COVINGTON

Final FAR Cyber Rule Issued on Safeguarding of Contractor Systems

May 16, 2016

Government Contracts

Today, the Department of Defense (DoD), General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) issued a Final Rule to add a new subpart and contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) "for the basic safeguarding of contractor information systems that process, store, or transmit Federal contract information." *See* 81 Fed. Reg. 30439 (May 16, 2016). The Rule imposes a set of fifteen "basic" security controls for contractor information systems upon which "Federal contract information" transits or resides. Federal contract information is defined as information provided by or generated for the Government under a contract to develop or deliver a product or service for the Government, but does not include either: (1) information provided by the Government to the public, such as on a website, or (2) simple transactional information, such as that needed to process payments. Based on the scope of the rule, the vast majority of federal contractors will be covered by this Rule once they accept the clause.

The Final Rule does not relieve obligations that a contractor may face for the safeguarding of other government information, including controlled unclassified information or covered defense information. Indeed, the Final Rule is only the first step in a number of interrelated regulatory actions being taken in the cybersecurity area. Last summer, the Office of Management and Budget (OMB) published Draft Guidance intended to improve and clarify cybersecurity protections in federal acquisitions. The Draft Guidance proposed direction to federal agencies on "implementing strengthened cybersecurity protections in Federal acquisitions for products or services that generate, collect, maintain, disseminate, store, or provide access to Controlled Unclassified Information (CUI) on behalf of the Federal government." CUI was defined in a recently issued proposed FAR rule as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The comments preceding the Final Rule explain that it is "intended to provide a basic set of protections for all Federal contract information, upon which other rules, such as a forthcoming FAR rule to protect CUI, may build." 81 Fed. Reg. 30441 (May 16, 2016). As noted in NIST Special Publication (SP) 800-171, a single FAR clause eventually will apply the full set of 800-171 requirements on contractors that have CUI on their systems. *See* NIST SP 800-171 (June 2015) at vi.

Background

Proposed FAR Rule

In August 2012, DoD, GSA, and NASA proposed a government-wide rule to address basic requirements for safeguarding contractor information systems (the "Proposed FAR Rule"). 77 Fed. Reg. 51,496, 51,497 (Aug. 24, 2012). The Proposed FAR Rule prescribed policies and procedures for protecting information "provided by or generated by the Government (other than public information) that will be resident on or transiting through government contractor systems." 77 Fed. Reg. 51498 (proposed FAR 4.1700). This proposed rule would have applied to all solicitations and contracts where a contractor's information systems may have contained nonpublic government information. 77 Fed. Reg. 51,496, 51,498 (scope of the Proposed FAR Rule included solicitations and contracts for commercial items and commercially available off-the-shelf items).

The Proposed FAR Rule included basic safeguarding requirements such as: (i) prohibiting contractors from processing nonpublic government information on publicly available computers and from posting such information on publicly available webpages; (ii) requiring contractors to maintain at least one physical or electronic barrier (*e.g.*, locked room or log-on procedure) between nonpublic government information and the public; (iii) protecting against network intrusion and data exfiltration; and (iv) encrypting all controlled unclassified information on mobile computing devices. 77 Fed. Reg. at 51,499. Many of these requirements have been modified in the Final Rule.

The Final Rule Focuses on Basic Controls for Safeguarding Contractor Information Systems Rather Than the Information Itself

FAR Definitions

The Final Rule adds a new clause - FAR 52.204-21 - which includes definitions for "covered contractor information system" and "Federal contract information" and deletes definitions for "public information" and other terms in the Proposed Rule except for "information," "information system," and "safeguarding." The Final Rule defines these terms as follows:

- Covered contractor information system - means "an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information." FAR 52.204-21(a).
- Federal contract information - means "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." It does "not include information that the Government has provided "to the public (such as on public Web sites)," or "simple transactional information, such as necessary to process payments." FAR 52.204-21(a). There is no requirement that the information be marked in any way by the Government.
- Information - is defined as any communication or representation of knowledge in any form, including audiovisual. FAR 52.204-21(a).
- Information System - is a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information." FAR 52.204-21(a). The comments preceding the Final Rule clarify that separately accredited information systems that "interface through loosely coupled

mechanisms such as email or Web-services will not be considered 'direct connections'" under the Final Rule. 81 Fed. Reg. 30441 (May 16, 2016).

- Safeguarding - is defined as "measures or controls that are prescribed to protect information systems." FAR 52.204-21(a).
- Residing and Transiting - information "residing on" an information system means information "being processed by or stored on the information system." 81 Fed. Reg. 30441 (May 16, 2016). Information "transiting through" an information system "means simple transport" (no local storage). *Id*.vv

Scope and Applicability

The Final Rule will apply to a contractor once it accepts a contract that contains FAR 52.204-21, "Basic Safeguarding of Covered Contactor Information Systems." *See* FAR 4.1903. The Government intends for this clause to be applied broadly because it "requires only the most basic level of safeguarding." 81 Fed. Reg. 30441 (May 16, 2016). Consequently, Contracting Officers are required to include FAR 52.204-21 in "solicitations and contracts when the contractor or a subcontractor at any tier *may have* Federal contract information residing in or transiting through its information system." FAR 4.1903 (emphasis supplied). Similarly, prime contractors must flow the substance of this clause to subcontractors (except for COTS suppliers) if that subcontractor "may have" Federal contract information residing in or transiting through its information systems. FAR 52.204-21(c). Although COTS items at both the prime and subcontractor level are excluded from coverage, the comments to the Final Rule explain that there may be "subcontracts for commercial items (especially services, e.g., a consultant) at lower dollar values that would involve covered contractor information systems. In such instances, it is still necessary to apply basic safeguards to such covered contractor information systems." 81 Fed. Reg. 30444 (May 16, 2016).

The focus of the Final Rule was shifted to safeguarding of contractor systems rather than specific government information. 81 Fed. Reg. 30441 (May 16, 2016). The Councils noted that the narrowing of requirements to a particular type of information would be appropriate for CUI and other more sensitive information, but not at this level of basic safeguarding requirements. *Id*.

Safeguarding Requirements

The Final Rule imposes 15 categories of security controls that contractors with Federal contract information on their information systems must, at a minimum, employ. FAR 52.204-21(b). The Final Rule "replaces the requirements in the proposed rule with requirements from NIST guidelines (NIST SP 800-171), which are appropriate to the level of technology, and are updated as technology changes." 81 Fed. Reg. 30442 (May 16, 2016). The full set of 800-171 security controls are imposed on Department of Defense contractors in DFARS 252.204-7012. *See* DFARS 252.204-7012(b)(1)(ii). Presumably, contractors that are in compliance with DFARS 252.204-7012 will be in compliance with this new FAR provision, but the Final Rule does not address this explicitly. Contractors will need to consult with their IT experts to confirm such compliance and factor in any 800-171 controls that the company may not have implemented yet given the December 2017 deadline. DFARS 252.204-7012(b)(1)(ii).

The basic safeguarding security controls imposed by the Final Rule are listed below. All of the security controls listed in the Final Rule are directed at protection of the system, and none are

devoted to perimeter devices, although some (see numbers 10 and 11 below) are applied at the perimeter of the system. 81 Fed. Reg. 30441 (May 16, 2016).

1. Limit access to authorized users.
2. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3. Verify controls on connections to external information systems.
4. Impose controls on information that is posted or processed on publicly accessible information systems.
5. Identify information system users and processes acting on behalf of users or devices.
6. Authenticate or verify the identities of users, processes, and devices before allowing access to an information system.
7. Sanitize or destroy information system media containing Federal contract information before disposal, release, or reuse.
8. Limit physical access to information systems, equipment, and operating environments to authorized individuals.
9. Escort visitors and monitor visitor activity, maintain audit logs of physical access, control and manage physical access devices.
10. Monitor, control, and protect organizational communications at external boundaries and key internal boundaries of information systems.
11. Implement sub networks for publically accessible system components that are physically or logically separated from internal networks.
12. Identify, report, and correct information and information system flaws in a timely manner.[1]
13. Provide protection from malicious code at appropriate locations within organizational information systems.
14. Update malicious code protection mechanisms when new releases are available.
15. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

FAR 52.204-21(b).

[1] The use of the term ”report” in this section presumably refers to internal reporting of information system flaws given the lack of any mention of reporting to the Government.

Comparison to DFARS Cybersecurity Provisions

Because many contractors will be subject to both the Final Rule and the DFARS rule, set forth below is a comparison of some of the key provisions from DFARS 252.204-7012 and FAR 52.204-21.

Requirement	FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems (May 2016)	DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2015)	Key Differences/Comments
Applicability	All solicitations and contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system. Does not apply to contracts or subcontracts for COTS items.	Applies to DoD solicitations and contracts and subcontracts, including those for the acquisition of commercial items. The safeguarding requirements apply to "covered defense information" residing in or transiting through covered contractor information systems. No exception for COTS items.	FAR rule excludes COTS contracts. DFARS rule applies only to DoD contracts, but some latitude for subcontractor flow down.
Scope	Applies to information systems that hold "Federal contract information," which is "information, not intended for public release, that is provided by or generated by the Government under a contract to develop or deliver a product or service to the Government." It does "not include information that the Government has provided to the public" or "simple transactional information, such as that necessary to process payments."	Applies to "covered defense information," which includes information provided to the contractor by or on behalf of DoD or "collected, developed, received, used or stored" in support of contract performance, which also falls within one of these four categories: (i) controlled technical information, (ii) critical information, (iii) export control information, as well as (iv) any additional information marked or otherwise identified in the contract that is subject to controls imposed by law, regulation, or government-wide policy.	FAR rule is limited to the information systems where Federal contract information transits or resides. DFARS rule applies to both covered defense information itself and the information systems on which covered defense information transits or resides. Both rules include within their coverage information provided by the Government to a contractor and information generated by a contractor during performance of a government contract. Neither rule requires any marking of data to identify it as Government information.
Security Requirements	Imposes 15 specific basic safeguarding requirements on information systems where Federal contract information resides or transits. Although	Imposes a requirements to have "adequate security." The clause defines the baseline security requirements depending on whether the	More extensive security controls required by the DFARS provision. DoD contractors have until December 2017 to

	not explicitly tied to particular 800-171 controls, the Final Rule characterizes them as "comparable."	information system is operated on behalf of the Government or is an internal contractor system. For systems operated on behalf of the USG, either the requirements in clause 252.239.7010 or for IT services other than cloud computing, "security requirements specified elsewhere in [the contract]." For systems not operated on behalf of the USG, contractors must implement: ▪ The security requirements in NIST SP 800-171; or ▪ "Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement" approved in writing by the DoD CIO. The contractor is also required to apply other security measures it deems necessary. Contractors have until December 2017 to fully implement 800-171 security controls.	implement 800-171 security controls on internal systems. In contrast, FAR requirements are imposed upon acceptance of the clause. Full 800-171 security controls are expected to be imposed on contractors with the final FAR CUI rule.
Cyber Incident Reporting	No reporting requirements to the Government.	Must "rapidly report" a cyber incident to http://dibnet.dod.mil within 72 hours of discovery.	No reporting requirements to the Government for the FAR rule. Such requirements may be included in the final CUI rule.
Post-incident Investigation	No requirement.	Contractors must preserve and protect images of all known affected information and systems for at least 90 days from reporting to allow DoD to determine whether it will conduct a damage assessment and provide DoD access to additional information or equipment necessary to	FAR rule does not provide the government any independent access to a contractor's information systems due to a cyber incident.

		conduct a forensic analysis. Contractors must submit to DoD any malicious software connected to the incident that was discovered and isolated.	
Subcontractors	Prime contractors are required to flow down the substance of the clause in all subcontracts (except those for COTS items).	Contractors are required to flow down the clause to (i) subcontracts for operationally critical support, or (ii) where subcontract performance will involve a covered contractor information system.	DFARS clause permits some flexibility in flowing down the clause to subcontractors.

If you have any questions concerning the material discussed in this client alert, please contact the following member of our Government Contracts practice group:

Susan Booth Cassidy +1 202 662 5348 scassidy@cov.com