Global Regulatory Enforcement Law Blog

Updates and analysis on global regulatory and enforcement issues

Riding the cybersecurity compliance wave: How defense contractors can navigate the rising tide of cybersecurity regulations


By Elizabeth Leavy and Liza Craig on 23 September 2019
Posted in Data Security, Privacy & Management, Government Contracts & Grants

Cybersecurity attacks targeting government information have drastically increased, and both the federal government and private industry have struggled to implement effective means of protecting this information. Federal agencies continue to strive for a unified approach to protect critical data; however, the various regulations leave contractors without a clear set of requirements that are applicable to all government contracts. Contractors can easily get lost in the alphabet soup of cybersecurity requirements, whether they be in the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), National Institute of Standards and Technology (NIST) publications, or the upcoming Cybersecurity Maturity Model Certification (CMMC). To aid some of that confusion, in this post we address: (a) the current cybersecurity regulations applicable to defense contractors, (b) the tentative cybersecurity certification program proposed by the Department of Defense (DoD) and new regulations imposed by the Department of Navy (DoN), and (c) what contractors can do now to ensure compliance with the ever-changing regulatory framework. Notwithstanding the implementation of these regulatory requirements, cybersecurity attacks and breaches continue to be a reality. Consequently, the search for ways to increase cybersecurity measures continues to be a priority.

How did we get here?

Without question, the DoD has been on the front line battling against cybersecurity threats in recent years. The Department has established regulatory frameworks to protect U.S. interests and codify cybersecurity responsibilities and procedures in defense acquisition policy. Using security controls published by NIST, in 2013 the DoD implemented a final rule which was incorporated into DFARS 252.204-7012. This DFARS clause applies to all DoD contracts for the acquisition of commercial items, other than commercial off-the-shelf (COTS) items. As it reads today, the DFARS clause imposes an affirmative obligation on defense contractors to implement information security protections to their own information services and systems that are consistent with the NIST standards. Thus, defense contractors are required to review and implement all the security measures that are expressly set forth in NIST Special Publication 800-171.

How are the regulations changing?

The DoD has once again taken the lead by expanding upon existing cybersecurity requirements imposed by the NIST and DFARS. The DoD has announced that it is working to develop the CMMC framework, through which all defense contractors will be required to obtain certification. Through CMMC certification, the DoD seeks to verify that contractors have employed appropriate levels of cybersecurity controls and processes to protect controlled unclassified information (CUI) that is housed on contractor systems.

The CMMC framework is intended to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB), and will require demonstrated contractor capabilities across a number of technical areas. CMMC differs from existing requirements in that the DoD will engage independent third-party evaluators to assess and measure each company's

Search

STAY CONNECTED

SUBSCRIBE

Subscribe to our mailing list

TOPICS

Antitrust & Competition
Data Security, Privacy & Management
Financial Regulation
Financial Regulatory
Government ContractoRx Corner
Government Contracts & Grants
Government Investigations & White Collar Criminal Defense
International Trade & National Security
Public Policy & Infrastructure
Securities Litigation & Enforcement
Uncategorized

RECENT UPDATES

Riding the cybersecurity compliance wave: How defense contractors can navigate the rising tide of cybersecurity regulations
The Securities Commission Malaysia announces new anti-corruption action plan – what does this mean for listed companies?
CNIL imposes hefty sanction on French company under GDPR
French Council of State Confirms GDPR Sanction, Lowers Penalty Fee
Recent 'firsts' shape UK collective actions

REED SMITH SITES

AdLaw By Request
Antitrust and Competition Update

maturity/institutionalization of cybersecurity practices and processes. The independent third party will certify each company based on the maturity level (1–5) that it deems appropriate based on the organization's level of maturity and capabilities. Level 1 equates to "basic cybersecurity" which is designed to be achievable for small businesses. Level 2 means the contractor has incorporated "universally accepted cybersecurity best practices." Level 3 is consistent with the NIST SP 800-171 controls, and therefore any contractor that is currently compliant with DFAR 252.204-7012 should, theoretically, be eligible for this level. Level 4 indicates the contractor has "advanced and sophisticated cybersecurity practices." And finally, Level 5 indicates "highly advanced cybersecurity practices" and is reserved for the most critical systems.

The DoD seeks to implement the CMMC framework in January 2020 and implement the framework into requests for proposal (RFP) by fall 2020. It is not clear yet how the DoD will utilize these levels, or limit competition, in drafting solicitations to require CMMC certification. The DoD's proposed timeframe raises a number of questions, such as:

1. How long will it take contractors to get certified?
2. Can contractors have pending certifications prior to submitting a proposal?
3. What will be the cost for certification and who will cover it?
4. How long will a certification last, and what is the process for re-certification?
5. Will contractors have any recourse if a certification is denied or reduced to a lower level than expected?

We expect the DoD to consider these issues before CMMC is implemented.

In addition to the DoD's proposed CMMC framework, the Department of the Navy (DoN) has implemented its own set of cybersecurity requirements for contractors seeking to do business with the DoN. Last September, the Assistant Secretary of the Navy for Research Development & Acquisition (ASN (RD&A)) published Memorandum for Distribution: Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks (The DIB Memo). The Navy issued this memorandum because the DoN desired to take immediate steps to increase the protection of critical controlled unclassified information that was being housed on contractor networks from cybersecurity threats. The DIB Memo required contracting officers to, in addition to ensuring compliance with NIST SP 800-171 and DFARS 252.204-7012, include a contract data requirement list (CDRL) requiring delivery and approval of a systems security plan (SSP) whenever it had been determined that the risk to a critical program and/or technology warranted it.

On September 6, 2019, the Office of the ASN for RD&A published Memorandum for Distribution: Change 18-08 of the Navy Marine Corps Acquisition Regulation Supplement (NMCARS). This Memo requires contracting officers to implement the DIB Memo, which can be found in the new NMCARS Annex 16, into all DoN applicable solicitations – where the risk to a critical program and/or technology warrants inclusion. The new NMCARS requires contractors to: (1) implement SSP and Plans of Action and Milestones (POAM) reviews, (2) ensure NIST SP 800-171 compliance, (3) develop a cyber-incidence response plan, and (4) participate in Naval Criminal Investigative Service (NCIS) outreach, and (5) participate in NCIS/industry monitoring. The prescribed language details what the contractor must do in these five areas to ensure that covered information is being properly safeguarded and that cyber incidences are being properly reported. Failure to comply with these new requirements can result in reduced or suspended payments, or equitable reductions, per NMCARS Subpart 5204.73. Contractors seeking to do business with the DoN or already engaged in performance of a DoN contract should be mindful of these requirements and the impact that non-compliance may have on them when it comes to matters of cybersecurity and cyber incidence reporting.

How can contractors reduce the risk of noncompliance?

While the DoD CMMC certification requirements are still in development, defense contractors can utilize this time to evaluate their compliance with the existing DFARS 252.204-7012 and NIST SP 800-171. Additionally, defense contractors seeking to do business with the DoN should familiarize themselves with the applicable NMCARS Subpart and Annex 16. Compliance with those existing regulations will inform the CMMC maturity level rating for which the contractor will ultimately be eligible.

With the transition from self-disclosure to an external auditor to ensure cyber security compliance, contractors can expect to see an increase in enforcement litigation for failure to comply with the cybersecurity regulations. The federal government has already demonstrated its willingness to employ the False Claims Act (FCA) against contractors for failure to comply with the existing cybersecurity requirements. Going forward, contractors that are found to have falsely certified compliance with the applicable cybersecurity regulations will be under the microscope, likely leading to an increase in FCA litigation.

Asset Finance in Brief
EHS Law Insights
Employment Law Watch
Financial Regulatory Report
Financial Services Litigation Report
FinTech Update
Global Regulatory Enforcement Law Blog
Global Restructuring Watch
Health Industry Washington Watch
Legal Flight Deck
Lending Law Report
Life Sciences Legal Update
Massachusetts SALT
Policyholder Perspective
Private Funds Law Update
PTAB Musings
Real Estate Legal Update
Reed Smith
Ship Law Log
Structured Finance in Brief
The Swap Report
Taxing Tech
Technology Law Dispatch

ARCHIVES

Select Month

In conclusion, contractors should be mindful of this increased scrutiny and take steps to ensure compliance. Contractors can and should conduct internal audits prior to CMMC certification and address gaps in their compliance to get ahead of the coming changes.

TAGS: CYBERSECURITY, DEPARTMENT OF DEFENSE (DOD), DFARS, FEDERAL ACQUISITION REGULATION (FAR), GOVERNMENT CONTRACTS