Set-Aside Alert™

www.setasidealert.com

Vol. 25, No. 21 Your source for Federal set-aside and small business contracting news since 1992 October 20, 2017

Column: Cybersecurity Compliance Deadline Looms for Government Contractors

By Kimi N. Murakami, counsel, PilieroMazza PLLC

Now that the government fiscal year end has passed, government contractors who handle Controlled Unclassified Information (CUI) must turn their attention – if they haven't already – to the quickly-approaching calendar year-end deadline for being compliant with cybersecurity obligations imposed under Defense Federal Acquisition Regulation Supplement (DFARS) § 252.204-7012.

Dec. 31 deadline

U.S. Department of Defense (DOD) rules adopted in 2016 require that government contractors handling CUI have until Dec. 31, 2017, to implement standards set forth in the National Institute of Standards and Technology Special Publication (SP) 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST SP 800-171).

Security requirements

According to DFARS § 252.204-7012(b)(i), in order to constitute "adequate security" for "covered contractor information systems" (systems that are not part of an information technology service or system operated on behalf of the government), the covered contractor information system "shall be subject to the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the Contracting Officer."

Furthermore, the DFARS regulations make clear that time is of the essence because:

- The contractor shall implement NIST SP 800-171, as soon as practical, but not later than Dec. 31, 2017.
- Under DFARS § 252.204-7012(b)(ii)(A), for all contracts awarded prior to Oct. 1, 2017, the Contractor shall notify the DoD Chief Information Officer via email at *osd.dibcsia@mail.mil*, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

Definitions

CUI is information of the federal government that is sensitive but unclassified. Under the regulations, CUI requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, and is "(1) 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; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."

NIST SP 800-171

While compliance may seem daunting, most federal contractors that handle CUI most likely have already been following NIST SP 800-171, which outlines the basic safeguarding requirements that must be implemented. The publication includes 14 families of security requirements, comprising 109 individual controls. The CUI requirements within NIST SP 800-171 are directly linked to the baseline controls described in NIST Publication SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations).

Best practices

To comply with CUI requirements, contractors must fully understand what CUI it stores, processes, or transmits in the course of doing business with the federal government. Compliance requires that contractors provide adequate documentation describing technical solutions and policies, and evidence of being able to detect and respond to incidents. Again, these are best practices that most contractors in the federal government space handling CUI already should have in place.

For contractors handling CUI for the federal government, the time has come to ensure that internal controls and best practices align with the agency specific regulations, contract terms related to CUI and NIST SP 800-171 by taking the following steps.

Steps to compliance:

- Know what CUI you're handing. Carefully review contracts for CUI handling requirements. Be sure to understand the various types of CUI that you're handling under existing contracts.
- Perform a "gap assessment" to understand what requirements your current security plan is not meeting under the new rules.
- Update internal controls, procedures and policies to ensure compliance with the new rules. Again, hopefully this will only require revising controls already in place to remediate identified gaps.
- If you do not have a plan in place for CUI, develop an IT Security Plan to implement such controls, procedures and policies right away to be in compliance by the year-end deadline.
- Depending on the agency, as with DOD's DFARS § 252.204-7012, there could be agency-specific rules implemented, so become familiar with the specific requirements for handing CUI depending on which government customer you work for.
- Finally, prime contractors must also add provisions to flow down CUI clauses to their subcontractors and have policies for monitoring subcontractor compliance as also required by DFARS § 252.204-7012(m).

There's still enough time during the fourth quarter of 2017 to achieve compliance imposed by DFARS § 252.204-7012 and put NIST SP 800-171 controls for handling CUI in place within your IT Security Plan. But the time has come as failing to do so will preclude you from contracting with the DOD.

Kimi Murakami is counsel with PilieroMazza PLLC in the Business & Corporate Law and Government Contracts Law Groups.