DoD Adopts Broad New Cyber Security and Incident Reporting Rules

By Benjamin J. Lambiotte

On August 26, 2015, the Department of Defense adopted interim DFARS regulations requiring DoD contractors and subcontractors to provide "adequate security" to safeguard "covered defense information" (a term defined more broadly than ever before; see below), to report cyber incidents, and to establish policies and procedures for procurement of commercial cloud services. These measures, adopted in response to mandates in recent national defense budget authorization legislation, increase the cybersecurity requirements on DoD-related information stored in or transiting contractor and subcontractor information systems. The interim rule builds on 2013 DFARS provisions and contract clauses designed to protect Unclassified Controlled Technical Information. The scope of the interim rules is expansive. The heart of the rules is a substantial revision of the standard DFARS clause on safeguarding UTCI, 252.204.7012.

The requirements now apply to all unclassified "covered defense information." That term is broadly defined, and includes all information provided to, collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract; and which falls into any of the following categories: controlled technical information (any information with space or military applications that is subject to controls on access, use, reproduction, modification, release, disclosure or dissemination); designated critical operational security information; export controlled information (including dual use information); and any other information, marked or otherwise identified in the contract as requiring safeguarding or dissemination controls. Standard contract clauses implementing the interim rules must be incorporated into commercial item contracts and flowed down to lower-tier subcontractors.

"Adequate security," is measured by a proportionality concept, and defined, generally, as protective measures commensurate with the consequences and probability of loss, misuse, unauthorized access to, or modification of the information. Specifically, where a contractor's system is part of an IT service or system operated on behalf of the government, and includes cloud services, the system must comply with the new cloud computing security requirements in a new standard DFARS clause, 252.239-1010, Cloud Computing Services, and any non-cloud systems are subject to the specific security requirements of the contract. Where the contractor's information system is not operated on behalf of the government, but "covered defense information" is stored on or transits such system, then, at a minimum, the system must meet the requirements of NIST SP-800-171 "Protecting Unclassified Information in Non-Federal Information Systems and Organizations."

DoD views NIST SP-800-171 guidelines as less onerous to the contractor and easier to use than federal system-oriented FIPS 200 and NIST SP-800-53 standards, a highly debatable premise. To introduce a degree of flexibility, the rules add another new clause, 252.204-7008, Compliance with Safeguarding Defense Information Controls, to be added to solicitations, which affords bidders a process to explain how proposed alternatives to SP-800-171 protections will be equally effective, and why a particular requirement should not apply. Approved deviations from SP-800-171 are to be incorporated into the award.

Reporting requirements are triggered when the contractor discovers a cyber incident that result in an adverse effect on a contractor's information system, the covered defense information residing therein, or on a contractor's ability to provide support designated as "operationally critical," meaning supplies or services designated by the government as critical for airlift, sealift, and intermodal transportation services, or logistical support essential to contingency operations. When such an incident occurs, the contractor must conduct a review and analysis of its systems and networks for evidence of compromised covered defense information, identifying compromised computers, servers, specific data, and user accounts, and then "rapidly" (within 72 hours) report to DoD and its upper tier contractor, the incident. The report shall include the elements required at http://dibnet.dod.mil, and in order to submit such reports the contractor needs to already have, or obtain, a DoD-approved medium assurance certificate. Also, if the contractor is able to discover and isolate malicious software, it must submit the malware in accordance with the CO's instructions. In any event, the contractor must preserve and protect images of all known affected information systems, and all relevant monitoring/packet data for at least 90 days following the report, to give DoD an opportunity to request the media, or decline interest.

Recognizing that contractors may be required to submit competitively-sensitive and proprietary information in connection with an incident report, the interim rules require the government to protect against unauthorized use or release outside DoD information obtained from the contractor or derived from such information. To the extent practicable, the contractor must mark or identify such sensitive proprietary/attributional material. Nevertheless, consistent with the current federal information-sharing cyber incident response philosophy, the rules provide that DoD may share contractor-provided or derived information outside the agency, to entities with missions that may be affected by the incident, or called upon to assist in the diagnosis, detection or mitigation of the incident, to Government law enforcement or counterintelligence agencies, for national security purposes, including with participants in Defense Industrial Base program participants, and to support services contractors operating under a contract containing yet another new clause, 252.204-7009, Limitations of the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, designed to protect contractor information in the hands of forensic support service providers.

While the interim rules are not yet final, they are currently in force and in effect. DoD contractors and subcontractors at all tiers, including commercial item contractors, should expect their requirements and the mandatory clauses prescribed by the rules to be included in awards and task orders issued after August 26, 2015. Any affected contractor or subcontractor, at any tier, with information systems upon which "covered defense information" resides or transits should immediately take steps to ensure that:

- Its information systems meet applicable security requirements, including specific standards applicable to cloud environments and, at a minimum, NIST SP-800-171;
- Its IT personnel are familiar with the steps that must be taken upon discovery of a cyber-incident, including analysis, preservation and reporting requirements;

- To facilitate secure reporting to DoD, it has obtained a DoD-approved medium assurance certificate. See http://iase.disa.mil/pki/eca/Pages/index.aspx

***

Benjamin J. Lambiotte is an Owner at Garvey Schubert Barer working out of its Washington, D.C. office. His practice areas include government contracts and cybersecurity. For any questions or comments, please contact him at blambiotte@gsblaw.com or at 202.298.252.