Adequate Security?

Covered contractors must implement NIST Special Publication (“SP”) 800-171 which contains 110 security requirements for protecting the confidentiality of CUI in non-federal information systems. Covered contractors also must ensure that any cloud service providers holding CUI data on their behalf meet FedRAMP Moderate Baseline (or equivalent) security requirements. This implies that companies will need strong third-party risk management practices.

More on SPRS Scores

The security requirements of NIST SP 800-171 are each given a numerical value of either one (42 controls), three (14 controls), or five points (54 controls) and that value is subtracted from a total score of 110 when a requirement is deemed as “not implemented”.

Scores can range from 110 (all requirements implemented) to -204 (no requirements implemented).

Note that the SPRS score is a representation to the DoD of your cybersecurity regardless of contract privity while the June 16 Memo only applies to contracts held with the DoD, the SPRS may imply downstream liability in the supply chain.

The Five-Step Process: Inventory, Assess, Remediate, Maintain, Audit

Compliance with FAR/DFARS cybersecurity requirements may seem like an insurmountable task, but the June 16 Memo reemphasizes the DoD's commitment to enforcing these requirements. If your organization is receiving or creating covered information subject to a contract with DFARS clauses, consider taking these important initial steps:

Conduct a data flow mapping and asset inventory.

The DFARS regulations only apply to covered contractor information systems, or "unclassified information system[s] that [are] owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information." Therefore, an organization can materially reduce the costs of NIST SP 800-171 compliance by limiting the environments where federal government data resides. Contractors also can optimize compliance efforts by identifying other compliance obligations (i.e., export controls) and ensuring implementation of common controls will satisfy both standards.

Conduct a current-state compliance assessment.

Whether you already have a SPRS score submitted, or require one, conducting a robust assessment is important to an organization's ability to plan an appropriate course of action. Whether it involves applying for an exception, creating a budget line item for remediations, standing up a Plan of Action and Milestones ("POA&M"), or changing strategic business direction, it is important to invest in an assessment up front so that leaders may choose the best course of action based on all available essential information. A POA&M should "describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented." Additionally, the assessment should involve feedback from all organization stakeholders. This means that it should not just be completed with input from the IT department, but rather from legal, operations, Human Resources, and other key departments as well.

Deliberately implement a POA&M and keep the document updated with progress.

The POA&M is an essential tool that can act as a bridge from identifying compliance gaps to achieving full compliance. Additionally, the June 16 Memo made it clear that "[f]ailure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements." It is essential that the POA&M is comprehensive and accurate. An adequate POA&M: 1) identifies deficiencies and vulnerabilities; 2) contemplates corrective action: and 3) is actually used by the organization for progressing its cybersecurity program. NIST SP 800-171 Table D-12 makes clear that a POA&M should be drafted in concert with the organization's System Security Plan ("SSP") (See Table D-12 grouping control group 3.12 with POA&M creation). The SSP

focuses on the current state of the compliance program while the POA&M focuses on the future state.

Even partially implemented controls should appear in a POA&M as partial implementation is not sufficient to satisfy a security requirement. An organization's POA&M should be sufficiently specific to satisfy DOD that the organization has a plan to remediate deficiencies and will be able to take steps toward remediation. Items that are prohibitive to remediate (due to operational or safety requirements) should **not** go in a POA&M but, instead, become an application submitted to the Contract Officer, then DoD for an exception.

Maintain and monitor.

Maintenance and monitoring are essential to ensuring covered information systems remain in compliance. This means an organization, depending on size, will need an independent internal audit or controls monitoring function. If a control ever fails to operate as intended or to produce the desired results with respect to the security and privacy objectives of the organization, then it should be added to a POA&M until the deficiency is remediated.

Plan for an audit.

Organizations would be well-advised to create an audit assurance package in the event they are subject to an audit. Keeping an up-to-date assurance package, for example in a GRC tool, can reduce operational stress on an organization in the event of an audit.

By following these five steps, organizations can ensure preparedness for obtaining DoD contracts (and subcontracts) and any potential government audits. This iterative process not only helps to bring organizations into compliance, but also helps them maintain a steady state of compliance. In addition, it incorporates feedback from essential stakeholders to ensure implementation comports with operational and legal requirements.

While the costs of achieving and maintaining DFARS compliance can seem daunting, it is critical to continuing to do business with the DoD and its contractors. Done right, DFARS compliance can become one of a company's biggest strengths and create a competitive advantage by enhancing a company's reputation and increasing the company's likelihood of securing work from DoD and its contractors. Done wrong or inadequately, as reiterated in the June 16 Memo, the consequences may be severe. Company's face risk of withheld payments and losing out on potential future contracts, both of which can materially impact cash flow. Compliance failures also threaten a company with material reputational harm in its current and future dealings with DoD and its contractors. As a result, actively maintaining DFARS compliance is critical for serious companies that want to continue to succeed when doing business with DoD.

How Ankura Can Help

Cybersecurity Program Assessment.

Ankura's experts have extensive experience assessing cybersecurity programs of all sizes to ensure compliance with DoD contract requirements and the NIST SP 800-171 and 800-171A. A credible independent assessment will ensure that your organization has an accurate picture of its current cybersecurity posture to support effective compliance and remediation efforts.

Governance Program Design and Implementation.

Ankura's team of former prime contractor compliance executives, in-house counsel, export control attorneys, and cybersecurity experts are perfectly placed to help defense contractors design, implement, and enhance compliance programs answerable to multiple regulated data requirements, including Controlled Unclassified Information. Ankura has helped numerous clients build right sized, cost effective, and accountable compliance programs which have helped companies win and sustain lucrative work in the defense supply chain.

POA&M Documentation and Management.

Ankura's NSTT team routinely serves as a force multiplier for organizations attempting to meet their DFARS contract requirements under tight deadlines. Pursuant to an independent assessment, Ankura's experts will work with company personnel to effectively document POA&Ms to ensure timely and effective remediation. Expert, third-party assurance can be key to reaching and maintaining compliance.

Technical Remediation.

Ankura will work with company personnel as well as identified third-party firms to design and implement the technical remediations required to meet NIST SP 800-171 security requirements. From infrastructure migration to network architecture design, Ankura's team will provide the experienced professional oversight to make sure that technical implementations effectively meet security requirements.