Articles + Publications | October 8, 2024

Federal Cybersecurity Requirements Ought Not Be Ignored by Contractors

WRITTEN BY

Daniel Waltz | Bonnie Gill | Timothy L. McHugh | Hilary S. Cairnie

1. The Real Risk of Cybersecurity: Choosing to be Unaware

Since 2016, the federal government has implemented numerous procurement regulations and associated contract clauses to address cybersecurity by requiring contractors to adopt various controls and standards to protect sensitive, unclassified information, and to harden information technology (IT) systems to make them more resilient to all manner of cyber hacks. The easy part (not that it was at all easy) was developing the controls and standards – NIST SP 800-171 (currently up to Rev. 3), and contract clauses (most notably, FAR 52.204-21, and DFARS 252.204-7012, 7019, 7020, 7021, and others). The difficult part is getting contractors to take seriously the obligation to invest in cybersecurity.

According to the Government Accountability Office (GAO), during the period 2015-2021, the DOD and the Defense Industrial Base (DIB) reported more than 12,000 detected "cyber incidents."[1] While that figure might seem quite small at first glance, it really is the tip of the iceberg. As discussed more fully below, by contract clause, contractors are obligated to report "cyber incidents" and take a host of actions following the detection of a cyber incident.

The operative word is "detection." Before the contractor can fulfill its obligation to report a cyber incident, the contractor must first be in a position to actually detect a cyber incident. In order to detect a cyber incident, the contractor must have a reasonably robust framework of IT controls, monitoring and detection procedures, and effective communication protocols and reporting functions. In other words, the contractor must have an effective cybersecurity program. As gauged against DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting (May 2024), most contractors simply do not have an effective cybersecurity program. Many contractors have bits and pieces of a cyber security program, for example, they may have prepared a Project Objectives and Milestones (POAM) tracking tool, but progress toward achieving objectives and milestones has effectively stalled.

Having a POAM is just not enough. Contractors must make measurable progress year over year toward filling in cyber security gaps. In the absence of a reasonably robust cyber security program, it is to be expected that many thousands of hacks, phishing attacks, malware intrusions, ransomware attacks, trojan horses, and similar IT system intrusions, are going undetected by contactors every day, for weeks, maybe months and possibly years. So, now is a good time to take a fresh look at the cybersecurity framework that, perhaps, the majority of government contractors are subject to whenever they receive a prime contract or accept a subcontract in support of someone else who is the prime contractor.

2. Cybersecurity Regulations for Federal Contractors – FAR and DFARS

a. FAR 52.204-21 – Basic Safeguarding of Covered Contractor Information Systems (NOV 2021)

FAR 52.204-21 establishes a baseline of fifteen (15) basic cybersecurity controls for contractor IT systems which store, transmit, or process "federal contract information." Federal contract information is information received from or generated for the federal government in the performance of a procurement contract. These 15 baseline cybersecurity controls correspond to Level 1 security under the Cybersecurity Maturity Model Certification (CMMC) program, which is inching aver forward toward realization and implementation (more about that below).

Under FAR 52.204-21, federal contract information is defined as any information, not intended for public release, which is provided by or generated for the government under a contract to develop or deliver a product or service to the government. These "safeguarding requirements" include controls relating to user access, authorization, appropriate information disposal, system protection, system scanning and logging, among others. Rather than list all such controls, the contractor is encouraged to review the clause as it appears in their federal contracts.

Many contractors that perform civilian agency contracts also participate in DOD contracts, and that subjects them to an even more robust set of requirements. Must a contractor comply with both of these cybersecurity clauses (FAR and DFARS) if they are included in one or more contracts? Where the contractor is subject to the DFARS clause, even if just in one contract, it must comply with that clause and, in so doing, it will also comply with the less extensive set of controls established in FAR 52.204-21. Of course, the savvy contractor will closely review its performance deliverables (COTS?) to determine whether the clause has mistakenly been included in the contract (*see* FAR 4.1902).

b. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)

Since 2017 the DOD has implemented its cybersecurity requirements through DFARS 252.204-7012. Among other things, the DOD clause requires contractors to satisfy each of the 110 cybersecurity controls established in NIST SP 800-171 (currently, Rev. 3) – .Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The DOD clause and NIST SP 800 171, in combination, are directed at protecting all manner of unclassified covered defense information (CDI), such as Controlled Unclassified Information (CUI) or Controlled Technical Information (CTI) that is received, generated, transmitted and/or stored on "covered contractor" information systems. Such a system is broadly defined to include "an unclassified information system that is owned, or operated, by or for a contractor and that receives, processes, stores, or transmits" CDI. DFARS 252.204-7012(a). In a perfect world, at the time of award and going forward, the contracting agency is, theoretically, supposed to identify various categories of information that is to be treated as CUI or CDI during the life of the contract. Practically speaking, contracting agencies have struggled to timely and/or adequately inform contractors of the categories of information that are to be covered as CDI or CUI leaving contractors with no choice but to chase agency officials for guidance and direction.

There are several other DOD cybersecurity clauses that also may be applicable, such as the following:

DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (OCT

2016). This is a solicitation provision requiring contactor to include as part of its offer a representation that it will implement the security requirements specified in NIST SP 800-171 not later than December 31, 2017, or timely request a variance therefrom. DoD is required to adjudicate a request for variance before the contract is awarded. Contractors routinely miss this solicitation provision, or they will elect to provide the representation in their offer without knowing whether their IT systems timely achieved compliance with NIST SP 800-171, arguably a basis for an alleged misrepresentation.

DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (NOV 2023). This is a relatively new solicitation provision required anytime the contract will involve CDI. The requirement embodied in this provision appears to be mandatory, as follows:

(b) Requirement. In order to be considered for award, **if** the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology (Emphasis added).

Chances are very good that if the solicitation includes DFARS 252.204-7012, that DOD is not procuring COTS-only supplies or services, and as such, the contractor must comply with NIST SP 800-171 and must have a current assessment (basic, medium, or high) under that specific standard. If, during the evaluation, selection, and award of the contract it is determined that the contractor does not have a current assessment, it may be ineligible for award.

DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements (NOV 2023). This too is a relatively recent clause required for inclusion in the solicitation as well as the resulting contract. It requires contractors to periodically provide DoD with a summary level score of their compliance with NIST SP 800-171 for each relevant covered contractor information system, and to flow-down to lower tier contractors the same reporting obligations. The contractor must also provide the government with access to its facilities, systems, and personnel when it is necessary for the DoD to conduct or renew a higher-level assessment.

c. Cybersecurity Maturity Model Certification (CMMC)

While the DOD's CMMC Program moves ever closer to final implementation, it is not yet in final form for contract implementation. In September 2024, the Office of Management and Budget (OMB)'s final rule as rendered on June 27, 2024, made its way through the interagency review process via OMB's Office of Information and Regulatory Affairs (OIRA) and was approved by OIRA on Sept. 13, 2024. That rule will eventually be published at 32 CFR thereby making CMMC an official DOD program.

There is also a proposed rule also concerning CMMC which is currently receiving public comment through October 15, 2024. That proposed rule makes changes to DFARS provisions pertaining to CMMC, and this proposed rulemaking need not be finalized in order for DOD to be able to officially launch CMMC as an active program. Some may recall that the Biden administration paused the CMMC program initiative in 2021 to allow for additional review and adjustment. It is an open question whether a change in administration will elect to implement CMMC in its then present form or choose to make additional changes or scrap it all together. For the moment, there is a

DOD solicitation and contract clause establishing CMMC requirements:

DFARS 252.204-7021, **Cybersecurity Maturity Model Certification Requirements (CMMC) (JAN 2023)**:

(a) Scope. The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes.

(b) Requirements. The Contractor shall have a current (i.e., not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) Subcontracts. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

Apparently, DOD is not yet enforcing the CMMC clause, which is to say, even though it is required to be included in solicitations and contracts, DOD in its buying activities is electing not to include the clause or, if included, choosing not to police contractors in connection with current CMMC certifications.

---

[1] NOV 2022, DOD Cybersecurity – Enhanced Attention Needed to Ensure Cyber Incidents are Appropriately Reported and Shared.

RELATED INDUSTRIES + PRACTICES

- Government Contracts
- Privacy + Cyber