Bloomberg BNA

Federal Contracts Report™

Cybersecurity

'Adequate Security' and Full Disclosure: The DOD's New Cyber Rules for Contractors




BY RONALD D. LEE, CHARLES A. BLANCHARD, NICHOLAS L. TOWNSEND AND TOM MCSORLEY

Entering the cybersecurity fray alongside civilian agencies that have promulgated rules and guidance related to cybersecurity in recent months (including the FTC, FCC, SEC,[1] and OMB[2]), the Department of Defense (DOD) recently released its long anticipated cybersecurity rules governing contractors whose systems may touch certain defense-related information. The interim rules, which became effective on August 26, build on and expand previous, less comprehensive, cybersecurity regulations under the Defense Federal Acquisition Regulation Supplement (DFARS).

Contractors and subcontractors that may have ''covered defense information'' (a newly defined term that goes far beyond classified or even controlled technical information) transiting or residing on their systems[3] are subject to the new and significant ''adequate security'' and cyber reporting requirements. Because of the broad scope of ''covered defense information'', a wide range of DOD contractors and subcontractors, potentially including, for example, many commercial suppliers of DOD prime contractors are subject to the rules. Companies that do any DOD-related business must carefully assess whether they may have covered defense information transiting or residing on their systems and, if so, whether their covered systems and IT processes and personnel are prepared to meet the new requirements.

In brief, the interim rules:

[1] ''SEC Guidance, While Noting Potential Compliance Risks, Suggests Cybersecurity Framework for Investment Firms.''

Ronald D. Lee, a partner in Arnold & Porter's Government Contracts and National Security practice, advises and represents clients in national security, cybersecurity and privacy, and government contracts matters. Charles A. Blanchard is a partner in the firm's Government Contracts and National Security practices. Nicholas L. Townsend, a counsel in the firm's Government Contracts and National Security practices, has extensive experience in cybersecurity, export controls, trade sanctions, and intelligence information sharing. Tom McSorley, an associate in the firm's Government Contracts and National Security, and Telecommunications practices, focuses on the intersection of law and technology.

[2] ''New Proposed Regulations and Guidance for Federal Contractors: Complying With President Obama's Fair Pay and Safe Workplaces Executive.''

[3] *See* 80 Fed. Reg. 51739 (August 26, 2015), *available at* http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf.

 ISSN 0014-9063

■ Requires all DOD contractors and subcontractors that may have ''covered defense information'' residing on or transiting their systems (as detailed below) to implement ''adequate security'';

■ Includes a more specific definition than previous rules for ''adequate security,'' which, for most contractors and subcontractors, is based primarily on the National Institute of Standards and Technology (NIST) Special Publication 800-171;[4]

■ Provides offerors some flexibility in varying from the requirements of ''adequate security'' as defined in the rule (and justifying their variance), through an approval process, before entering into particular contracts or subcontracts;

■ Requires contractors and subcontractors to report any ''cyber incidents,'' which is a broadly defined term, that may have affected covered contractor systems and to provide significant information to the government about their systems if the government opens an investigation into any such incident;

■ Contains limitations on the use and disclosure of the cyber incident information collected by the government, and limits the use and disclosure of reported cyber incident information by contractors and subcontractors that support the government's activities related to safeguarding covered defense information and cyber incident reporting; and

■ Adds a number of new provisions to DFARS that address the acquisition and use of cloud computing services.

The interim rules are several years in the making. They meet the mandate for DOD to generate a new cybersecurity regime for defense contractors contained in both Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year 2013 and Section 11632 of the NDAA for Fiscal Year 2015.

The current regulatory focus on cybersecurity also follows the major breach of the Office of Personnel Management that was reported at the beginning of the summer. The new and expanded DFARS provisions, along with the multitude of other regulatory actions taken recently to address cybersecurity, underscore the need for companies—whether they operate primarily in the public or private sector—to recognize and respond to the current regulatory focus, across the federal government, on implementing information security controls and responding to cyber incidents.

The DOD's rule, along with the other recent regulatory activity, also raises a number of questions, including those related to how contractors are to deal with the inevitable conflicts that will arise between the need to protect sensitive and proprietary data and the need to report cyber incidents, and how to develop processes to address the potential need to report cyber incidents to multiple elements of the US government. Thus, the interim rules add an additional dimension to the debates playing out across the Executive Branch, and in Congress, state governments, and the private sector, over how best to balance security, privacy, and costs in light of growing cyber threats at home and abroad.

[4] ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'', *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

The interim rules are effective as of the publication date (August 26, 2015), but comments may be submitted on or before October 26, 2015, and these comments will be considered before the rule becomes final.

'Covered Defense Information.' Many of the provisions that were replaced or amended by the interim rules previously applied only to the protection of unclassified controlled technical information or ''UCTI.'' The new rule creates a new term, ''covered defense information,'' that encompasses UCTI and more. The interim rules apply to any ''covered contractor information system'' which means any information system that is owned, or operated by or for, a contractor and which processes, stores, or transmits covered defense information.

Under the rule, ''covered defense information'' means unclassified information provided to the contractor by or on behalf of the DOD in connection with performance of a contract *or* that is ''[c]ollected, developed, received, transmitted, used, or stored by or on behalf of [a] contractor in support of the performance of [a] contract'' and that falls into any of four categories. Two of the categories of information already carried cybersecurity obligations for contractors and subcontractors that may have such information transiting or residing on their systems:

■ ***Controlled Technical Information.*** Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions.

■ ***Export Control.*** Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

But two new categories of information within the definition of ''covered defense information'' have the potential to significantly expand the scope of covered systems, including a final ''catch-all'' provision that, if construed broadly, would likely cover many contractors and subcontractors that may not otherwise recognize they have sensitive information on their systems:

■ ***Critical Information (Operations Security).*** Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

■ ***Catch-all Provision.*** Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

'Adequate Security.' DFARS part 204.7304 now requires that all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures

  FCR ISSN 0014-9063

for the acquisition of commercial items, include the contract clause found at DFARS part 252.204-7012. That clause now has two main elements: a requirement that all contractors provide ''adequate security'' to covered defense information and that contractors report any cyber incidents.

First, the clause requires that contractors and subcontractors implement a minimum level of information system security protections on all covered contractor information systems. For covered contractor information systems that are part of an IT service or system operated by or on behalf of the government, the clause requires the implementation of the new cloud computing security requirements created by the interim rules (discussed below) or, otherwise, the security requirements specified in the relevant IT service or system contract.

For all other covered contractor information systems that are not part of an IT services contract, ''adequate security'' means complying with:

- The security requirements in NIST Special Publication 800–171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations''[5] that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer; *or*''Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the DOD CIO prior to contract award.''

The second definition of ''adequate security'' is implemented through new DFARS part 252.204-7008, which permits offerors to propose to deviate from any of the security requirements in NIST Special Publication 800-171. Offerors may do so by submitting to the relevant Contracting Officer, for consideration by the DOD Chief Information Officer, a written explanation of why a particular security requirement is not applicable or how an alternative, but equally effective, security measure will be used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection. Any approved deviation from NIST Special Publication 800–171 will be incorporated into the resulting contract.

Contractors and subcontractors must also apply additional other security measures when they reasonably determine that such measures may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. In other words, a contractor or subcontractor is not necessarily providing adequate security merely by relying on NIST Special Publication 800-171.

Cyber Incident Reporting. Alongside the ''adequate security'' requirements, the interim rules also require all contractors and subcontractors to report ''cyber incidents'' that are discovered on covered contractor information systems. A ''cyber incident'' is defined as any actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. The cyber incident reporting rule contains a number of specific requirements:

- First, in order to report cyber incidents under the rule, all contractors and subcontractors must obtain a ''DOD-approved medium assurance certificate[.]'' The details of this requirement are not yet available.

- When a contractor discovers a reportable cyber incident, they must conduct a review of any covered contractor information systems, as well as other information systems on the contractor's networks that may have been accessed as a result of the incident, for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts.

- Cyber incidents must be ''rapidly'' reported at http://dibnet.dod.mil/. The report will be treated as information created by or for the DOD. This website also includes detail on the specific elements required for any report.[6]

- Any contractor or subcontractor that discovers and isolates malicious software in connection with a reported cyber incident must submit the malicious software in accordance with instructions provided by the relevant Contracting Officer.

- When a contractor discovers a cyber incident the contractor must preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DOD to request the media in order to conduct a damage assessment, or to decline interest.

- Upon request by DOD, the contractor must provide DOD with access to additional information or equipment that is necessary to conduct a forensic analysis.

Limitations on Use or Disclosure of Cyber Incident Information. The interim rules also impose a number of limitations on when and how the government can use and disclose information it obtains in the course of a cyber incident report or investigation. In particular, the government is required to protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor). In order to protect such information, ''to the maximum extent practicable,'' contractors should identify and mark attributional/proprietary information.

Information that is obtained from the contractor (or derived from information obtained from the contractor) that is *not* created by the DOD may be released outside of DOD:

- ''To entities with missions that may be affected by such information;''

- ''To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;''

- ''Government entities that conduct counterintelligence or law enforcement investigations;''

- ''For national security purposes, including cyber situational awareness and defense purposes''; or

[5] *See* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

[6] *See* http://dibnet.dod.mil/staticweb/ReportCyberIncident.html.

■ ''To a support services contractor . . . that is directly supporting [g]overnment activities under a contract that includes the [DFARS] clause at 252.204–7009[.]''

Information that *is created* by or for DOD, which includes any information contained in a cyber incident report, may be used and released outside of DOD for these purposes and activities ''and for any other lawful [g]overnment purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the [g]overnment's use and release of such information.''

The interim rules also create DFARS 252.204-7009, which requires a new clause to be inserted into any contracts or subcontracts for services that include support for the government's activities related to safeguarding covered defense information and cyber incident reporting. The clause imposes additional obligations on such contractors or subcontractors, including that information obtained from a third-party's cyber incident report may only be used in support of certain authorized technical assistance and related activities, that the contractor will protect against its unauthorized release or disclosure, and that the contractor (including its participating employees) must be subject to a non-disclosure agreement between the contractor and the government before being provided any such information. The clause makes any third-party contractor that submitted a cyber incident report a third-party beneficiary to the required non-disclosure agreement. The provision also authorizes criminal, civil, administrative, and contractual actions, penalties, damages, and other remedies for the breach of these obligations.

Cloud Computing Provisions. Finally, the interim rules create a number of new provisions related to cloud computing and the government's acquisition of cloud computing services.

The rule broadly defines ''cloud computing'' as ''a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.''

Any offeror responding to a solicitation to provide information technology services to the DOD must state in its solicitation whether it does or does not anticipate that cloud computing services will be used in performance of the contract.

The rule imposes additional requirements on contractors and subcontractors that anticipate using cloud computing services in the performance of any DOD contract providing information technology services, including commercial contracts under FAR part 12. First, contractors must implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the DOD's Cloud Computing Security Requirements Guide (SRG).[7] Second, contractors using cloud computing services must maintain ''within the United States or outlying areas'' all government data that is not physically located on DOD premises, unless the contractor receives written notification from the government to use another location.

Conclusion. The interim rules contain many new requirements for DOD contractors, particularly IT services contractors, as they contemplate new and existing business with the government. It will also be important for all federal contractors to closely monitor the development of and interplay between these and other related cybersecurity regulations and guidance with respect to both the private sector and other elements of the federal acquisition system.

[7] *See* http://iase.disa.mil/cloud_security/Pages/index.aspx.

  FCR ISSN 0014-9063