DOD Increasing Oversight of Contractor Cybersecurity and Cyber Supply Chain Risk Management

Published on March 7, 2019

Susan Warshaw Ebner | ✓ Following
Partner at Stinson Leonard Street LLP
12 articles

By Susan Warshaw Ebner

On January 21 and February 5, 2019, the Under Secretary of Defense for Acquisition and Sustainment, Ellen Lord, issued two memoranda outlining steps that the Department of Defense (DOD) is taking to increase the scrutiny and consideration of a government contractor's implementation of DOD cybersecurity requirements. These memoranda make clear that the DOD is ratcheting up its scrutiny of government contractor cybersecurity and supply chain risk management. On February 26, 2019, the Defense Contract Management Agency (DCMA) updated its Contractor Purchasing System review (CPSR) Guidebook to specifically address this supply chain management (SCM) audit area. Contractors at all tiers would be well advised to take steps now to internally audit their compliance with these cybersecurity requirements and to confirm that they are properly addressing them when engaged in bidding and performing government contracts and subcontracts.

DFARS 252.204-7012 and NIST SP 800-171

Contractors whose contracts contain DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, are required to implement the 110 controls in the National Institute of Standards and Technology (NIST) Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, or to request and obtain approval of any variation to these requirements to provide "an alternative, but equally effective, security measure that may be implemented in its place." Compliance requires, among other things, a System Security Plan (SSP) and Plan of Action and Milestones (POA&M) for the implementation and continuing compliance with NIST SP 800-171. Compliance also requires that contractors report to the Government regarding an actual or suspected cyber incident within 72 hours of its discovery. The clause also obligates the contractor to preserve and protect data relating to such an incident for at least 90 days in order to allow DOD the opportunity to request such data.

Contractors are obligated to flow down these requirements to their subcontractors or similar agreement holders, including those that provide commercial items, where their performance will involve Covered Defense Information (CDI) or operationally critical support. Since the clause must be flowed down unchanged, subcontractors and similar agreement holders receiving the clause are also required to ensure that they properly flow down and ensure compliance of their subcontractors and suppliers, including those providing commercial

items. The only commercial item subcontracts excepted are those where solely Commercial-Off-The-Shelf (COTS) items are being provided; services are not considered COTS items.

DOD to Audit Compliance with DFARS and NIST Requirements

DOD intends to audit government contractors' compliance with the cybersecurity program and reporting requirements of DFARS 252.204-7012 and NIST SP 800-171. In addition to assessing the state of government contractors' implementation of their own cybersecurity requirements, the DOD will be assessing whether contractors are properly identifying and flowing down cybersecurity requirements to covered subcontractors whose performance will involve CDI that includes DOD's Controlled Unclassified Information (CUI). In the memoranda, Ms. Lord directs DOD to take steps to audit 1) contractor compliance with marking and distribution requirements relating to DOD CUI and 2) contractor procedures for ensuring the compliance of their "Tier 1 Level Suppliers" with the DFARS and NIST requirements.

Pursuant to Ms. Lord's memoranda, the Defense Contract Management Agency (DCMA) has been charged with conducting purchasing system audits of contractors for which it currently provides contact administration and oversight to audit the contractors' compliance with these cybersecurity requirements. As noted above, DCMA's February 2019 update to its CPSR Guidebook Appendix 24 specifically addresses Ms. Lord's SCM direction, in addition to counterfeit electronic parts detection and avoidance system and other SCM requirements. Under the revised Guidebook, contractors SCM "processes should address the SCM methodology either combined into one overarching supply chain process or in separate processes for the following issues; Sourcing Strategy, Work Transfer, Vendor Rating System, Supplier Risk Management, Purchasing, Government Notification, Internal Audit & Controls (metrics), Surveillance & Performance Monitoring, *Safeguarding Covered Defense Information, Cyber Incident Reporting,* and Supplier Corrective Action."

DOD intends to ensure that contractors that are not subject to DCMA contract administration and oversight are audited for compliance in these areas as well. For these contractors, DOD will be working with the affected communities, such as the Navy's shipbuilding program, to develop a similar approach for auditing.

Follow up

Contractors would be advised to ensure that they include the appropriate flow down terms and procedures for ensuring that their subcontractors and similar agreement holders are receiving the clause and complying with its terms. Though the term "Tier 1 Level Suppliers" is not defined in the memorandum and we traditionally think of Tier 1 suppliers as those subcontractors or suppliers that directly contract with the contractor, DFARS 252.204-7012 requires that prime contractors flow down the clause to subcontractors *without alteration except for the names of the parties,* meaning that the clause's subcontract flow down requirement--subparagraph (m)--must be included in their lower tier subcontractor agreements. The rulemaking to implement the clause and the DOD memoranda make clear that it is DOD's ultimate intent to ensure that contractors are taking adequate steps to protect DOD CUI whenever and wherever in the supply chain it is being used or provided.

Susan Warshaw Ebner is responsible for the contents of this article.

Report this

10 Likes

1 Comment

Add a comment...

Michael Carpenter • 2nd
Chief Information Security Officer at Michael Baker International
3h ···
Good article Susan, it is certainly what we have been expecting.
Like Reply

Susan Warshaw Ebner
Partner at Stinson Leonard Street LLP

✓ Following

More from Susan Warshaw Ebner See all 12 articles

The Government May Not Be Shut Down Now, But Contractors Mind Your Funding!
Susan Warshaw Ebner on LinkedIn

Small Business Runway Extension Act of 2018 signed into law
Susan Warshaw Ebner on LinkedIn

DoD Issues new Other Transactions Guide
Susan Warshaw Ebner on LinkedIn

Supply Chain S Imperative
Susan Warshaw E

Messaging