Professional Perspective

# Supply Chain Regulation, Cybersecurity & Product Integrity

Sarah Bishop, Susan Cassidy, Alexander Hastings, and Robert Huffman,
Covington & Burling

Bloomberg Law

# Supply Chain Regulation, Cybersecurity & Product Integrity

*Contributed by Sarah Bishop, Susan Cassidy, Alexander Hastings, and Robert Huffman, Covington & Burling*

The U.S. continues to experience a supply chain crisis. Disruptions in the supply chain for microchips and other essential items threaten the post-Covid 19 recovery and contribute to inflationary pressures. The presence of foreign adversaries—entities controlled by foreign adversaries—could lead to shutdowns and other threats to critical infrastructure. Moreover, vulnerabilities in software and vendor cybersecurity capabilities are increasingly exploited by those same adversaries as well as criminal gangs to extract ransom, plant malware, steal sensitive national security information, or infringe intellectual property rights.

The U.S. government is responding to these supply chain risks and threats with several initiatives. Common to all these initiatives is an increase in actual or likely federal regulation of supply chains.

This is the first article of a two-part series examining four of these supply chain initiatives. This article examines enhanced requirements for cybersecurity throughout the supply chain and the increased emphasis that companies are facing to incorporate environmental, social and governance (ESG) considerations into their sourcing decisions. The second article will examine domestic preferences in federal government procurement and highlight tools developed by the federal government to eliminate products and sources believed to present a national security risk.

Several cybersecurity regulatory regimes are currently applicable or may become applicable to government contractors and their subcontractors. They include:

- The Federal Acquisition Regulation (FAR) cybersecurity clause that must be included in most federal agency procurement contracts and subcontracts
- The Department of Defense-specific regulations and clauses that impose cyber incident reporting and other requirements on DOD contractors and subcontractors
- New regulations that may result from implementing the Biden administration's May 2021 executive order on enhancing cybersecurity
- Other changes that could result from various bills pending in Congress

## FAR Basic Safeguarding Cybersecurity Clause

FAR 52.204-21 includes basic cybersecurity safeguarding requirements for government contractors. This clause must be included in any solicitation or contract that will involve "federal contract information (FCI)." The clause defines FCI as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government."

The clause requires a contractor to apply 15 basic safeguarding requirements to its information systems that store or process FCI. These requirements correspond to 17 of the National Institute of Standards and Technology (NIST) 800-171 standards for non-federal information systems. The contractor must include the substance of the clause in all subcontracts (except for subcontracts for the acquisition of commercial off the shelf (COTS) items) where the subcontractor may have FCI residing in or transmitting through its information system.

## DOD's Cyber Safeguarding and Reporting Requirements

The Department of Defense imposes cybersecurity safeguarding and reporting requirements more stringent than those of the FAR by requiring the inclusion of certain DOD Federal Acquisition Supplement (DFARS) clauses in its procurement contracts.

 

### *DFARS Cyber Safeguarding and Incident Reporting Clause*

The primary clause affecting the supply chain is DFARS 252.204-7012, which requires DOD contractors to provide "adequate security" on all "covered contractor information systems." The clause defines "adequate security" to mean "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information," and it requires the contractor, at a minimum, to implement the 110 security requirements of NIST Special Publication 800-171 by no later than Dec. 31, 2017.

The '7012 clause defines "covered contractor information system" to mean an unclassified information system that is owned, or operated by or for, a contractor, and that processes, stores, or transmits "covered defense information." The clause defines CDI as "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information ("CUI") Registry, which requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies." CDI is further defined as:

- Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract
- Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract

In addition to imposing safeguarding requirements on covered contractor information systems, the '7012 clause imposes reporting and data preservation requirements for "cyber incidents" that affect such systems or the CDI residing thereon. The clause defines "cyber incident" to mean "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing thereon." It requires the contractor to report such incidents to the DOD Cyber Crime Center (DC3) within 72 hours of discovery if such incidents affect a covered contractor information system or CDI residing thereon.

The clause also requires the contractor to isolate and submit to DC3 any malicious software associated with the reported cyber incident, and to preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days to allow DOD to request the media or decline interest.

Two features of the '7012 clause pose significant compliance challenges for contractors:

- Identification of CDI (or CUI) that may be on their (or their subcontractors') systems
- Implementation of the 12/31/2017 deadline for NIST 800-171 security requirements

DOD attempted to alleviate the first problem by issuing guidelines to government program managers and contracting officers regarding the proper designation and marking of CUI. However, confusion remains over whether data is CDI, CUI, or FCI.

DOD addressed the December 2017 deadline by providing informal guidance that allows contractors to add a security control that requires a System Security Plan (SSP) and Plans of Actions and Milestones (POA&Ms), which specify how and when the contractor will meet outstanding requirements.

Contractors' heavy reliance on SSPs and POA&Ms has led DOD to question the readiness of its supply chain to withstand cyberattacks.

### *Self-Assessment and Certification Clauses*

Perceived shortcomings in contractors' compliance with the '7012 clause led DOD to promulgate interim final amendments to the DFARS on Sept. 29, 2020. This action added three new clauses to the DFARS effective Nov. 30, 2020 that are intended to move DOD away from contractor "self-attestation" to a system requiring contractor self-assessment and, in some instances, third-party assessment and certification.

These clauses are DFARS 252.204-7019 and 7020—both of which impose NIST 800-171 Assessment Requirements—and DFARS 252.204-7021, which addresses the Cybersecurity Maturity Model Certification Program (CMMC).

Assessment Requirement Clauses

The ‘7019 clause states that to be considered for award, a contractor with a covered system must have an assessment of its NIST 800-171 implementation that is not more than 3 years old—unless a shorter period is specified in the solicitation—for each covered system that is relevant to the offer, contract, task order, or delivery order covered by the solicitation.

These assessments are either “Medium-” or “High-” level assessments conducted by the Defense Contract Management Agency (DCMA), or a “Basic Assessment” conducted by the contractor in accordance with a DOD-specified methodology. The ‘7019 clause requires DCMA to post the summary results of a Medium or High Assessment in the Supplier Performance Risk System (SPRS), and requires offerors to do the same with their Basic Assessment. DOD personnel may access all summary level scores posted in SPRS, but offerors and contractors are limited to accessing their own scores.

The ‘7020 clause repeats the assessment and posting requirements of the ‘7019 clause, and it requires contractors to include those requirements in all subcontracts and other contractual instruments (except for the acquisition of COTS items). This means that subcontractors and *their* subcontractors—except for COTS subcontractors—must conduct Basic Assessments and post the scores of such assessments in SPRS.

The ‘7020 clause prohibits a contractor from awarding a subcontract or other contractual instrument to an entity that has not completed at least a Basic Assessment within the past three years for all covered contractor information systems relevant to its offer.

The current DOD Assessment Methodology provides for a top score of 110 based on compliance with all 110 NIST 800-171 requirements. Failure to meet a requirement will result in a reduction in the score; the amount of each reduction depends on the significance of the factor and the degree of shortfall in meeting that requirement. Some controls are worth 5 points (42 controls), some 3 points (14 controls), and some 1 point (54 controls). This means that a negative score is possible. DOD has not provided guidance as to what scores are acceptable, how these scores are be evaluated, or whether a score will preclude an award at either the prime or subcontractor level.

Neither the ‘7019 nor the ‘7020 clause requires an offeror to ask potential subcontractors for their assessment scores or to validate whether the scores were properly calculated. However, some offerors have asked their potential subcontractors for their scores to better gauge the effect of those scores on the likelihood of award, and to make contingency plans for alternative suppliers in the event the potential subcontractor's score is too low or otherwise suspect.

Other offerors have simply asked for representations or certifications from potential subcontractors that they have performed the relevant self-assessments and posted their scores in SPRS.

It should be noted that knowledge of a subcontractor's low score could present issues for a prime contractor charged with maintaining adequate security over DOD's data.

***CMMC Clause***

The interim final rule also includes DFARS 252.204-7021, which addresses CMMC requirements once implemented. CMMC is a framework for third-party certification of a contractor's cybersecurity maturity as measured by its implementation of NIST 800-171 along with other cybersecurity practices and processes.

CMMC assigns ascending maturity levels 1-5 depending on the type and sensitivity of the information to be protected and the range of threats to be protected against. Thus, for example, CMMC Level 1 (“Basic Cyber Hygiene”) is adequate for an information system that houses or transmits only FCI, while CMMC Level 3 (“Good Cyber Hygiene”) is designed for systems that house or transmit CUI.

Importantly, a contractor or subcontractor will not be able to use SSPs and POA&Ms to demonstrate its implementation of the NIST 800-171 requirements for CMMC purposes.

DOD intends to use CMMC maturity levels 1-5 as “go/no go” evaluation criterion in future procurements, starting with a limited number of “pilot” solicitations currently scheduled for FY 2022. The solicitations for these procurements will identify the CMMC level required to be eligible for the prime contract and potentially for certain subcontracts.

When included in the prime contract, DFARS '7021 will require the contractor to have in place a current—i.e., not more than three years old—certificate at the specified CMMC level and to maintain its CMMC certificate at the required level for the duration of the contract.

The prime contractor will also be required to flow the substance of the DFARS '7021 clause down to its subcontractors (except for those providing COTS items or where the subcontract is below the micro-purchase threshold). Thus, subcontractors would also be required to have a current certificate in place at the required CMMC level and to maintain that certificate for the duration of the subcontract.

Moreover, before awarding a subcontract, the contractor will be required to ensure that the subcontractor has a certificate at the appropriate CMMC level.

Third-party assessment of CMMC maturity levels will be performed by accredited (licensed) assessors employed by accredited CMMC Third Party Assessment Organizations (C3PAOs), all of which will be accredited and overseen by a private, non-profit corporation known as the CMMC Accreditation Board (AB).

Among other functions, the AB will provide for the training and accreditation of assessors and C3PAOs, will certify contractors' CMMC levels based on the assessments of the C3PAOs and their licensed assessors, and will resolve disputes between contractors and C3PAOs regarding the merits of particular C3PAO assessments.

Implementation of CMMC in RFIs and RFPs is temporarily on hold pending a review of the program conducted by the Office of the Undersecretary of Defense for Acquisition and Sustainment, and Deputy Secretary of Defense Kathleen Hicks. In addition, the DAR Council could possibly make changes to the DFARS '7021 clause or otherwise impact the timing or impact of CMMC.

## President Biden's Cybersecurity Executive Order

On May 12, 2021, President Joe Biden issued an executive order on Improving the Nation's Cybersecurity (EO 14028). The cyber EO imposes requirements and deadlines on federal agencies to protect and secure the federal government's computer systems. Implementation of EO requirements will impact federal contractors and subcontractors, along with software developers, vendors, and owners and operators of critical infrastructure.

The EO requirements that will likely have the most impact on federal contractors are those pertaining to the removal of barriers to sharing threat information. Section 2 of the EO seeks to remove such barriers by updating the FAR language in a manner that requires IT and operational technology service providers to report cyber incidents and potential cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA)—and potentially other agencies—and to collect and share with those agencies information relating to such incidents.

The EO also requires federal contractors to notify CISA and the affected agency upon discovery of a cyber incident involving a software product or service provided to the agency or involving a support system for such software. Finally, the EO requires DHS and other agencies to review existing agency-specific cybersecurity requirements and to recommend to the FAR Council standardized contract language for cybersecurity requirements. The FAR Council has opened two FAR cases to prepare for the implementation of these requirements.

## Environmental, Social and Governance (ESG) Requirements

Focus on ESG considerations in government procurement is rising. ESG-related FAR provisions come amid a growing array of new ESG-related enforcement risks and laws, such as the prohibition of imports produced by forced labor (19 U.S.C. § 1307), prohibitions on human trafficking, and emerging supply chain due diligence laws in Europe.

### *FAR Anti-Human Trafficking Provisions*

Human trafficking compliance obligations for federal contractors were augmented in Jan. 2015, when the FAR Council published the Final Rule implementing Executive Order 13627 and title XVII of the National Defense Authorization Act of 2013. The Final Rule, implemented by FAR 52.222-50, is applicable in large part to all federal contractors and subcontractors, regardless of contract type or dollar amount.

FAR 52.222-50, which has been the subject of increased focus and enforcement in recent years, prohibits contractors, subcontractors, and their employees and agents from:

- Engaging "in severe forms of trafficking in persons during the period of performance of the contract" (not limited to activities directly related to contract performance)
- Procuring "commercial sex acts during the period of performance of the contract" (not limited to activities directly related to contract performance)
- Using forced labor in the performance of the contract

Forced labor is broadly defined to include actions such as destroying, concealing, confiscating, or otherwise denying access to the employee's identity or immigration documents, using misleading or fraudulent recruiting practices, and charging recruitment fees.

Contractors and subcontractors have obligations to inform employees and agents of these prohibitions, to take appropriate action against personnel and subcontractors that engage in prohibited conduct, to cooperate with government investigations, and to inform the contracting officer, agency inspector general, and possibly law enforcement of any credible information regarding a human trafficking violation.

***Executive Order on Climate-Related Financial Risk***

On May 20, 2021, President Biden signed Executive Order 14030 on Climate-Related Financial Risk. Among other things, E.O 14030 calls on the FAR Council, in consultation with the chair of the Council on Environmental Quality and the heads of other agencies as appropriate, to consider climate-related FAR requirements for major federal suppliers, addressing:

- Disclosure of greenhouse gas emissions and climate-related financial risk
- Establishment of science-based reduction targets
- Consideration of greenhouse gas emissions in procurement decisions

The FAR Council has opened two FAR cases to address the potential implementation of such requirements.

***Supply Chain Sustainability Recommendations***

In June 2021, the Biden Administration released its report on the results of its 100-day review of U.S. supply chains for critical products. The report followed President Biden's Feb. 24 Executive Order on America's Supply Chains, which directed federal departments and agencies to conduct reviews of supply chain risks in four critical product areas: semiconductor manufacturing and advanced packaging; large capacity batteries; critical minerals and materials; and pharmaceuticals and active pharmaceutical ingredients.

Sustainability considerations were a central theme of the DOD's review of critical mineral and material supply chains, which included a recommendation to take "a whole-of-government approach to diversify international supply chains and move global markets toward sustainably, responsibly produced sources of critical minerals and materials."

Among other potential steps, the DOD recommended developing a "sustainably produced" standard and directing the FAR Council to publish a rule for public comment that would establish a preference or requirement for the selection of products with higher sustainably produced content.

## Conclusion

As the U.S. faces a supply chain crisis, we can expect that the U.S. Government will respond with several initiatives, including an increase in actual or likely federal regulation of supply chains. These regulations are impacting or are likely to impact cybersecurity requirements and companies' approaches to (ESG) considerations into their sourcing decisions. Additionally, as we will address in our next article, we expect continued emphasis on domestic preferences in federal government procurement and increased use of tools by the federal government to eliminate products and sources believed to present a national security risk.