Federal Cybersecurity Requirements and Information Governance

CHESS CONSULTING LLC

Complex Accounting
Disputes
Investigations
Regulatory Compliance

Overview

Contractors to the federal government are familiar with managing numerous and consistently increasing requirements in order to comply with contractual terms and conditions. In recent years, cybersecurity has become an area of escalating focus for the Department of Defense ("DOD"), and federal agencies in general, with significant regulatory coverage of cybersecurity being added to the Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS"). The exfiltration of sensitive defense related and personal information from contractor managed systems is one of the largest risks to the United States' technological advantage, which has resulted in increasing scrutiny of how companies secure federal contract and program information.

There has been a flurry of activity, primarily from the DOD, to ensure that contractors are implementing mandated security controls and are designing procedures to adequately oversee suppliers who are being provided with defense information. This includes regulations such as, but not limited to, FAR 52.204-12 "Basic Safeguarding of Covered Contractor Information Systems," DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting," DFARS 252.204-7019 and 7020 regarding "NIST SP 800-171 DOD Assessment Requirements," and DFARS 252.204-7021 "Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement."

- FAR 52.204-21 is a contract clause included in all executive agency federal contracts that requires the protection of Federal Contracts Information ("FCI"). The clause includes 15 security requirements that must be implemented by contractors as well as the requirement for the clause to be included in subcontracts where FCI will reside or transit through the subcontractor's information system.
- DFARS 252.204-7012 is a requirement under DOD contracts to protect Covered Defense Information ("CDI"). It goes further than the FAR requirement in that it prescribes the implementation of 110 security requirements found within the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 framework. Contractors must document their implementation status in a system security plan and any gaps identified in a plan of actions and milestones ("POAM"). The clause also requires that contractors report to the DOD's Chief Information Officer, within 72 hours, any cyber incident impacting CDI. Lastly, the clause must be included in subcontracts where CDI will be required for subcontractor performance.
- DFARS 252.204-7019 & 7020 formalize the evaluation procedures of the DOD when determining the implementation status and compliance posture of contractors. Under this requirement, contractors must provide access to government auditors to evaluate documents and evidence that support control functioning. The depths of assessments are defined as Basic, Medium, and High with the extent of evaluation procedures aligned with the desired level of assurance.
- DFARS 252.204-7021 incorporates the Cybersecurity Maturity Model Certification ("CMMC") framework that will be utilized by the DOD to ensure that contractor cybersecurity practices have been assessed and verified by qualified and objective third parties prior to those contractors being awarded a government contract. Building on the self-assessment model of DFARS 252.204-7012, the CMMC framework will utilize a maturity rating of Levels 1 – 5 to assign an increasingly robust set of security requirements for contractors based on the sensitivity of the data in DOD contracts. To be eligible for award, contractors must receive a third-party certification validating that all required cybersecurity requirements are implemented and operating.

Information Governance and Supply Chain Considerations

The intent of the DOD in issuing these regulations is to improve contractors' ability to identify sensitive information and apply appropriate technical and process driven safeguards. However, a major challenge faced by many in the Defense Industrial Base ("DIB") is determining what information requires protection. While under the cited

regulations, the DOD does provide definitions for FCI, CDI, and Controlled Unclassified Information ("CUI"), and points to regulatory guidance issued by the National Archives and Records Administration ("NARA"), the provided definitions also state that covered information could be "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." This broad and vague wording puts contractors in the difficult position of having to evaluate the work being performed under DOD contracts and self-classifying the types of information being developed and generated in association with their contracts. While mature defense contractors have experience with self-classifying program related information, for many commercial companies with a smaller portfolio of government contracts and who do not have the compliance regimes of larger contractors, this requirement can cause confusion and operational disruption.

Additionally, prime contractors must consider how the information they provide to their subcontractors and the information being developed under the scope of work of the subcontract may invoke the requirements of the various contractual regulations. At a minimum, prime contractors must flow down the contract clause when the use of CUI or CDI is anticipated, but regulators have expressed through guidance that oversight from the prime extends beyond this to actions such as vetting supplier capabilities and tracking the transmission of information. As the DOD has identified the supply chain as the highest risk for contractor breaches of information, it is expected that continued and increased oversight of suppliers will be required from primes.

Risk of Non-Compliance and Importance of an Organizational Approach

Depending on the contract terms and factual circumstances, and on a contract-by-contract basis, the Government may consider the following actions in the event a contractor fails to comply with contract terms and conditions:

- Contractual

  - Withhold payment for non-compliant contract performance
  - Disapprove business system/contractor purchasing system
  - Decline to issue future orders on contract
  - Decline to exercise future contract options
  - Document negative past performance rating
  - Issue a stop work order
  - Issue a cure notice
  - Issue a show cause notice
  - Consider contract termination proceedings
  - Find the contractor non-responsive
  - Issue the contractor a Corrective Action Request ("CAR")

- Administrative/Judicial

  - Suspension and debarment proceedings
  - Pursuit of civil claims/penalties
  - Pursuit of criminal prosecution/penalties

With the potential for non-compliance to have significant impact, organizations must implement processes and controls across functional departments to ensure that organizational risk is addressed. Key stakeholders from functions such as legal, compliance, IT, security, contracts, programs, and supply chain should all be aware of relevant requirements and the role they play in ensuring government related information is managed throughout the contract lifecycle.

The Chess Consulting Advantage

Chess Consulting's highly experienced team of government contract advisory, cybersecurity, and regulatory compliance experts have worked with contractors and their legal counsel on a multitude of FAR and DFARS cybersecurity compliance matters, ranging from readiness assessments and internal audits to drafting system security plans, policies, and procedures. Additionally, we have assisted numerous new entrants to enhance and tailor their existing security strategies, frameworks, and assessment programs to align with contractual requirements based on their current and expected federal scopes of work.

Chess's experience with government contract compliance matters paired with a deep understanding of cybersecurity and risk management programs uniquely positions us to assist our clients to holistically address federal cybersecurity requirements.

Chess Consulting Differentiators

Deep industry knowledge and technical expertise which helps each client deal effectively with the complexities of the processes and issues facing its business.

Profitability focus concentrating on actions and solutions that create a competitive business advantage while fully complying with regulatory requirements.

Practical and creative solutions that effectively address difficult compliance and business issues.

Supportable positions that have been proven to withstand scrutiny from regulatory agencies such as the SEC, DCAA, DCMA, DOJ, and GAO.