AN A.S. PRATT PUBLICATION
JULY 2018
VOL. 4 • NO. 7

# PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

# PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 4 NUMBER 7 JULY 2018



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at ..... 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



*An A.S.Pratt® Publication*

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub.4938)

# *Editor-in-Chief, Editor & Board of Editors*

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc.  For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

# U.S. Government's New Focus on Cybersecurity

***By Kyle R. Jefcoat, Dean W. Baxtresser, Morgan L. Maddoux, and Shira Epstien Hollander****

*In recent years, the government has made significant strides in strengthening cybersecurity requirements for contractors. This article describes the basic parameters of the Federal Acquisition Regulations Rule; the Defense Federal Acquisition Regulation Supplement Rule; President Trump's Executive Order; and additional regulatory changes that are on the horizon in the realm of cybersecurity for contractors.*

As recently as several years ago, the U.S. government's requirements for contractors regarding cybersecurity were fairly minimal and were considered by many to be outdated—particularly in light of the increasing cybersecurity threats individuals, corporations and governments all face. In recent years, however, the government has made significant strides in strengthening these types of requirements for contractors. Thus, virtually overnight (in government terms), government contracting regulatory requirements regarding cybersecurity have gone from practically nothing to a relatively extensive regulatory and contractual regime applicable to a broad range of government contracts. Compliance with these requirements is now a critical part of many government contractors' operations.

The process of creating the government's cybersecurity regulations began in earnest in August 2012, when the Department of Defense ("DOD"), General Services Administration ("GSA") and the National Aeronautics and Space Administration ("NASA") proposed a government-wide rule that was essentially the first attempt to address the safeguarding of contractor information systems in the Federal Acquisition Regulations ("FAR").[1] The proposed rule

---

* Kyle R. Jefcoat, counsel at Latham & Watkins LLP and a member of the Board of Editors of *Pratt's Government Contracting Law Report*, practices in the area of government contracts including compliance, bid protests, and False Claims Act litigation. Dean W. Baxtresser is an associate at the firm specializing in government contracts litigation and corporate compliance. Morgan L. Maddoux is an associate at the firm focusing her practice on white collar defense, internal and government investigations, and compliance matters in the healthcare industry. Shira Epstien Hollander is senior associate director of policy development at the American Hospital Association. The Latham & Watkins authors may be reached at kyle.jefcoat@lw.com, dean.baxtresser@lw.com, and morgan.maddoux@lw.com, respectively.

[1] *See* Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51,496 (Aug. 24, 2012).

required only that contractors "provide protective measures to information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems" in certain areas.[2] That proposed provision—weak as it was—was not enacted.

However, as cyber incidents impacting both government agencies and government contractors continue to make headlines, cybersecurity has become an increasing concern among government contractors which often possess sensitive government information. In response to these continued and increasing threats, the government imposed new requirements on contractors in the FAR and in the Defense Federal Acquisition Regulation Supplement ("DFARS") regarding the safeguarding of contractor information systems that may store, transmit, or process government data. President Trump also last year issued Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which suggests that the government will remain focused on this area and that there will likely be additional changes to cybersecurity requirements for government contractors in the future.

The new FAR and DFARS provisions modify and greatly strengthen the basic requirements set forth in that original proposed FAR provision by imposing far more stringent requirements on virtually all contractors and aiming to ensure the safeguarding of government data that is stored, transmitted, or processed on contractor information systems.

Furthermore, while the FAR and DFARS rules—and other federal cybersecurity requirements—are continuing to change and evolve, contractors will be required to certify compliance with those requirements and potentially be subject to compliance enforcement either through contractual obligations or potentially through anti-fraud mechanisms such as the False Claims Act ("FCA").[3]

This article describes the basic parameters of the FAR Rule; the DFARS Rule; President Trump's Executive Order; and additional regulatory changes that are on the horizon.

## THE FAR RULE

### Application

On May 16, 2016, the agencies issued a final rule amending the FAR that added a new FAR Subpart 4.19 and a new contract clause FAR 52.204-21 ("FAR Rule"). The focus of the new provisions is the basic safeguarding of

---

[2] 77 Fed. Reg. at 51,497.

[3] *See* 31 U.S.C. § 3729 *et seq.*

contractor information systems—in other words the processes and devices that store or host information rather than the information itself—that contain "Federal contract information," defined 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."[4] Commenters on the proposed FAR rule expressed concern that "the rule would cover nearly all information and all information systems of any company that holds even a single Government contract."[5] In response, when the final FAR Rule was published, the DOD, GSA, and NASA explained: "The intent is that the scope and applicability of this rule be very broad, because this rule requires only the most basic of safeguarding. However, applicability of the final rule is limited to covered contractor information systems, *i.e.,* systems that are owned or operated by a contractor that process, store, or transmit Federal contract information."[6] In short, the FAR Rule's focus on protecting "information systems," rather than protecting the more broadly defined "information" covered by the provision was meant to alleviate the burden on contractors who anticipated that nearly all information in company systems would have been regulated. However, because the provision applies broadly, it is likely that most government contractors, because they own or operate at least some covered "contractor information systems," will be subject to the new FAR Rule.[7]

The FAR Rule also applies to all acquisitions including commercial items (other than commercial off-the-shelf ("COTS") items) and to all systems that process, store or transmit "Federal contract information."[8] The FAR Rule expressly excludes information that the government provides to the public or simple transactional information used, for example, to process payments.[9]

**Requirements**

The FAR Rule's new clause, at FAR 52.204-21(b), mandates that contractors implement 15 "minimum" security controls on covered systems to satisfy the FAR Rule's requirement that contractors provide a basic level of "safeguarding" of federal contract information. It states:

> Requirements and procedures for basic safeguarding of covered con-

---

[4] *See* FAR 4.1901.

[5] *See* 81 Fed. Reg. 30,439, 30,440 (May 16, 2016).

[6] 81 Fed. Reg. at 30,441.

[7] *See* 81 Fed. Reg. at 30,441.

[8] *See* FAR 52.204-21(a).

[9] *See* FAR 52.204-21(a).

tractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) 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.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

> (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.[10]

The FAR Rule directs that new clause FAR 52.204-21 be flowed down to all levels of subcontracts, and be included in *all* "solicitations and contracts when the contractor or a subcontractor at any tier *may have* Federal contract information residing in or transitioning through its information system."[11] Notably absent from this list of 15 requirements are any specifics regarding contractors' post-incident investigation and reporting obligations. The FAR Rule also does not specifically address cloud computing or prescribe any controls that directly address the use of cloud solutions. However, the Preamble to the FAR Rule did include a note that it will not be the last word on cybersecurity requirements for contractors, but rather is "just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems."[12]

**Industry Reaction**

Some commenters to the FAR Rule criticized it for being too broad, too vague or too unsophisticated, all of which could prevent the rule from achieving its intended purpose, while simultaneously prompting contractors to design overly stringent security standards so as to avoid disputes with the government.[13] Commenters representing small businesses were particularly concerned about the cost of complying with broad safeguarding requirements that they do not necessarily employ as part of routine business practice.[14]

## DFARS FINAL RULE

In contrast to the new FAR requirements described above, the DFARS requirements impose stricter standards on defense contractors.[15] On October 21, 2016, the DOD issued a final rule which made changes to a prior interim rule and included amendments to multiple DFARS provisions including, most significantly, modifications to DFARS 252.204-7012, Safeguarding Covered

---

[10] FAR 52.204-21(b)(1).

[11] FAR 4.1903 (emphasis added); *see also* 81 Fed. Reg. at 30,446.

[12] 81 Fed. Reg. at 30,440.

[13] *See* 81 Fed. Reg. at 30,440, 30,443.

[14] *See* 81 Fed. Reg. at 30,444–45.

[15] The first version of DFARS 252.204-7012 was initially promulgated in 2013. *See* 78 Fed. Reg. 69,273, 69,280 (Nov. 18, 2013). This article does not describe all of the interim changes in the DFARS standard contract clause, and instead focuses on describing the current rule.

Defense Information and Cyber Incident Reporting ("DFARS Rule").[16] The DFARS Rule imposed safeguarding and cyber incident reporting obligations on contractors who have contracts with DOD and whose information systems process, store, or transmit "covered defense information" ("CDI").[17] While the DFARS Rule generally took effect immediately, one of its major changes—requiring contractors to comply with the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171—did not take effect until December 31, 2017. As explained below, the DFARS Rule

> (A) implements requirements for contractors to provide adequate security to covered information systems;
>
> (B) establishes certain benchmarks for compliance;
>
> (C) imposes obligations to investigate and report cyber incidents; and
>
> (D) creates flow-down obligations for prime contractors.

**Requirements to Provide Adequate Security**

DFARS 252.204-7012 requires contractors to have "adequate security" on all covered contractor information systems,[18] and applies to all solicitations and contracts, including those for commercial items (other than COTS items).[19] In particular, the DFARS Rule focuses on protecting CDI—which it defines broadly.[20] CDI includes both information that the government marked as CDI

---

[16] 81 Fed. Reg. 72,986 (Oct. 21, 2016).

[17] *See* 81 Fed. Reg. at 72,998. "Covered defense information" ("CDI") is defined as "unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry, http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DOD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

[18] DFARS 252.204-7012 defines the term "covered contractor information system" as "unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

[19] *See* DFARS 252.204-7012; *see also* Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 and DFARS Subpart 239.76 and PGI Subpart 239.76 ("DFARS FAQs") (Jan. 27, 2017), http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf.

[20] Contractors should note that the CUI Registry contains a broad range of categories and subcategories of information that is now considered CDI. For example, the CUI Registry

and information that the contractor "collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract."[21] However, at DOD's Industry Day on June 23, 2017, DOD representatives took the position that CDI "in support of the performance of the contract . . . is not meant to include a contractor's internal information (e.g., human resources or financial) that is incidental to contract performance."[22]

For contractors subject to both the DFARS Rule and the FAR Rule, the DFARS Rule imposes more extensive security controls and requirements than the FAR Rule. Specifically, the DFARS Rule requires the investigation and reporting of cyber breaches—requirements that are not included in the FAR Rule.

Significantly, the DFARS Rule defines the basic security requirements a defense contractor must implement and maintain. With the exception of cloud service providers ("CSP") using a cloud solution to store data on DOD's behalf—who have to comply with DFARS 252.239-7010, Cloud Computing Services[23] —as of December 31, 2017, a defense contractor generally must implement the security requirements in the version of NIST SP 800-171[24] then in effect at the time of the solicitation.

The NIST SP 800-171 security requirements[25] were developed for use on contractors' internal systems and were expected to enable contractors to comply using systems and practices that they already have in place rather than forcing

---

includes a "Privacy" as a category with several subcategories, including "Health Information" and "Student Records," which are two types of information one would not traditionally view as covered defense information.

[21] DFARS 252.204-7012(a).

[22] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 25, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[23] DOD has also provided additional guidance on when DFARS 252.239-7010 may apply: "DFARS clause 252.239-7010 is included in contracts for information technology services and applies when a contractor is using cloud computing to provide information technology services to DOD in the performance of the contract. It does not apply to cloud computing data centers operated as an extension of a contractor's internal IT system. DFARS clause 252.204-7012 is included in all DOD contracts (except those solely for COTS items) and a reference to DFARS clause 252.239-7010 is provided at paragraph (b)(1)(i) to notify contractors of the security requirements that must be followed when DoD is contracting for cloud services." *Id.* at 26.

[24] NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, http://dx.doi.org/10.6028/NIST.SP.800-171.

[25] *See* DFARS FAQs at 12.

them to build a new system and develop practices from scratch in order to be in compliance.[26] DOD further provided guidance that contractors who were in compliance with the previous security requirements can accomplish compliance with the NIST SP 800-171 requirements "by policy/process changes or adjusting the configuration of existing IT."[27] Of course, as discussed below, the practical reality of these additional requirements is that some contractors will likely need to make substantial investments in protecting their own IT systems in order to comply with the specific requirements under NIST SP 800-171. This may be particularly burdensome for smaller businesses and for contractors who were previously not subject to many cybersecurity requirements due to the type of information being exchanged, but who now find this information falling under the broad scope of CDI.

**Potential Steps for Complying with DFARS 252.204-7012**

Below, we outline several steps contractors should consider taking when addressing the compliance requirements of the DFARS Rule. These steps are based not only on the text of DFARS 252.204-7012 and DFARS Part 4, but also on additional guidance that DOD has issued since the DFARS Rule was published in October 2016. This additional guidance comes from several meetings and publications issued by DOD including:

- On June 23, 2017, DOD held an Industry Day during which it addressed cybersecurity challenges and went over the new DFARS rules.
- On September 21, 2017, the Director of the Defense Pricing/Defense Procurement Acquisition Policy ("DPAP") issued guidance ("DPAP Memo") to DOD acquisition personnel in anticipation of the December 31, 2017 deadline for contractors to be in compliance with DFARS 252.204-7012.[28]
- On November 28, 2017, NIST released a draft SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, the goal of which is to better educate contractors, third parties and

---

[26] *See* DFARS FAQs at 12.

[27] DFARS FAQs at 13. One addition to the security requirements that could require additional software or hardware is the implementation of multifactor authentication, which DOD discusses in more depth in its FAQs. DOD also sets forth a reasonable approach for how companies unfamiliar with or new to the requirements can evaluate and come into compliance.

[28] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

government agencies on SP 800-171's requirements.[29] This guidance outlined ways in which a contractor can come into compliance with the requirements.

- On December 1, 2017, DOD's office of Defense Procurement and Acquisition Policy updated its Procedures, Guidance, and Information ("PGI") with guidance regarding DFARS 252.204-7012.[30] Though the PGI is internal guidance for DOD contracting officers, it provides contractors with insight into how DOD interprets and plans to apply DFARS 252.204-7012.
- On April 2, 2018, DOD issued a Frequently Asked Questions ("FAQs") regarding the DFARS Rule.[31] This updated a prior set of FAQs issued in January 2018, and provides additional guidance on the implementation of these requirements.

Perhaps the most significant result of all of this additional guidance was to clarify that the DFARS Rule requirement that contractors "implement" NIST 800-171 did not mean full compliance with NIST 800-171 was required before the December 31, 2017 implementation deadline. The DPAP Memo explains that to "implement NIST 800-171" a contractor must have implemented a System Security Plan ("SSP") and a Plan of Action and Milestones ("POA&M") reflecting the extent to which a contractor currently complies with NIST 800-171 and its plan to come into full compliance.[32] DOD's definition of "implementation of the NIST 800-171" to include a plan to remedy

---

[29] Ron Ross, *et al.*, Assessing Security Requirements for Controlled Unclassified Information, Draft NIST Special Publication 800-171A (Nov. 2017), https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf.

[30] *See* DOD's Office of Defense Procurement and Acquisition Policy Procedures, Guidance, and Information ("PGI") (revised Dec. 1, 2017), https://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/current/PGI204_73.htm.

[31] *See* DOD's Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76, https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf.

[32] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf. ("To document implementation of the NIST 800-171 security requirements by the December 31, 2017, implementation deadline, companies should have a System Security Plan in place, in addition to any associate plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems.").

non-compliance may continue to apply even after the December 31, 2017 implementation deadline. However, as more time passes since that original implementation deadline, it is not clear if DOD will change its position as to what "implementation of NIST 800-171" means. In other words, DOD may require that contractors certifying compliance to the DFARS Rule after December 31, 2017 actually have full compliance with the NIST 800-171 standard rather than just a plan to come into compliance.

The DOD guidance also explained that the DOD entity is responsible for making clear to defense contractors what contract information is considered by DOD to be CDI. In particular, this guidance addresses the breadth of the DFARS Rule's definition of CDI, which includes not only information affirmatively designated as CDI by the DOD agency, but also information "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[33] The DPAP Memo explained that DOD is responsible for informing the contractor what information is CDI.[34] Moreover, the PGI issued by DPAP clarifies that the government is required to provide "a work statement or specification that includes identification of covered defense information or operationally critical support."[35] However, in its FAQs, DOD once again emphasized that CDI would still include information "developed, produced or used by a contractor . . . in performance of the contract and exclude other information that may be developed by the contractor but not associate with contract performance."[36]

Based on the new DFARS Rule and this updated guidance, contractors should consider taking steps now to ensure compliance with the DFARS Rule including:

- Examine the requirements of DFARS 252.204-7012 to determine which requirements the contractor meets and where there are gaps in the contractor's systems.
- Assess compliance with NIST SP 800-171. In particular, while NIST's November 28, 2017 SP 800-171A is still in draft form, contractors

---

[33] DFARS 252.204-7012(a).

[34] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[35] DOD's Office of Defense Procurement and Acquisition Policy Procedures, Guidance, and Information ("PGI") (revised Dec. 1, 2017), https://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/current/PGI204_73.htm.

[36] DOD's FAQs (Q29), https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf.

should consult this guidance, among other resources, when evaluating compliance with NIST SP 800-171.

- Consider whether to submit a written request to the contracting officer to implement an "[a]lternative but equally effective, security measure"[37] rather than be subject to NIST SP 800-171. However, it is not immediately clear what alternative measures would satisfy this requirement given the broad nature of the NIST SP 800-171 requirements.
- Determine whether additional requirements apply. For example, the preamble to the DFARS Rule indicates that the security requirements from the Committee on National Security Systems ("CNSS") Instruction No. 1253, based on NIST SP 800-53, apply to DOD internal information systems.[38] Other agency-specific requirements may also apply, particularly if the contractor is performing government contracts for civilian agencies as well as for the DOD.
- In addition to compliance with either NIST SP 800-171 or "equally effective security measures," contractors must also implement other security measures that a contractor deems necessary.
- Make applicable changes to policies, IT configuration, and adding software and hardware to support increased protection of CDI, as needed.
- Develop an SSP to document implementation of NIST SP 800-171.[39] The SSP is specifically required by Contracts that incorporate NIST SP 800-171, revision 1—which was finalized in December 2016. Moreover, even for contracts that do not incorporate NIST SP 800-171, revision 1, DOD recently issued guidance that provides: "[e]ven without Revision 1 of the NIST SP 800-171—the contractor may still document implementation of the security requirements with a system security plan."[40]

---

[37] DFARs 252.204-7012(b)(2)(i)-(ii).

[38] *See* DFARS FAQs at 11.

[39] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[40] Note Regarding NIST Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Security Requirement 3.12.4, System Security Plan, http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-11/Note%20Regarding%20NIST%20Special%20Publication%20800-171%20System%20Security%20Plan.pdf.

- If the contractor's request to use an "alternative but equally effective, security measure" is favourably adjudicated, the contractor should include the DOD's assessment to this effect in the contractor's SSP.[41]
- Develop a plan of action and milestones to implement the requirements and document any "plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when [a contractor] will correct deficiencies and reduce or eliminate vulnerabilities in the systems."[42] A contractor can document their SSP and plans of action as separate or combined documents and in any chosen format.
- Retain copies of the SSP and any associated plans of action in the event the responsible federal agency representative or contracting officer requests these documents. These documents can help demonstrate the contractor's implementation or planned implementation of the security requirements.[43] The DOD has indicated that the responsible federal agency may consider an offeror's implementation of NIST SP 800-171 in the source selection process in a few key ways, including establishing the implementation of NIST SP 800-171 as a separate technical evaluation factor, so contractors will want to retain all applicable documents to show their compliance with NIST SP 800-171.[44]
- Mark any SSPs or plans of action as "Confidential" or "Proprietary," as appropriate, to protect company sensitive information that would otherwise potentially be incorporated as part of the contract and potentially available to the public.[45]

Contractors should note that, by submitting a proposal to a solicitation that contains DFARS 252.204-7012 after December 31, 2017, they are representing

---

[41] *Id.*

[42] *See* NIST SP 800-171, Security Requirement 3.12.2; *see also* Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[43] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 61, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[44] *Id.* at 62.

[45] Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, Office of the Under Secretary of Defense, September 21, 2017, https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

that they are in compliance with the requirements.[46] While this is currently a self-certification process and the DOD may not be independently certifying that a contractor is compliant with the security requirements,[47] contractors must still be prepared for later audits or government reviews and investigations. Because of this potential future liability, audits, and investigations, contractors may consider engaging consultants to perform independent assessments of their cyber-security systems and defenses and to make recommendations regarding changes needed to achieve full compliance.

**Investigating and Reporting: What to Do After a Breach**

With the new FAR and DFARS cybersecurity requirements, the question most asked by government contractors is what obligations they now have in the case of a cyber incident or breach. The new FAR clause, FAR 52.204-21, does not expressly require contractors to investigate and report cyber incidents to the government.[48] In contrast, the DFARS Rule imposes extensive and immediate investigation and reporting requirements on defense contractors after a cyber incident occurs.

DFARS 252.204-7012 defines a "cyber incident" as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." The DFARS clause provides extensive requirements for contractors regarding the investigation and reporting of cyber incidents after discovery, most notably a requirement that contractors report cyber incidents within 72-hours of discovery. Some commenters to the interim DFARS rule expressed concern that the 72-hour reporting requirement was unrealistic and unduly burdensome;[49] however, the DOD did not change the final DFARS

---

[46] *Id.*

[47] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 60, *available at* http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.; *see also* Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, at 25, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940 (indicating that the Defense Contract Management Agency will have a role in verifying: (1) that appropriate contract clauses are included in agreements; (2) contractors have a system security plan; and (3) that contractors have DoD approved External Certificate Authority issued medium assurance public key infrastructure certificate.).

[48] Note that new FAR 52.204-21 does not supersede or otherwise impact any other FAR clauses that may be included in government contracts. Contractors should continue to ensure that they are in compliance with all FAR provisions included in their government contracts.

[49] *See* 81 Fed. Reg. at 72,991.

Rule based on these comments, instead reemphasizing the need for rapid reporting of cyber incidents.

Upon discovery of a cyber incident, DFARS 252.204-7012 imposes potentially burdensome requirements on the contractor to investigate and report the breach. Specifically, the contractor must:

- Conduct a review for evidence of compromised CDI, including identifying compromised computers, servers, specific data, and user accounts. Evidence of "compromise" includes, but is not limited to: disclosure of information to unauthorized persons; violation of a system security policy; unauthorized intentional or unintentional disclosure, modification, destruction or loss of an object; and copying information to unauthorized media.[50] This review shall include analyzing covered contractor information systems and other related systems that were part of the cyber incident in order to identify compromised CDI.[51]
    - Some industry stakeholders advocate for companies reporting every piece of evidence of compromise, even if it is minor, so as to avoid an allegation that the company hid any part of a breach. Other participants in the industry have recommended documenting every aspect of a review so that the company can demonstrate the company's compliance with the DFARS Rule if requested.[52]
- Report to the DOD within 72-hours of discovery of any cyber incident.[53] This report should include the required elements specified by the DFARS clause and applies to contractors at both the prime and the sub level.[54] The DOD clarified with the Final DFARS Rule that it anticipates a piecemeal approach to this reporting. Thus, if the contractor does not have all of the information required within 72-hours of discovery, then they should submit an initial report and supplement it with added information.[55]

---

[50] *See* 81 Fed. Reg. at 72,991.

[51] *See* DFARS 252.204-7012(c)(1)(i).

[52] *See* "Cybersecurity for Government Contractors: Preparing for Cyber Incidents in 2017," A Live Webinar (2017), https://www.bdo.com/getattachment/Insights/Business-Financial-Advisory/Cybersecurity-for-Government-Contractors-Next-Ste/ADV_Cybersecurity-GovCon_Cybersecurity-for-Gov-Con_2-18-(1).pdf.aspx.

[53] Report incident at https://dibnet.dod.mil.

[54] DFARS at 252.204-7012(c)(1)(ii).

[55] *See* DFARS FAQs at 17.

- Acquire and maintain a DOD-approved "medium assurance certificate" to report cyber incidents.[56]
- Submit any malicious software, to the extent the contractor discovers any malicious software related to the cyber incident, to the DOD Cyber Crime Center ("DC3") in accordance with the instructions provided by DC3 or the contracting officer.[57]
- Preserve and protect images of all known affected information and systems for at least 90 days from submission to allow DOD to determine whether it will conduct a damage assessment.[58] Companies may want to align their record retention policies with this 90 day requirement and should consider, in advance of any breach, how to clearly and consistently mark attributional and proprietary information in order to best protect it.[59]
- Provide DOD with access to additional information or equipment necessary to conduct a forensic analysis.[60]

Contractors may want to involve counsel early on in the breach investigation and reporting process to better understand their obligations, coordinate post-incident investigations, preserve legal privilege, and help address communication and any issues between prime- and sub-contractors.[61]

**Prime Contractors Must Flow Down DFARS 252.204-7012 and Associated Clauses, Where Applicable**

In addition to directly complying with these additional cybersecurity requirements, contractors are now responsible for ensuring that subcontractors are aware of these requirements and agree to comply with them. In the final DFARS Rule, DOD clarified that the DFARS Rule directs that DFARS 252.204-7012 be flowed down to all subcontracts for "operationally critical support, or for which subcontract performance will involve 'covered defense

---

[56] Contractors or subcontractors seeking information regarding obtaining a medium assurance certificate can visit http://iase.disa.mil/pki/eca/Pages/index.aspx.

[57] DFARS at 252.204-7012(d).

[58] DFARS at 252.204-7012(e).

[59] *See* "Cybersecurity for Government Contractors: Preparing for Cyber Incidents in 2017," A Live Webinar (2017).

[60] DFARS at 252.204-7012(f).

[61] *See* "Cybersecurity for Government Contractors: Preparing for Cyber Incidents in 2017," A Live Webinar (2017).

information.' "[62] At the DOD's June 23, 2017 Industry Day, the DOD recommended that a prime contractor minimize the provision of CDI to subcontractors unless the information is required for subcontractor performance. Additionally, if a subcontractor does not agree to comply with the terms of DFARS 252.204-7012 for any reason, the prime contractor should not share CDI with the subcontractor or otherwise allow the information to reside on the subcontractor's system(s).[63] If a defense contractor is unsure when it needs to flow down this requirement to subcontractors, the DFARS Rule encourages contractors to consult with the contracting officer.[64]

More specifically with regard to the incident reporting requirements, defense contractors should also be flowing down the DFARS Rule and additional language to require that subcontractors rapidly report cyber incidents directly to the DOD and provide the DOD-assigned incident report number to the prime contractor (or next higher-tier subcontractor).[65] Given the requirements related to subcontractor reporting, prime contractors should consider the following questions when establishing relationships with subcontractors:

- Will there be some negotiated degree of information sharing?
- Do the subcontractor's efforts involve CDI? In particular, will the subcontractor's systems contain CDI?
- How will the prime contractor set information management requirements and how will the subcontractor comply with those requirements?
- Does the subcontractor provide operationally critical support?
- Is the subcontractor capable of complying with the DFARS Rule including the cyber incident reporting requirements?
- Is it possible to arrange for the subcontractor to furnish to the prime contractor a redacted copy of any cyber incident reports?
- Can the subcontractor confirm that the prime contractor's attributional information will not be disclosed?

Notably, the DFARS Rule flowdown requirements appear to apply even to subcontracts for commercial items. Thus, while subcontracting for commercial items typically results in many fewer FAR and DFARS clauses being flowed

---

[62] DFARS 252.204-7012(m)(1).

[63] Cybersecurity Challenges: Protecting DoD's Unclassified Information, DoD Industry Information Day, June 23, 2017, http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940.

[64] *Id.*

[65] DFARS at 252.204-7012(m)(2)(ii).

down to the subcontractor, the flowdown requirements of this clause do not appear to make a distinction between commercial item and noncommercial contracts.

## CYBERSECURITY EXECUTIVE ORDER

The push for greater cyber security requirements in government contracting has not yet reached its end. As contractors implement these new FAR and DFARS requirements, additional requirements from civilian agencies, or even the DOD, may be on the horizon. Most significantly, on May 11, 2017, President Trump issued Executive Order 13800 titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[66] Though this Executive Order has not directly impacted the FAR and DFARS Rules as of yet, it prescribed a risk management plan regarding cybersecurity that may lead to later changes in the FAR and DFARS Rules as well as to the creation of additional cybersecurity initiatives that could impact government contractors. The key sections of Executive Order 13800 that could lead to future changes in government contracting cybersecurity requirements include:

- Section 1(a) allows the President to hold executive departments and agencies accountable for managing cybersecurity risk to their enterprise.[67]
- Section 1(c) pertains to risk management and discusses how:
    - Agency heads are accountable "for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data."
    - Each agency must use "The Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework") developed by the NIST to manage cybersecurity risk.
    - Each agency has to provide a risk management report within 90 days of the issuance of Executive Order 13800 to the Secretary of Homeland Security ("DHS") and the Director of the Office of Management and Budget ("OMB"). This report shall "document the risk mitigation and acceptance choices made by each agency head as of the date of this order [and] describe the agency's action plan to implement the Framework."

---

[66] Exec. Order No. 13800 (May 11, 2017), https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[67] *Id.*

- The DHS Secretary and the OMB Director then must assess within 60 days of receipt each agency's risk management report to determine whether each agency's strategies for mitigating cybersecurity risk are appropriate and acceptable. The DHS Secretary and the OMB Director then are to submit a final determination and a plan regarding risk management to the President, through the Assistant to the President for Homeland Security and Counterterrorism.[68] Depending on each agency's risk assessment, the DHS Secretary of and the OMB Director of may propose additional strategies for agencies to consider—including further strengthening cybersecurity requirements for government contractors—when it comes to managing cybersecurity risks.

On January 5, 2018, the Commerce Secretary and the DHS Secretary released a draft "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" for public comment.[69] The final report was due on May 11, 2018. This draft report responds to the May 11, 2017 Executive Order but focuses on the Executive Order's call for "resilience against botnets and other automated distributed threats" rather than on agencies' risk management reports, which were supposedly due in August 2017. It is currently unclear whether and how agencies are providing risk management reports to DHS and the OMB and what will become of these reports in terms of their impact on the cybersecurity landscape.

It remains to be seen how Executive Order 13800 may further change the landscape of cybersecurity for government contractors, but its issuance underscores just how focused the government—up to and including the White House—is on cybersecurity. With allegations of hacking and revelations regarding security breaches a regular part of the news cycle, the government's focus in this area is likely only to increase in the coming years as cyber threats remain one of the world's biggest challenges.

## DEVELOPMENTS ON THE HORIZON

Cybersecurity requirements will likely continue to evolve, due in part to the risk management discussion contained in Executive Order 13800. Notably, on

---

[68] *Id.*

[69] A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (Jan. 5, 2018), https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf.

September 14, 2016, the National Archives and Records Administration ("NARA") released a new regulation, 32 C.F.R. Part 2002 ("NARA Rule"), which establishes the approved categories and subcategories of Controlled Unclassified Information ("CUI") and requires that NIST 800-171 will govern when CUI is maintained on non-federal computer systems.[70] However, to date, only the DFARS Rule appears to be in compliance with the NARA Rule and its requirements. As a consequence, it is highly likely that contractors will see other agency supplemental rules or even a new revised FAR Rule to address CUI. And potentially more concerning, the NARA Rule specifically calls for agencies to require non-federal entities that possess CUI on behalf of the agency to protect CUI in accordance with Executive Order 13556, Controlled Unclassified Information, November 4, 2010 and the NARA Rule.[71] Contractors working with non-DOD entities may begin to face ad hoc clauses crafted by individual agencies for specific procurements in an attempt to comply with this NARA Rule.

As for broader efforts to comply with the NARA Rule, in April 2017, the FAR Council opened a new FAR case, No. 2017-016, Controlled Unclassified Information, which appears to indicate that a new FAR provision will be forthcoming to address this issue.[72] However, to date no proposed regulation has been published and the timeline for implementing a new FAR requirement is uncertain.

In addition to DOD's implementation of the DFARS Rule, other agencies also appear to be moving forward with proposed regulations regarding cybersecurity. For instance, the Department of Homeland Security ("DHS") issued three new proposed cybersecurity regulations for DHS contractors. Though these rules are just proposals and still have to undergo notice and comment and agency amendment, contractors should still be aware of these proposed rules, which seek to impose more requirements on DHS contractors regarding cybersecurity including safeguarding systems, handling information, reporting cyber incidents, and conducting training.[73] At least as currently

---

[70] 32 C.F.R. § 2002.1 *et seq.*; 81 Fed. Reg. 63,336 (Sept. 14, 2016).

[71] 32 C.F.R. § 2002.16(a)(5).

[72] https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf (indicating that as of April 6, 2018, a report on the FAR Case is not due until April 11, 2018).

[73] The three new rules include changes to the following: (1) CUI Safeguarding; (2) IT Awareness Training; and (3) Privacy Training. For more information about these proposed rules, see Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information, 82 Fed. Reg. 6429 (Jan. 19, 2017); Homeland Security Acquisition Regulation (HSAR); Information Technology Security Awareness Training, 82 Fed. Reg. 6446 (Jan. 19,

proposed, these rules do not appear to comply with the requirements set forth in the NARA Rule.[74]

Moreover, on January 12, 2018, the GSA announced in the Federal Register that it was considering two new sets of requirements for its FAR supplement—the General Services Acquisition Regulations ("GSAR")—although as of the publication of this article the text of the actual proposed regulations has not been released. The announcement regarding these proposed regulations explains that the new regulations are intended to update and replace current GSA policies, which are not formal regulations and have not gone through the formal notice and comment process. One set of requirements would be an update to GSA current cybersecurity policies regarding safeguarding systems and information and is titled "Information and Information Systems Security." GSA explains that it would require compliance with NIST and NARA standards. The second set of requirements is titled "Cyber Incident Reporting," and appears to be somewhat similar to the DOD cyber incident reporting requirements.

Since the DFARS and FAR Rules are still in their infancy and will likely evolve, it remains to be seen exactly how the government may investigate, sue, and/or prosecute contractors that violate the DFARS and FAR Rules. However, given the government's (as well as *qui tam* relators) increasing use of the FCA to investigate and sue government contractors for any alleged violations of contract terms, contractors who fail to comply with these rules despite certifying they are in compliance with these requirements may face liability under the FCA, and could face other consequences as well, such as criminal prosecution and suspension/debarment proceedings. Contractors may also face breach of contract cases related to any alleged failure to comply with these cybersecurity requirements. While the future of government action in response to noncompliance with the DFARS and FAR Rules remains to be seen, the government has made it clear that its continued focus will be on cybersecurity.

---

2017); Homeland Security Acquisition Regulation (HSAR); Privacy Training, 82 Fed. Reg. 6425 (Jan. 19, 2017).

[74] In particular, the DHS Rule uses different categories of CUI than those set out in the NARA Rule, *compare* 82 Fed. Reg. 6429 *with* NARA Rule, despite the requirement in the NARA Rule which states: "Agencies may use only those categories or subcategories approved . . . and published in the CUI Registry to designate information as CUI." 32 C.F.R. § 2002.12(b). Moreover, the DHS Rule does not use NIS TSP 800-171 to set standards for contractors even though the NARA Rule states: "Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems." 32 C.F.R. § 2002.15(h)(2).

## CONCLUSION AND OUTLOOK

The FAR and DFARS Rules significantly changed the landscape of cybersecurity requirements for government contractors.

Although some government contractors were prepared for the changes that the new FAR and DFARS rules on cybersecurity required, many were not and were therefore forced to scramble to review the requirements and implement adequate safeguards to ensure compliance. With continued changes to the cybersecurity requirements expected, contractors need to ensure that they continue to monitor and develop their adequate safeguards on an ongoing basis.