WILMERHALE

Final Government Contractor Basic Data Security Rule Issued

MAY 17, 2016

Yesterday, the Federal Acquisition Regulations ("FAR") Council published the final FAR rule on Basic Safeguarding of Contractor Information Systems.[1] The rule is intended to prescribe "the most basic level" of safeguards, "reflective of actions a prudent business person would employ."[2]

Applicability

The rule, which includes a new contract clause, will apply to all acquisitions by any federal executive agency, beginning June 15, 2016, when a contractor's information system may contain "Federal contract information," including acquisitions below the simplified acquisition threshold and for commercial items other than commercially available off-the-shelf ("COTS") items.[3]

A key factor in applying the new rule is whether a contractor's information system contains "Federal contract information." That term is defined intentionally broadly as "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, but not including information by the Government to the public (such as that on public websites) or simple transaction information, such as that necessary to process payments."[4]The safeguarding requirements apply to all "covered contractor information systems," namely, those information systems owned or operated by a contractor that process, store, or transmit Federal contract information.[5]

The substance of the contract clause prescribed by the rule must be flowed down in all subcontracts, other than contracts for COTS items, in which the subcontractor may have Federal contract information residing in or transiting through its information systems.[6]

Safeguards

The contract clause requires contractors to implement fifteen specified safeguards, including access control; identification and authentication safeguards; media, physical, system, and communication protection; and system and information integrity. The fifteen safeguards are listed at the end of this discussion. Each of the listed safeguards is drawn from the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171,[7] which was intended to apply to more sensitive "Controlled Unclassified Information" ("CUI").

This is not the first time that NIST SP 800-171 has been used to impose requirements on federal contractors. Department of Defense ("DoD") contractors and subcontractors handling "Covered Defense Information" have until December 31, 2017 to fully implement all NIST SP 800-171 requirements on their covered systems pursuant to the recently implemented interim final DoD FAR Supplement ("DFARS") rule on *Network Penetration Reporting and Contracting for Cloud Services*.[8]Unlike the DFARS rule, the new FAR rule does not impose all NIST SP 800-171 requirements on covered entities, but instead draws upon the requirements of NIST SP 800-171 with the intent of reflecting basic good cyber practices. As such, many contractors and subcontractors are likely to be in compliance with the new FAR rule's requirements, particularly those contractors who are subject to the DFARS rule and are implementing NIST SP 800-171.

However, some safeguards mandated by the new FAR rule may present challenges for some contractors who do not currently have significant security safeguards. For example, contractors with information systems processing, storing, or transmitting Federal contract information will be required to:

- "Monitor . . . organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems."[9]
- "Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks."[10]
- "Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed."[11]

While there are a variety of ways to implement these requirements, some companies subject to the rule may not meet these requirements and will have to upgrade their security practices accordingly.

One of the requirements is to "[i]dentify, report, and correct information and information system flaws in a timely manner."[12] In response to comments on the proposed rule suggesting imposing additional requirements, including an incident detection, reporting, and response requirement, the Federal Register notice states that "[t]his rule establishes minimum standards for contractors' information systems that process, store, or transmit Federal contract information where the sensitivity/impact level of the Federal contract information being protected does not warrant a level of protecting necessitating . . . detecting, reporting, and responding to security incidents . . ."[13] The scope of the requirement to report information and information systems flaws is unclear, but these official comments suggest that the requirement may be an internal reporting requirement and not a requirement to report flaws to the contracting agency.

Looking Forward

- ***Focus on Information Systems Rather than Information***. The most significant change between the final rule and the proposed rule, published in 2012,[14] was the shift in focus from protecting specific types of information to protecting the systems processing, storing, or transmitting that information. This is consistent with the construct in the DFARS rule, and may reflect a new government approach that will be carried through in future rulemaking,

including pending rules from the National Archives and Records Administration ("NARA"), discussed below.

- ***Compliance and Enforcement***. The new rule does not include any new compliance or monitoring mechanisms. However, contractors failing to comply with the rule could be subject to liability under existing laws and regulations, such as the False Claims Act. Notably, one of the comments on the proposed rule expressed concern that an inadvertent release of information "could be turned into not only an information security issue but also a potential breach of contract." In response, the Federal Register notice states that, "[g]enerally, as long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract."[15]
- ***Other Contractor Data Security Rules and Requirements***. The Federal Register notice notes that this rule is being issued as "just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems."[16] The notice specifically highlights the draft Office of Management and Budget ("OMB") guidance issued last summer regarding the protection of CUI (which recommended requiring contractor compliance with all of NIST SP 800-171 for contractors handling CUI),[17] a rule addressing CUI being finalized by NARA, eventual FAR Council coordination and implementation when the OMB guidance and NARA rule are finalized, and the DFARS interim rule.[18] As such, this rule establishes a baseline, and "does not relieve [] contractor[s] of any specific safeguarding requirement[] specified by Federal agencies and departments as it relates to covered contractor information systems generally or other Federal requirements for safeguarding [CUI]."[19] Contractors should continue monitoring other developments, as well as reviewing any clauses regarding the protection of information or data security requirements that may be included in their contracts.

Full List of Safeguards

The rule requires covered contractor information systems to include, at a minimum, the following security controls:

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems);
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute;
- Verify and control/limit connections to and use of external information systems;
- Control information posted or processed on publicly accessible information systems;
- Identify information system users, processes acting on behalf of users, or devices;
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems;
- Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse;
- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals;
- Escort visitors and monitor visitor activity; maintain audit logs of physical access; and

control and manage physical access devices;

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems;
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks;
- Identify, report, and correct information and information system flaws in a timely manner;
- Provide protection from malicious code at appropriate locations within organizational information systems;
- Update malicious code protection mechanisms when new releases are available; and
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.[20]

---

[1] 81 Fed. Reg. 30439 (May 16, 2016), available here.

[2] *Id*. at 30440-41.

[3] FAR § 4.1902.

[4] *Id*. §§ 4.1901, 52.204-21(a).

[5] *Id*.

[6] *Id*. § 52.204-21(c).

[7] NIST SP 800-171 is available here.

[8] 80 Fed. Reg. 81472 (Dec. 30, 2015), available here. For more information on the DoD interim final rule, see our previous alert, available here.

[9] FAR § 52.204-21(b)(x).

[10] *Id*. §52.204-21(b)(xi).

[11] *Id*. § 52.204-21(b)(xv) (emphasis added).

[12] *Id*. § 52.204-21(b)(xii) (emphasis added).

[13] 81 Fed. Reg. at 30443-44.

[14] 77 Fed. Reg. 20881 (Aug. 24, 2012), available here.

[15] 81 Fed. Reg. at 30444.

[16] *Id*. at 30440.

[17] The draft guidance is available here. For more information about the draft guidance, view the recording and materials from the recent installment of our Cybersecurity, Privacy and

Communications Webinar Series: *Recent Data Security Developments for Government Contractors*, available here.

[18] 81 Fed. Reg. at 30440.

[19] *Id*.

[20] FAR § 52.204-21(b).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Stephen W. Preston

PARTNER

Chair, Defense, National Security and Government Contracts Practice

stephen.preston@wilmerhale.com

+1 202 663 6900

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195