Cooley

October 19, 2015

The Department of Defense (DoD) has published regulations that require DoD contractors to report cyber incidents impacting unclassified DoD contractor systems. The new regulations mandate compliance with elements of the formerly voluntary DoD-Defense Industrial Base (DIB) Cybersecurity (CS) information sharing program that permitted contractors to share actionable cyber threat information. Under the new regulations, DoD contractors must report cyber incidents affecting covered contractor information systems or covered defense information residing on those systems. However, the new regulations continue to allow voluntary participation in the portion of the program that permits contractors to receive cyber threat information from the government and other program participants.

Created in 2013, the DoD-DIB CS program sought to assist DIB participants in protecting DoD information that resides on or transits through unclassified information systems. The program permitted the DIB participant to enter into a voluntary agreement with DoD to share cybersecurity information relating to information assurance for covered information on DIB systems. Under the program, the DIB participant could report cyber incidents involving covered information and receive information from the government related to cyber threats and information assurance practices.

Mandatory reporting scheme for cyber incidents

The new regulations, published by DoD on October 2, 2015 and effective the same day, shift from voluntary reporting of cyber incidents to a mandatory reporting scheme. The regulations provide that covered DoD contractors must "report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support." The regulations apply to a contractor that has "accepted any type of agreement or order to provide research, supplies, or services to DoD," and affect both prime contractors and subcontractors. The regulations define "covered defense information" to include controlled technical information, operations security information, export controlled information or other information marked or identified by the government as requiring safeguarding.

Under the new regulations, when a contractor discovers a cyber incident that affects a covered contractor information system or covered defense information, the contractor initially must conduct a review for evidence of compromise of covered defense information. This review includes identifying compromised computers, servers, specific data and user accounts; analyzing covered contractor information system(s) that were part of the cyber incident; and analyzing other information systems on the contractor's network that may have been accessed as a result of the incident. Once the review has been conducted, the regulations direct the contractor to **report the incident** "rapidly" to DoD. Information provided in the report includes contractor and contract information as well as details on the cyber incident and the contractor's efforts to investigate. The regulations also specify that DoD contractors and subcontractors must maintain a DoD-approved medium assurance PKI (Public Key Infrastructure) digital certificate to securely report cyber incidents.

Preservation of information required

Apart from the reporting requirements, the new regulations direct contractors to preserve and protect images of known affected information systems impacted by a cyber incident and all relevant monitoring/packet capture data for at least 90 days from submission of the cyber incident report. In addition, the contractor must submit any malicious software discovered or isolated to the

DoD Cyber Crime Center for forensic analysis. The new regulations also provide that if DoD elects to conduct a damage assessment, DoD will request that the contractor provide all of the damage assessment information gathered by the contractor.

Further impact on DoD contractors and subcontractors

As previously noted, the new regulations apply to covered defense information, and do not address cyber incident reporting requirements for other types of controlled unclassified information, such as personally identifiable information or budget or financial information. The regulations state that the outlined cyber reporting requirements do not abrogate the contractor's responsibility for any other applicable cyber reporting requirements, such as notification requirements that may be triggered under the laws of any of the 47 states that currently have data breach notification statutes in place, or notification requirements under the Gramm-Leach-Bliley Act (GLBA) or under the Health Information Technology for Economic and Clinical Health Act (HITECH).

The new regulations also modify eligibility requirements to allow for greater participation in the voluntary DoD-DIB CS information sharing program. In order to be eligible, the contractor must have an existing facility clearance granted under the NISPOM and execute a standard Framework Agreement, which implements the requirements of the program. The program permits participating contractors to share cybersecurity information with the government and other participants, and establishes protections for the safeguarding of such information.

Practical considerations

DoD contractors and subcontractors who maintain information systems or defense information covered by these new regulations must understand the scope of their obligation to monitor and report cyber incidents. DoD's shift from voluntary participation to mandatory compliance will affect many contractors who may not have participated in the DoD-DIB CS program and have not implemented necessary processes to ensure compliance with the reporting requirements. Given the increasing emphasis placed by the government on safeguarding information and monitoring and reporting cyber incidents, DoD contractors should ensure they comprehend the requirements of the new DoD-DIB CS regulations and their impact upon the contractor.

The regulations are published at **80 Federal Register 59581 (October 2, 2015)**.

Key Contacts

Andrew Lustig Reston	alustig@cooley.com +1 703 456 8134

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090