Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

DOD Takes Data-Centric Approach To Contractor Cybersecurity

Law360, New York (September 11, 2015, 10:07 AM ET) --

Hilary Cairnie

Randy Gainer

Under the U.S. Department of Defense's recently announced interim cyber rules (See DFARS Parts 202, 204, 212, 239 and the corresponding implementing clauses at DFARS Part 252), contractors and their subcontractors (by operation of mandatory flow-down language) are subject to many new requirements applicable to covered information and covered information systems. Central to these rules is the 72-hour window for reporting cyberincidents "in a broader scope of circumstances." Contractor cyber reports are not directed to agency contracting or program personnel or offices. Instead, the DOD has established a sort of clearinghouse to receive all cyber reports from all DOD contractors. (The new rules are found here.) The interim rules require the reporting of very specific information pertaining to each cyberincident and caution that it may be necessary to retain specialized information technology experts to forensically extract the required information in a way that does not destroy the cyber fingerprints left behind by the perpetrator.

The new rules also encompass cybersecurity measures applicable to cloud computing services. The cloud security measures are, in most respects, substantially the same as what is promulgated for covered information and covered information systems.

Not surprisingly, the rules are complicated because cyber problems are complicated. What is surprising about DOD's interim cyber rules is that they are data centric; the measures focus on categories of information, requiring contractors to better understand the kind and character of information that resides on or transits through their networks and information systems. To comply with the new rules, contractors must start by understanding the DOD's new terminology and examining their own information systems to identify weaknesses and gaps.

Covered Contractors

The DOD anticipates that these rules will impact approximately 11,000 contractors (including subcontractors), and anticipates the filing of over 60,000 annual cyberincident reports, each report requiring approximately four hours to research and prepare.

New Terms and Definitions

The DOD introduces several new terms, including (1) adequate security, (2) compromise, (3) contractor attributional/proprietary information, (4) contractor information system, (5) controlled technical information, (6) covered contractor information system, (7) covered defense information, (8) cyber incident, (9) forensic analysis, (10) information system, (11) malicious software, (12) media, (13) operationally critical support, (14) rapidly report(ing), (15) cloud computing, (16) government data, (17) government related data, and (18) spillage. These terms appear throughout the new regulations as well as the implementing contract clauses of which the DOD has added five new clauses.

Contractors large and small may own and operate a single fully integrated IT system that houses all programs and applications and all information without regard to the originating source of that information. Or, a company may actually have multiple IT systems (such as separate servers for email, accounting and operations) with each system holding discrete informational silos. Setting aside for the moment the risks and consequences associated with cyberattacks, both systemic approaches have their advantages and disadvantages in terms of simplicity, uniformity and cost of operation. But, when you factor in the many implications associated with a cyberattack, the functional vulnerabilities of a single IT system, and the benefits of segmented information systems, become apparent.

For one, an attacker can hack his way into all data stored or processed in a single system, whereas with segmented IT systems, the attacker must penetrate each system to access the data in those systems. Also, multiple IT systems (each geared toward storing or processing specific kinds of information, depending on the sensitivity of such information) allow the contractor to create tiered information and data storage systems with each system receiving an appropriate level of data security.

For example, a contractor arguably would not apply the same security restrictions to publicly available information as it would to controlled unclassified information even if both were provided by the government and were necessary to performance of work required under the contract. Instead of having to apply the same heightened level of cybersecurity to all information residing on a single contractor IT system, with multiple IT systems deployed the contractor can distribute information according to sensitivity and install appropriately rigorous (or not) cyber protection for each information system. This approach, sometimes referred to as “network segmentation,” invariably, makes sense for most contractors in most settings. With the interim rules now on the street, the DOD is steering contractors toward such segmentation.

Covered Contractor Information System and Covered Defense Information

The real benefit of this approach (creating segmented contractor IT systems) is self-evident under the interim rules. If contractor houses all information — including covered defense information — on a single IT system, then the entire system will be a covered contractor information system. But, if covered defense information resides on just one of several contractor IT systems, then contractors' compliance obligations under the interim rules have been reduced to just that single IT system and the information that resides on that system.

What is a covered contractor information system? It is “an information system that is owned or operated by or for, a contractor and that processes, stores, or transmits covered defense information.” DFARS 252.204-7012(a). In turn, covered defense information encompasses the following categories of unclassified information:

(i) Any information that is (A) provided to the contractor by or on behalf of DOD in connection with performance of the contract; or (B) collected, developed, received transmitted, used or stored by or on behalf of the contractor in support of performance of the contract; and

(ii) Encompasses any of the following: (A) controlled technical information, (B) critical information (for operations security); (C) export controlled information (D) any other information marked or otherwise identified in the contract, that requires safeguarding or dissemination controls (such as privacy information or proprietary business information).

As defined, covered defense information is any information furnished by the DOD for performance purposes or resides on a covered contractor information system (however received) in support of performance of the contract — and fits within one of the four defined subcategories of information.

Providing Adequate Security for Covered Defense Information and Covered Contractor Information Systems

The DOD retooled and renamed a pre-existing clause, DFARS 252-204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (August 2015), to cover the safeguarding of covered defense information residing on contractor (or subcontractor) information systems and to require contractors to report any “cyberincident.” Under this clause, contractors must provide “adequate security,” which means “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to or modification of information.” Contractors are called upon to make a judgment call as to the adequacy of protective measures given the consequences and probability of adverse outcomes were a cyberincident to occur.

Under this new safeguarding and reporting clause, contractors are required to provide adequate security “for all covered defense information on all covered contractor information systems that support the performance of work under the contract.” The DOD enumerates protective measures that, at a minimum, contractors are obligated to provide, depending on whether the contract calls for operation of a covered contractor information system that is (1) part of an information technology service or system operated for or on behalf of the government, or (2) not part of such a service or system.

Where the covered contractor information system is part of an IT service or system operated for or on behalf of the government, the contractor’s cloud computing services are subject to the requirements specified in DFARS 252.239-7010 Cloud Computing Services. Other contractor IT services or systems must meet such other “security requirements as are specified in the contract.”

For covered contractor information systems that are not part of an IT service or system operated for or on behalf of the government, the contractor must implement (1) the security protections specified in National Institute of Standards and Technology Special Publication (SP) 800-171 that is in effect as of the date of the solicitation or as authorized by the contracting officer; or (2) alternative but “equally effective” security procedures that achieve “equivalent protection” if it is unable to satisfy a particular NIST requirement — but those alternative protective measures must first be approved by an authorized

representative of the DOD chief information officer prior to contract award; and (3) any other security measures when the contractor "reasonably determines" that such measures may be required to provide reasonable security "in a dynamic environment based on an assessed risk or vulnerability."

The Process of Reporting Cyberincidents

The DOD contemplates receiving over 60,000 cyberincident reports annually, roughly 5,000 per month, 165 per day. To accommodate such a large volume of cyberincident reports, the DOD has established a cyberincident clearinghouse: http://dibnet.dod.mil.

To be clear, a cyberincident occurs anytime actions have been taken "through the use of computer networks that results in an actual or potentially adverse effect on an information system and/or the information residing therein." Thus, a cyberincident report is required anytime contractor discovers a cyberincident that affects or potentially affects (1) a covered contractor information system or (2) covered defense information residing therein, or (3) the contractor's ability to perform those requirements of the contract that are identified as operationally critical support.

In support of preparing and submitting a cyberincident report, contractors must do the following:

(1) Obtain a DoD-approved medium assurance certificate by providing the information specified at http://iase.disa.mil/pki/eca/certificate.html.

(2) Conduct a review of the cyber incident to identify evidence of compromise of covered defense information, including, without limitation, "identifying compromised computers, servers, specific data and user accounts." By necessity, the required review encompasses those covered contractor information systems that were part of the cyber incident as well as any other information systems on the contractor's network(s) that may have been accessed "in order to identify compromised covered defense information," or that affect contractor's ability to provide operationally critical support. DFARS 252.204-7012(c). Where malicious software has been discovered and isolated by contractor in connection with a reported cyber incident, the software must be submitted in accordance with instructions to be received from the contracting officer.

(3) Prepare and submit the cyber incident report, in all likelihood, with the assistance of outside information system specialists, such as a certified information systems security professional (CISSP).

(3) Protect and preserve images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from submission of the cyber incident report to allow DOD sufficient time to assess the situation and either request delivery of the media or decline interest. DFARS 252.204-7012(e).

(4) Upon request, provide DOD with access to additional information (beyond what has been reported to date) or equipment that is necessary to conduct forensic analysis, i.e., gathering, retaining and analyzing computer-related data for investigative purposes in a manner than maintains the integrity of the data. DFARS 252.204-7012(a), (f).

DOD Protection of Contractor Information

In making a cyberincident report, it may be necessary for contractor to disclose to the DOD "contractor attributional/proprietary information." When making its cyberincident report, it is incumbent on

contractors “to the maximum extent practicable” to identify and mark contractor attributional/proprietary information so that the DOD may implement appropriate procedures specified at DFARS 252.204-2009(b) to limit the release of such information in connection with expressly authorized purposes. DFARS 252.204-7012(h).

Reported Cyberincidents, Alone, Do Not Constitute Proof of Inadequate Security

In recognition that attackers have compromised even well-secured networks, the DOD acknowledges that reported cyberincidents do not constitute proof of inadequate security measures for covered defense information or covered contractor information systems. Cyberincidents are to be but one factor in the contracting officer’s overall assessment of compliance with the safeguarding clause. DFARS 204.7302(d). To conduct a proper assessment, the contracting officer is required to consult with the DOD “component CIO/cyber security office” in accordance with PGI 204-7303-3(a)(2). In contrast, however, one could naturally conclude from this regulation that a contractor’s failure to incorporate appropriate monitoring and detection activities into its information systems (such that a cyberincident goes undetected and unreported) may well constitute prima facie evidence of inadequate security measures and material noncompliance with the safeguarding clause.

Compliance and Conformance with Other Contract Terms and Applicable Laws

Contractors are reminded (by way of mandate) that these newly minted rules and contract provisions do not operate to the exclusion of still other cybersecurity requirements that may be recited in the same contract or, in other contracts. And, when implementing the new requirements in the interim rules, contractors must fully comply with all applicable laws pertaining to the interception, monitoring, access, use, and disclosure of electronic communications and data. DFARS 252.204-7012(k), (l).

Subcontractors at Every Level Affected

The many requirements enumerated in DFARS 252.204-7012(a) through (l) are required to be flowed down to first-tier and lower-tier subcontractors by operation of DFARS 252.204-7012(m) and DFARS 204.7302(a), (b). Subcontractors at every tier must implement appropriate safeguarding measures to adequately secure covered defense information on their covered contractor information systems. And, if a subcontractor at any tier discovers a cyberincident, it too must obtain a DOD approved medium assurance certificate, conduct appropriately scoped review of the cyberincident, prepare and submit a cyberincident report directly to the DOD’s cyberincident clearinghouse, and notify the higher-level contractor of the cyberincident report.

Public Comment Period

The public comment period for the interim rules closes 60 days after publication, meaning on or about Oct. 26, 2015. Potentially affected contractors should consider how these rules will impact their operations, information systems and cost of doing business, and submit formal comments expressing their views and offering suggestions for improvement. (Instructions for the many ways in which to communicate contractor comments are provided here.) In the absence of public comments from potentially affected contractors, the interim rules will not likely be materially altered before becoming final rules.

Conclusion

With these interim rules now in hand, contractors have been provided a clear indication of the direction that the DOD is going to protect covered defense information and covered contractor information systems. Now is the time for contractors to take a fresh look at their information systems and consider implementing structural changes to establish segmented networks or information systems to process and store the various categories of information with security measures based upon the sensitivity and source of such information. This may not be an inexpensive undertaking as a preparatory measure, but in the long haul it will likely save the company many times over from incurring far greater cost for damages caused by cyberincidents.

—By Hilary Cairnie and Randy Gainer, BakerHostetler

Hilary Cairnie is a partner in BakerHostetler's Washington, D.C., office and heads the firm's government contract team. Randy Gainer is a partner in the firm's privacy and data protection team in Seattle.