BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

A Guide To Understanding Federal Contracting Cybersecurity Rules

*By Cameron S. Hamrick, David F. Dowd, Luke Levasseur, and Marcia G. Madsen**

In the summer of 2015, the U.S. Government revealed that over 20 million people were swept up in two enormous breaches of Government computer systems. The Office of Personnel Management (OPM) announced that every person given a Government background check for the prior 15 years was probably affected.[1] Notably, one of the hackers posed as an employee of an OPM contractor performing background investigations.[2] The Government launched a series of aggressive initiatives to spur agencies to improve their cybersecurity readiness and performance, including the 2015 "cyber sprints" executed in response to the OPM breaches.[3]

The Government is extremely concerned with cybersecurity for reasons that extend well beyond the enormous OPM breaches. Cybersecurity incidents have surged 38% since 2014, cyber attacks cost companies $400 million every year, and impacts of successful attacks include downtime, loss of revenue, reputational damage, and loss of customers.[4] In 2016, federal agencies were inundated with over 30,899 cyber incidents that led to compromise of information or system functionality.[5] Several years before the OPM breaches, the Federal Government began enacting statutes, promulgating regulations, and publishing vast amounts of guidance and other information concerning cybersecurity.

As a result, during the last several years, Government contractors have been increasingly besieged by information concerning cybersecurity threats and rules. The profusion of rules, reports, instructions, memoranda, and other publications has become virtually impossible to track, much less comprehensively understand. Last year, 2016, in particular, was a landmark year for regulations imposing cybersecurity requirements on Government contractors, including a final Federal Acquisition Regulation (FAR) rule,[6] a final Defense FAR Supplement (DFARS) rule,[7] and a final rule concerning controlled unclassified information (CUI).[8] The final DFARS rule followed another final DFARS cybersecurity rule in 2013[9] and two interim rules in 2015,[10] leaving some contractors with multiple sets of requirements in different contracts. Contrac-

*Cameron S. Hamrick, David F. Dowd, and Marcia G. Madsen are Partners and Luke Levasseur is Counsel at Mayer Brown LLP in Washington, D.C. The invaluable assistance of Roger V. Abbott, an Associate at Mayer Brown LLP, is gratefully acknowledged.

IN THIS ISSUE:

tors need assistance cutting through the dense undergrowth of cybersecurity statutes, regulations, reports, and other materials so that they can understand precisely what is required of them as part of conducting business with the Government.

This BRIEFING PAPER discusses certain statutes, including the Federal Information Security Management Act of 2002,[11] which provided a comprehensive framework for ensuring the effectiveness of information security controls over federal information resources.[12] However, the primary focus of this BRIEFING PAPER is on cybersecurity regulations that govern your federal contracts and subcontracts—making sense of those regulations and explaining what you should do to ensure compliance. These regulations include the 2016 FAR rule, the DFARS rules, and the rule governing CUI referenced above. They also include regulations promulgated by individual agencies, cybersecurity rules governing cleared contractors that hold classified contracts, and rules that are part of the Defense Industrial Base Cybersecurity Program. The PAPER also sets out practical guidance with respect to managing cybersecurity risks in connection with your supply chain, including risks posed by DOD supply chain regulations.

Compliance with the regulations discussed in this PAPER, as with all Government contracting regulations, is important. Yet compliance with many of the cybersecurity rules will have the added benefit of helping to protect your information systems from costly attacks. In addition, because many of the regulations are relatively new and others have been proposed or are under consideration, Government contracting cybersecurity rules could generate the next wave of allegations under the civil False Claims Act (FCA), which, as most contractors know, presents the threat of penalties and treble damages.[13] Other potential consequences of noncompliance include negative past performance information, termination of your contract for default or cause, and suspension and debarment. It is therefore vital that you understand the cybersecurity requirements governing your federal contracts and subcontracts.

The Federal Information Security Management Act Of 2002

As the Internet continued to grow as a force after the turn of the century, Congress passed the Federal Information Security Management Act (FISMA) of 2002, which was part of the E-Government Act of 2002.[14] The FISMA of 2002 was enacted in part to provide a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets" and to "provide for development and maintenance of minimum controls required to protect Federal information and information systems."[15] The Act requires each agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source.[16] The Act also specifies that the National Institute of Standards and Technology (NIST), part of the Department of Commerce, will develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets except for national security systems.[17] NIST has issued standards and guidelines in numerous publications, including a critical publication (discussed below) that applies to certain contractors through two sets of regulations promulgated last year.

The Federal Information Security Modernization Act Of 2014

The Federal Information Security Modernization Act of 2014 amended the FISMA of 2002 in several important

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. Periodical Postage paid at St. Paul, MN. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

ways, including specifying that the Secretary of the Department of Homeland Security (DHS), in consultation with the Director of the OMB, is responsible for administering the implementation of agency information security policies and practices for non-national security information systems.[18] These responsibilities include developing and overseeing implementation of "binding operational directives" to agencies to implement certain policies, principles, standards, and guidelines. The term "binding operational directive" is defined in part as a means of compulsory direction to an agency that is for the purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.[19] In carrying out its implementation responsibilities, DHS must consider any applicable standards or guidelines developed by NIST and issued by the Secretary of Commerce under 40 U.S.C.A. § 11331.[20] Further, the Act requires agencies to report to certain congressional committees information about data breaches within 30 days after discovery.[21]

The 2016 FAR Amendment

One of the primary consequences for contractors of the Government's increasing cybersecurity concerns was a significant amendment of the FAR. On May 16, 2016, a final rule amended the FAR by adding a new subpart and contract clause governing basic safeguarding of contractor information systems that process, store, or transmit federal contract information.[22] The commentary accompanying the final rule indicates that the new safeguarding measures are generally employed as part of the routine course of doing business[23] and further indicates that contractor systems containing classified information or CUI require more than the basic level of protection.[24] The final rule is just one step in a series of coordinated regulatory actions being taken to strengthen protections of information systems.[25] We discuss several of these steps below, including a rule enacted last year governing CUI.

FAR Subpart 4.19 And The Clause At FAR 52.204-21

The final FAR rule added Subpart 4.19, which applies to all acquisitions other than acquisitions for commercially available off-the-shelf items (COTS) when a contractor's information system may contain "Federal contract information."[26] The term "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, but does not include information provided by the Government to the public, such as information on public web sites, or simple transactional information, such as information necessary to process payments.[27]

FAR 4.1903 requires the clause at FAR 52.204-21 to be included 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.[28] Thus, the scope of the rule is broad, and prime contractors and upper-tier subcontractors must include the clause in any lower-tier subcontract for non-COTS items—including such subcontracts below the simplified acquisition level and for commercial items—when the subcontractor may have federal contract information residing in or transiting through its information system.

Most of the relevant information is in the clause at FAR 52.204-21, including several definitions. The bulk of the clause sets forth numerous safeguarding requirements and procedures that are based on certain security requirements in a publication by NIST—Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."[29] However, unlike the 2016 DFARS amendment (discussed below), the FAR clause does not incorporate the SP 800-171 requirements. The safeguarding specified by the FAR clause applies to "covered contractor information system[s]," which means any information system owned or operated by a contractor that processes, stores, or transmits federal contract information.[30] The final FAR rule was preceded by a proposed rule issued in 2012.[31] The proposed rule generated several comments, including concerns about contractors' ability to identify protected materials. In response, the Government indicated that the focus of the final rule shifted from safeguarding specific information to safeguarding certain contractor information systems. Therefore, according to the Government, it is not necessary to consider factors such as whether the information is marked.[32]

If the clause applies, you should carefully review its requirements and procedures, which are set forth in 15 subparagraphs at FAR 52.204-21(b)(1). We have provided comments on certain controls below, with the parenthetical number corresponding to the subparagraph number in the clause.

(i) "Limit information system access to authorized users, processes acting on behalf of authorized users,

or devices (including other information systems)." The term "information system" is defined to mean a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[33] The Government provided commentary on this definition, explaining that in general, separately accredited information systems that interface through loosely coupled mechanisms, such as email or Web services, are not considered direct connections.[34]

(iii) "Verify and control/limit connections to and use of external information systems." The FAR rule and the accompanying commentary do not define "external information systems." However, the commentary accompanying the final rule states that "[a]ll of the controls listed are focused on protection of the information system (*e.g.*, the host servers, workstations, routers). None of the controls are devoted to protection of 'perimeter devices' although several (particularly paragraphs (b)(1)(x) and (b)(1)(xi)) are applied at the perimeter of the system."[35]

(vii) "Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse." As noted previously, the Government claims that the safeguarding applies to certain information systems, and not to specific types of information, and therefore it is not necessary to consider certain factors such as whether the information is marked.[36] However, this specific control requires contractors and subcontractors to be able to identify "Federal Contract Information" in order to be able to sanitize or destroy media containing such information. As such, for purposes of this control, it is important to be able to know whether, for example, information received from the Government is not intended for public release. Thus, you may need to take steps to verify with the Government what constitutes federal contract information.

(xii) "Identify, report, and correct information and information system flaws in a timely manner." The requirement in this control to "report" certain flaws does not mean reporting to the Government. The commentary accompanying the rule states that "[t]here are no reporting or recordkeeping requirements associated with the rule."[37] This contrasts with the 2016 DFARS rule, discussed below, that requires reporting of "cyber incidents" to DOD. The FAR requirement to "report . . . information and information system flaws in a timely manner" thus can reasonably be read to mean reporting within your organization.

Potential Consequences Of Noncompliance

The FAR rule does not include a provision specifying liability for failing to comply with any part of the rule. The comments include the following under the heading "Noncompliance Consequences":

> *Comment*: One respondent was concerned that any inadvertent release of information could be turned into not only an information security issue but also a potential breach of contract.
>
> *Response*: The refocus of the final rule on the safeguarding requirements applicable to the system itself should allay the respondent's concerns. Generally, as long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract.[38]

It is unclear what the Government meant by prefacing this last statement with the word "Generally." If a contractor complies with the FAR requirements, the Government should have no basis for a breach claim with respect to those requirements.

Failure to comply with the requirements in the FAR clause could have other consequences. Past performance information includes a contractor's record of conforming to requirements and is relevant for future contract selection purposes.[39] Accordingly, a contractor's failure to comply with FAR cybersecurity requirements could impair the contractor's ability to obtain certain Government contracts. Also, failure to comply with such requirements could cause the Government to terminate a contract for default[40] or cause.[41] In addition, it is possible that the Government or a creative whistleblower could allege liability under the civil FCA[42] if they believe they can meet the elements of one or more bases for liability under that Act.

Prime contractors and upper-tier subcontractors also have to consider the possibility that a subcontractor might release protected information due to inadequate safeguards. At a minimum, prime contractors should make sure they include the substance of the new clause in subcontracts in which the subcontractor may have federal contract information residing in or transiting through its information system. (See the "Supply Chain Management" section below.)

The DFARS Cybersecurity Requirements

In October 2016, DOD promulgated a final rule that implemented statutory requirements regarding contractor reporting of network penetrations and DOD policies and procedures regarding purchases of cloud computing services.[43] That rule built on a final rule from 2013,[44] two interim rules from 2015,[45] and comments on the second interim rule. These rules have culminated in significant and burdensome cybersecurity provisions in DFARS subparts and clauses, which we discuss as they stand after issuance of the 2016 rule. DOD acknowledged in the comments accompanying the 2016 final rule that if a contractor has not been subject to the previous iteration of the clause at DFARS 252.204-7012 (current version discussed below) and is now handling covered defense information (also discussed below), "the cost could be significant to comply."[46] DOD hosted an "Industry Information Day" on June 23, 2017, that included discussions of the DFARS requirements.[47] At that meeting, DOD recognized that because of the different rules (the 2013 final rule, the 2015 interim rules, and the 2016 final rule), a single contractor might be implementing contracts that have different requirements. A Government representative indicated that when that happens, DOD encourages both its Contracting Officers (COs) and contractors to work together to reach a bilateral agreement where they could implement the final (2016) version of the rule.[48]

The DFARS cybersecurity rules are substantially more onerous than the FAR rule, which only purports to establish "the basic level of protection."[49] The DFARS rules include provisions in Subpart 204.73 and related clauses. The Subpart applies to contracts and subcontracts that require contractors and subcontractors to safeguard "covered defense information" (CDI) residing in or transiting through "covered contractor information systems" by applying specified network security requirements. The Subpart also requires reporting of "cyber incidents," discussed further below.[50]

The clause at DFARS 252.204-7012 includes definitions of these and several other terms, and includes the bulk of the DFARS requirements for safeguarding CDI and cyber incident reporting. That clause is required in all solicitations and contracts, including those for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.[51] Contractors must include the clause in subcontracts or "similar contractual instruments" for "operationally critical support" or for which performance will involve "covered defense information."[52] The term "operationally critical support" means "supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."[53] The term "covered defense information" is discussed in the following section.

Covered Defense Information

The definition of "covered defense information" is a fundamental part of the DFARS rules and means:

> unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide 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.[54]

This definition is helpful in that it requires CDI provided to the contractor by or on behalf of DOD to be marked or otherwise identified in the contract, task order, or delivery order, which gives the contractor objective evidence of the existence of such information.

The definition is less helpful with respect to information collected, developed, received, transmitted, used, or stored by or on behalf of the contractor, which will not necessarily be identified with objective evidence. DOD has been less than clear in discussing this point, indicating in the comments to the 2016 final rule that contractors have a "shared obligation . . . to recognize and protect [CDI] that the contractor is developing during contract performance."[55] However, DOD subsequently issued answers to "Frequently Asked Questions (FAQs)" in January 2017 regarding implementation of Subpart 204.73 indicating that the "requiring activity" is responsible for determining if CDI is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor, and the CO must ensure that the contract includes the requirement, as provided by the requiring activity (such as a contract data requirements list) for the contractor to mark CDI developed in performance of the contract.[56] To help avoid confusion, you should be familiar with the definition of CDI, including the part of the defini-

tion involving the CUI Registry. That Registry, discussed further below as part of the 2016 CUI rule, is a publicly accessible online repository for information, guidance, policy, and requirements on handling CUI.

At the "Industry Information Day" held earlier in June 2017 (referenced above), DOD indicated that, with respect to the portion of the CDI definition "Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract," the term "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.[57]

Covered Contractor Information Systems

As noted previously, DFARS Subpart 204.73 applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information residing in or transiting through "covered contractor information systems."[58] These systems are unclassified information systems that are owned, or operated by or for, a contractor and that process, store, or transmit covered defense information.[59]

Adequate Security For Systems Operated On Behalf Of The Government

The clause at DFARS 252.204-7012 requires contractors to provide "adequate security" on all covered contractor information systems. "Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.[60] DFARS 252.204-7012 distinguishes between covered contractor information systems that *are* part of an IT service or system operated on behalf of the Government, and those that *are not* part of an IT service or system operated on behalf of the Government. For such systems that *are* part of an IT service or system operated on behalf of the Government, the following security requirements apply: (1) cloud computing services shall be subject to the security requirements in DFARS 252.239-7010 (discussed below); (2) any other such IT service or system, *i.e.*, other than cloud computing, shall be subject to the security requirements specified elsewhere in the contract.[61]

Adequate Security for Systems *Not* Operated On Behalf Of The Government

Most contractors will be required to implement the security requirements for covered contractor information systems that *are not* part of an IT service or system operated on behalf of the Government—and those requirements are substantial. They include the mandate that the covered contractor information system be subject to the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," in effect at the time the solicitation is issued or as authorized by the CO.[62] Moreover, contractors are required to implement NIST SP 800-171 no later than December 31, 2017.[63] Complying with NIST SP 800-171 is onerous and costly, for reasons discussed below.

Further, contractors must apply "other information system security measures" when the contractor reasonably determines such measures "may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (*e.g.*, medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability."[64]

The requirement that covered contractor information systems be subject to the requirements in NIST SP 800-171 is a critical and burdensome mandate and will be especially difficult and costly for many small businesses. In addition, the time and costs to implement these requirements may be particularly painful for companies that handle only a small amount of CDI or commercial companies with relatively few DOD contracts or subcontracts.

The most recent version of NIST SP 800-171 is Revision 1, issued in December 2016, and is the version discussed in this PAPER. A DOD memorandum states that the clause at DFARS 252.204-7012 requires the contractor to implement the version of SP 800-171 in effect at the time of the solicitation, or such other version authorized by the CO. Thus, according to the memorandum, if Revision 1 was not in effect a the time of the solicitation, the contractor should work with the CO to modify the contract to authorize use of Revision 1.[65]

NIST issued the publication to further its responsibilities under the FISMA of 2014.[66] SP 800-171 specifies 14 "Families" of security requirements: Access Control; Awareness and Training; Audit and Accountability; Configuration Management; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical Protection; Risk Assessment; Security Assessment; System and Communications Protection; and System and Information Integrity.[67] Each Family lists several specific requirements, which are divided between "basic se-

curity requirements" and "derived security requirements."[68] Basic security requirements are obtained from another NIST publication, Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," which provides the high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic requirements, are taken from NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."[69]

An example of requirements in one of the Families, "Maintenance," is set forth below:

> Basic Security Requirements:
>
> 3.7.1 Perform maintenance on organizational systems.
>
> 3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
>
> Derived Security Requirements:
>
> 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.
>
> 3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
>
> 3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
>
> 3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.[70]

As is evident from these requirements, the time and cost of implementing the requirements are not limited to a one-time process of setting up a compliant system, but involve ongoing efforts as well. A few examples of such ongoing efforts in other Families include "Monitor and control remote access sessions,"[71] "Track, review, approve/disapprove, and audit changes to organizational systems,"[72] and "Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls."[73] SP 800-171 includes a helpful Glossary of several terms used in the requirements.[74]

Based on significant attention devoted recently by DOD,[75] two NIST SP 800-171 requirements deserve particular focus: (1) "Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems" (Requirement 3.12.4), and (2) "Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems" (Requirement 3.12.2).[76] In guidance issued in September of this year, DOD indicated that in order to document implementation of the SP 800-171 requirements by the December 31, 2017, DFARS deadline, companies should have a system security plan in place, in addition to any associated plans of action to describe how and when any unimplemented 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.[77] In short, the system security plan and any associated plans of action are the mechanisms to demonstrate implementation of NIST SP 800-171.[78]

Complying With SP 800-171

While compliance with the SP 800-171 requirements is demanding, there are steps you can take that may help ease the process. The publication explains one approach that may yield benefits—limiting the scope of the requirements only to systems or components that process, store, or transmit covered information:

> Isolating CUI into its own *security domain* by applying architectural design concepts (*e.g.*, implementing subnetworks with firewalls or other boundary protection devices) may be the most cost-effective and efficient approach for nonfederal organizations to satisfy the security requirements and protect the confidentiality of CUI. Security domains may employ physical separation, logical separation, or a combination of both. This approach can reasonably provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond which it typically requires for protecting its missions, operations, and assets.[79]

Also, the clause at DFARS 252.204-7012 permits contractors to ask for variances from the NIST requirements after contract award by submitting a written request to the CO for consideration by the DOD Chief Information Officer (CIO).[80] A different DFARS clause, DFARS 252.204-7008, "Compliance With Safeguarding Covered Defense Information Controls" (discussed below), provides a process for making preaward requests. You do not have to implement any security requirement "adjudicated by an authorized representative of the DOD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."[81] DOD's FAQs issued in January 2017 indicate that when CDI is used in performing a subcontract, the requirement is for the subcontractor to request the CO to seek CIO adjudication on variances from the NIST SP 800-171 requirements.[82]

In addition, DOD provided helpful tips in the FAQs in response to the question: "How might a small business with limited IT or cybersecurity expertise approach meeting the requirements of NIST SP 800-171."[83] Before setting forth a "reasonable approach," DOD noted that most of the requirements are about policy, process, and configuring IT securely, while others require security-related software (such as antivirus), or additional hardware (such as a firewall).[84] You should review DOD's "reasonable approach" if your organization is not yet compliant with the requirements. You also should review the portion of the FAQs starting at page 18 entitled "Questions Specific to the NIST SP 800-171 Requirements."

DOD has identified additional helpful information. During the Industry Information Day in June 2017, DOD indicated that the "Cybersecurity Evaluation Tool" (CSET), developed by the Department of Homeland Security, provides a systematic approach for evaluating your organization's security posture by guiding asset owners and operators through a step-by-step process to evaluate their system and security practices. CSET generates questions that are specific to relevant requirements and presents the assessment results in both summary and detail form. CSET can be downloaded for free at https://ics-cert.us-cert.gov/Downloading-and-installing-CSET. You select "Advanced Mode," which provides the option to select NIST SP 800-171.[85]

Further, DOD posts helpful resources addressing DFARS clause 252.204-7012, including regulations, policy, and frequently asked questions, at the Cybersecurity tab at http://dodprocurementtoolbox.com/.[86]

Allowability Of Compliance Costs

As discussed above, the costs of complying with the DOD cybersecurity requirements can be substantial. DOD reasonably stated in the comments accompanying the 2016 rule that "[t]he cost of compliance is allowable and should be accounted for in proposal pricing (in accordance with the entity's accounting practices)."[87] Oddly, DOD backtracked from this position in the FAQs, noting that contractors should "consult with their Audit Compliance/Accounting/Finance departments for guidance" on the cost recovery options for complying with the clause at DFARS 252.204-7012.[88] The position in the comments is appropriate.

DFARS 252.204-7008

Another clause, DFARS 252.204-7008, is required in all solicitations except for those solely for the acquisition of COTS items.[89] That clause states that, for covered contractor information systems that are not part of an information technology (IT) service or system operated on behalf of the Government, "By submission of this offer, the Offeror represents that it will implement the security requirements specified by [NIST SP] 800-171 . . . that are in effect at the time the solicitation is issued or as authorized by the contracting officer, not later than December 31, 2017."[90] After December 31, 2017, this language may generate bid protests if contractors have information that a competitor has not implemented the NIST requirements.

As discussed above, DFARS 252.204-7008 also provides a method for offerors to identify situations in which a NIST requirement is not needed in performing the contract, or to propose an alternative to a NIST requirement. The offeror must submit a written explanation of why a requirement is not applicable or how an alternative but equally effective security measure can compensate for the inability to satisfy a requirement. An authorized representative of the DOD CIO will adjudicate such requests prior to contract award.[91]

Cyber Incident Reporting

Unlike the 2016 FAR rule, the DFARS requires contractors and subcontractors to "rapidly report cyber incidents."[92] The term "rapidly report" means within 72 hours of any cyber incident,[93] and "cyber incident" means "actions taken through the use of computer networks that result in a compromise of an actual or potentially adverse effect on an information system and/or the information residing therein."[94] You should keep the breadth of this definition in mind—it covers a *potentially* adverse effect. Similarly, the definition of "compromise"—a term used to define "cyber incident"—describes certain events that "*may* have occurred."[95] Contractors and subcontractors must submit the report to DOD at http://dibnet.dod.mil.[96] Subcontractors provide the incident report number assigned by DOD to the prime contractor (or next higher-tier subcontractor) as soon as practicable.[97]

The clause at DFARS 252.204-7012 establishes that reporting of cyber incidents is limited to such incidents "that affect[] a covered contractor information system or the covered defense information residing therein, or that affect[] the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract."[98] After discovering such an incident, you must conduct a review for evidence of compromise of CDI, including but not limited to identifying

compromised computers, servers, specific data, and user accounts. You also must analyze covered contractor information system(s) that were part of the incident, as well as other information systems on your ("the Contractor's") network(s), that "*may* have been" accessed as a result of the incident in order to identify compromised CDI, or that affect your ability to provide operationally critical support.[99]

Each cyber report must include the required elements at https://dibnet.dod.mil.[100] For DOD contractors not providing cloud services, that website states (under "Reporting a Cyber Incident," part of the "Resources" tab) the following:

> DOD contractors shall report as much of the following information as can be obtained to DOD within 72 hours of discovery of any cyber incident.
>
> 1. Company name
>
> 2. Company point of contact information (address, position, telephone, email)
>
> 3. Data Universal Numbering System (DUNS) Number
>
> 4. Contract number(s) or other type of agreement affected or potentially affected
>
> 5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
>
> 6. [U.S. Government] Program Manager point of contact (address, position, telephone, email)
>
> 7. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
>
> 8. Facility [Commercial and Government Entity (CAGE)] code
>
> 9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
>
> 10. Impact to Covered Defense Information
>
> 11. Ability to provide operationally critical support
>
> 12. Date incident discovered
>
> 13. Location(s) of compromise
>
> 14. Incident location CAGE code
>
> 15. DOD programs, platforms or systems involved
>
> 16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
>
> 17. Description of technique or method used in cyber incident
>
> 18. Incident outcome (successful compromise, failed attempt, unknown)
>
> 19. Incident/Compromise narrative
>
> 20. Any additional information.[101]

The commentary accompanying the 2016 DFARS final rule indicates that when a cyber incident is discovered, the contractor should report "whatever information is available" within 72 hours, and if the contractor does not have all of the required on the "Incident Collection Form" at the time of the report, and if more information becomes available, the contractor should submit a follow-on report with the new information.[102]

The commentary also states that "[a]n information technology expert will likely be required to provide information describing the cyber incident in the report, or at least to determine what information was affected."[103] This could be an in-house expert or a third-party consultant. Also, you must have, or acquire, a "DOD-approved medium assurance certificate" in order to be able to report cyber incidents. Information on obtaining this certificate, part of DOD's External Certification Authority (ECA) Program, is available at https://iase.disa.mil/pki/eca/Pages/index.aspx.[104] In short, you can purchase an ECA Certificate from one of two approved vendors listed at the website.[105]

You have additional responsibilities after discovering a cyber incident. If you discover and are able to isolate "malicious software," you must submit the software to the DOD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the CO—do not submit the software to the CO.[106] The term "malicious software" means "computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system." The definition includes "a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware."[107] Also, upon discovering a cyber incident, you 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 report to DOD in order to allow DOD to request the media or decline interest.[108] If DOD conducts a damage assessment, the CO will request that the contractor provide this media.[109] DOD also may ask for access to additional information or equipment necessary to conduct a "forensic analysis,"[110] defined as "the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data."[111]

Protections Against Disclosure Of Contractor Data

The clause at DFARS 252.204-7012 includes certain

protections against disclosure of your data submitted in connection with a cyber incident, stating that "[t]he Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information."[112] The term "contractor attributional/proprietary information" is defined as

> information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (*e.g.*, program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.[113]

The clause then cautions that, to the maximum extent practicable, contractors must identify and mark such information. This is important in part because, in addition to the possibility that the Government could inadvertently release your information to third parties, DOD can make "authorized release[s]."[114] The clause creates two types of authorized releases: release of contractor attributional/proprietary information not created by or for DOD,[115] and such information that was created by or for DOD.[116] For attributional/proprietary information not created by or for DOD, DOD can release such information in five designated entities/circumstances, including for national security purposes. DOD also can make releases to support services contractors directly supporting Government activities under a contract that includes the clause at DFARS 252.204-7009, "Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information."[117] That clause imposes restrictions on the third-party contractor with respect to information obtained from another party's reporting of a cyber incident, including, for example, ensuring that employees are subject to use and nondisclosure obligations.[118] However, the clause at DFARS 252.204-7012 also permits DOD to release contractor attributional/proprietary information to "entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents," with no corresponding restrictions on such subsequent releases by such "entities."[119] As such, in marking confidential information as part of a cyber incident, you should indicate that the information may not be released to any nongovernmental entity that is not subject to the restrictions in the clause at DFARS 252.204-7009. While there is no guarantee DOD will abide by that restriction, it could spur DOD employees involved in the release to seek such restrictions.

With respect to the second category of authorized releases, contractor attributional/proprietary information that was created by or for DOD, that information includes all of the information required to be submitted as part of the cyber incident report.[120] DOD can release that type of information in each of the five designated entities/circumstances discussed above with respect to attributional/proprietary information that was *not* created by or for DOD. In addition, DOD can release contractor attributional/proprietary information that was created by or for DOD "for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information."[121]

Flow-Down Of DFARS 252.204-7012

Contractors must flow down the clause at DFARS 252.204-7012 in subcontracts, or "similar contractual instruments," for operationally critical support, or for which subcontract performance will involve CDI, including subcontracts for commercial items, without alteration, except to identify the parties. The contractor also must determine if the information required for subcontractor performance retains its identity as CDI, and, if necessary, consult with the CO when uncertain if the clause should flow down.[122] DOD has indicated that prime contractors should minimize the flow-down of information requiring protection.[123]

Liability Considerations

Failure to comply with the requirements in the DFARS rules could have consequences discussed above in connection with the FAR rule, including negative past performance assessments, terminations for default or cause, and allegations of liability under the civil FCA. In addition, DFARS 204.7302(d) states that a cyber incident report will not, "by itself," be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to comply with the clause at DFARS 252.204-7012. That provision goes on to explain that when an incident is reported, the CO must consult with the DOD component CIO/cybersecurity officer "prior to assessing contractor compliance," citing DOD Procedures, Guidance, and Information (PGI) 204.7303-3(a)(3), and stating that the CO shall consider such incidents in the "context of an overall assessment of a contractor's compliance with the requirements of the clause at [DFARS] 252.204-7012."[124] In other words, while a reported incident may not by itself be interpreted as evidence of failure to comply with the clause

at DFARS 252.204-7012, it could easily trigger an overall assessment of compliance. The referenced PGI provision (PGI 204.7303-3(a)(3)) states that if requested by the requiring activity to assess compliance with the requirements of DFARS 252.204-7012, the CO must request a description of the contractor's implementation of the SP 800-171 requirements in order to support evaluation of whether any controls were inadequate or not implemented at the time of the incident, and provide a copy of the compliance assessment to the DOD CIO and others at DOD.

Cloud Computing Requirements

The DFARS establishes three sets of requirements concerning cloud computing: (1) requirements applicable to DOD's acquisition of cloud computing services; (2) requirements applicable to contractors that intend to use an *external* cloud service provider to store, process, or transmit any CDI in performing a contract; and (3) requirements applicable to contractors that intend to use *internal* cloud services to perform their own processing related to meeting a DOD contract requirement to develop/deliver a product. We discuss these three sets of requirements below.

Turning to the first set of requirements, these requirements apply when a cloud solution is being used to process data on DOD's behalf or DOD is contracting with a cloud service provider to host/process data in a cloud.[125] The DFARS includes specific cybersecurity requirements governing IT services contractors that provide cloud computing services. DFARS Subpart 239.76 governs the acquisition of cloud computing services and requires two clauses.[126] The first is at DFARS 252.239-7009, "Representation of Use of Cloud Computing," and is required in solicitations for IT services.[127] The clause defines "cloud computing" as follows:

> *Cloud computing* . . . means 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.[128]

This definition is important because the entire thrust of the clause is to obtain a representation from the contractor that it either does or does not anticipate using cloud computing services in performance of any contractor or subcontract resulting from the solicitation.[129]

Another clause specified by Subpart 239.76 is at DFARS 252.239-7010, "Cloud Computing Services," which must be included in solicitations and contracts for IT services.[130] Subparagraph (b) of that clause provides security requirements applicable when using cloud computing to provide IT services in performing the contract and requires the contractor to implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) at https://iase.disa.mil/cloud_security/Pages/index.aspx, unless notified by the CO that the requirement has been waived by the DOD CIO. The contractor must use the SRG version in effect at the time the solicitation was issued or as authorized by the CO.[131] Version 1, Release 3, is dated March 6, 2017, and is 242 pages long. As such, a description of the SRG's requirements warrants an entirely separate article and presents a substantial amount of homework and due diligence for any IT services contractor interested in providing cloud computing services pursuant to DFARS 252.239-7010. That clause also requires reporting of all cyber incidents related to cloud computing services provided under the contract (submitted to DOD via https://dibnet.dod.mil/, like incidents reported under DFARS 252.204-7012 discussed above);[132] submitting malicious software discovered and isolated in connection with reporting a cyber incident;[133] and, upon discovering a cyber incident has occurred, preserving and protecting images of all known affected information systems identified in the cyber incident report and all relevant monitoring/packet capture date for at least 90 days from the submission of the incident report.[134]

The second set of cloud computing requirements applies when a contractor uses an *external* cloud service provider to store, process, or transmit CDI on the contractor's behalf.[135] These requirements are in the clause at DFARS 252.204-7012, which imposes requirements on contractors that intend to use an external cloud service provider to store, process, or transmit any CDI in performing the contract. The requirements include that the cloud service provider meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) "Moderate baseline," available at https://www.fedramp.gov/resources/documents/.[136] FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for the Federal Government.[137] The contractor also must require and ensure that the external provider complies with the pro-

visions in DFARS 252.204-7012 for cyber incident reporting, malicious software, media preservation and protection, forensic analysis, and cyber incident damage assessment.[138]

With respect to the third set of requirements, the NIST SP 800-171 requirements apply when the contractor uses an *internal* cloud to perform its own processing related to meeting a DOD contract requirement to develop/deliver a product, *i.e.*, as part of the solution for its internal contractor system—an example is when the contractor is developing the next generation tanker and uses its cloud (not an external cloud service provider) for the engineering design.[139]

The 2016 CUI Regulations

In November 2010, President Obama issued Executive Order 13556 that established a program for managing CUI, which the Order defines as information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, but excluding classified information.[140] The Order appointed the National Archives and Records Administration (NARA) to be the Executive Agent responsible for implementing the Order.[141] The process of developing CUI regulations culminated in September 2016, when NARA issued a final CUI rule adding 32 C.F.R. Part 2002.[142]

CUI And CDI

The definition of CUI at 32 C.F.R. § 2002.4(h) includes:

> *Controlled Unclassified Information* (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

In comparing this definition to the definition of CDI, discussed above as part of the DFARS requirements, DOD has stated that the definition of CDI is in line with the CUI definition—both are defined as unclassified information, as described in the CUI Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Also, as discussed below, like CDI, adequate security for CUI requires implementation of NIST SP 800-171.[143]

Indirect Application Of The Rule Through Agreements

The CUI regulations do not apply "directly" to non-executive branch entities (which includes private organizations, except for foreign private or nongovernmental organizations),[144] but do apply "indirectly" to non-executive branch CUI recipients through incorporation into agreements.[145] The final rule states that when entering into agreements or arrangements with a foreign entity, agencies should encourage that entity to protect CUI in accordance with the Executive Order, 32 C.F.R. Part 2002, and the CUI Registry (a publicly accessible online repository for all information, guidance, policy and requirements on handling CUI, discussed below) to the extent possible, but may use their judgment as to what and how much to communicate, keeping in mind the ultimate goal of safeguarding CUI.[146] The definition of "Agreements" covers procurement contracts, grants, and licenses.[147] The regulations specify that agreements with non-executive branch entities must state that such entities must handle CUI in accordance with 32 C.F.R. Part 2002, Executive Order 13556, and the CUI Registry.[148] Agreements also must state that non-executive branch entities have to report any noncompliance with handling requirements to the disseminating agency using methods approved by that agency's CUI Senior Agency Official (SAO), who is responsible for oversight of the agency's CUI Program implementation, compliance, and management.[149] Thus, if you are required to handle CUI under an agreement, you should identify the proper reporting "methods" approved by the agency's SAO, and ensure that relevant employees are aware of this reporting requirement.

The regulations do not specify CUI clauses to include in agreements; however, DOD, the General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) are developing a FAR case (2017-016) to ensure uniform implementation of the CUI Program across the Government, and the case contemplates the creation of a FAR clause.[150] Thus, there are no standard clauses prime contractors can flow down to subcontractors. Prime contractors therefore should flow down all relevant CUI requirements in their contracts to subcontractors that will handle CUI as part of their work under the subcontract.

Agencies are still implementing NARA's CUI rule, as reflected by an August 17, 2017 NARA Memorandum requesting that executive departments and agencies report by November 1, 2017, on their efforts to implement the

Program.[151] This fact, along with the absence of uniform CUI clauses applicable across the Government, underscores the importance of reviewing contracts and subcontracts carefully prior to execution for any CUI requirements and assessing whether you have the capabilities to comply with such requirements.

Safeguarding Requirements

Among the requirements that likely will be in any contract or subcontract involving CUI will be the "Safeguarding" requirements at 32 C.F.R. § 2002.14. A June 12, 2017, NARA CUI Notice, which provides recommendations for agency implementation of the CUI Program, indicates that agencies should identify all contracts or agreements where safeguarding or handling guidance is conveyed for CUI and modify them to align to the safeguarding requirements at 32 CFR § 2002.14.[152] Those requirements mandate safeguarding using one of two standards: "CUI Basic" and "CUI Specified."[153] CUI Basic is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.[154] CUI Basic requirements are the baseline default requirements for protecting CUI, and apply to the vast majority to CUI.[155] Agencies handle CUI Basic according to the uniform set of controls in 32 C.F.R. Part 2002 and the CUI Registry.[156]

CUI Specified, by contrast, is the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. The CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic—the distinction is that the underlying authority spells out specific controls for CUI Specified and does not for CUI Basic.[157]

If you are required to handle CUI under your contract or subcontract, you should review the CUI Registry for relevant information and ensure that your employees are familiar with that information. The Registry is available at https://www.archives.gov/cui/registry/category-list. The CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.[158] The controls for any CUI Basic categories and subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic controls and from each other.[159]

The safeguarding requirements at 32 C.F.R. § 2002.14 include requirements for two types of information systems that process, store, or transmit CUI: (1) federal information systems, which are information systems used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency; and (2) nonfederal information systems, which are any information systems that do not meet the criteria for a federal information system.[160] Most contractors and subcontractors subject to the requirements at 32 C.F.R. § 2002.14 will not be operating information systems on behalf of an agency, and instead will be responsible for their own, nonfederal information systems.

Significantly, NIST SP 800-171—discussed above in connection with the DFARS rules— applies to the protection of CUI Basic on nonfederal systems:

> NIST SP 800-171 (incorporated by reference, see [32 C.F.R] § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).[161]

The reference in the parenthetical to "moderate confidentiality" is based on a standard found in FIPS 199, which requires agencies to categorize their information systems in each of the security objectives of confidentiality, integrity, and availability, including rating each system as low, moderate, or high impact in each category.[162] All CUI Basic categories will be controlled by the same standard—no less than moderate confidentiality, the lowest possible control level above the "low" standard already applied to all information systems without CUI.[163]

"Misuse" Of CUI

The CUI regulations also specify that agreements with non-executive branch entities must include provisions stating that "[m]isuse of CUI is subject to penalties established in applicable laws, regulations, or Government-wide policies."[164] The commentary accompanying the final rule notes that entities that "handle a given type of CUI should

make themselves familiar with the contents of the governing authorities," including any provisions about misuse of CUI.[165] This is good advice for contractors and subcontractors faced with CUI requirements in their agreements.

CUI Markings

In addition to becoming aware of provisions about misuse of CUI, you should be aware that the CUI regulations identify a responsibility that creates a need for special vigilance. The commentary accompanying the final rule states: "The basic rule is that Agencies must mark all CUI with CUI markings ...."[166] However, an agency's failure to apply a marking does not mean you can treat the information as exempt from CUI rules, because the final rule states: "The lack of a CUI marking on information that qualifies as CUI does not exempt the authorized holder from abiding by applicable handling requirements as described in the [Executive] Order, this part, and the CUI Registry."[167] Further, the commentary accompanying the final rule discusses improperly marked CUI:

> Anyone who is authorized to handle CUI is responsible for doing so in compliance with the requirements of the Order, this regulation, and the CUI Registry. If a contractor receives improperly marked CUI from an agency, the contractor is not responsible for having marked the CUI improperly, but the contractor *could be responsible* for knowing the types of CUI it receives from the agency pursuant to the contract, and for knowing which CUI Registry category the information falls into, the handling requirements for that type of CUI, and so forth. As a result, the contractor could, *in some cases*, also be held responsible for properly handling the CUI even if it is not marked properly when they receive it.[168]

While this language includes some fairly vague qualifiers (in the highlighted phrases), other commentary is not qualified: "The regulation does contemplate the possibility that some CUI may be unmarked or marked improperly. In such cases, agencies and non-executive branch agencies would still be subject to that CUI's governing law, regulation, or Government-wide policy's requirements, *including any penalties or sanctions for not handling it properly in accord with those authorities or the connected CUI Program requirements*."[169] Note also that the CUI regulations state that "[a]uthorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should notify the disseminating agency of this belief."[170]

As such, if your contract or subcontract includes requirements for handling CUI, you will benefit from having procedures designed to review all information received from the Government or prime contractor to assess (1) whether unmarked information qualifies as CUI and, if so, what type of CUI, and (2) whether marked CUI is properly marked. This could be a significant undertaking. At a minimum, you should establish procedures that provide for an initial screening of information received, followed by a dialogue with the Government or prime contractor customer that provided the information if there are any doubts concerning the CUI classification of the information. All such doubts should be adequately resolved in writing, so that both sides are in agreement on the proper classification.

Agency Cybersecurity Rules

In addition to DOD, a few other departments and agencies have implemented or proposed cybersecurity regulations applicable to their contractors.

Department Of State

Since 2007, the Department of State has implemented a supplemental acquisition regulation setting forth security requirements and including a contract clause concerning "Security Requirements for Unclassified Information Technology Resources."[171] The Department of State Acquisition Regulation (DOSAR) makes clear that, as a general matter, the "Contractor shall be responsible for [IT] security, based on [DOS] risk assessments, for all systems connected to a [DOS] network or operated by the Contractor for DOS, regardless of location."[172]

The DOSAR contract clause is applicable to "all or any part of the contract that includes [IT] resources or services in which the Contractor has physical or electronic access to DOS's information that directly supports the mission of DOS."[173] Numerous rules in the DOSAR apply broadly to IT support contractors, as well as any company with "[a]ccess to DOS general support systems/major applications at a level beyond that granted to the general public; *e.g.*, bypassing a firewall."[174] The DOSAR mandates that contractors develop and submit an "IT Security Plan" that complies with OMB guidance and the NIST guidelines, submission of proof of IT accreditation within six months of contract award, and annual verification of compliance with various requirements.[175]

General Services Administration

The General Services Administration Acquisition Manual (GSAM) contains a contract clause specifying "Security Requirements for Unclassified Information Technology

Resources."[176] If included in a contract, the GSAM contract clause is virtually identical to the Department of State clause described above (and thus is not discussed further here).

Department Of Homeland Security

DHS currently has a regulation applicable to Government contractors that imposes security requirements related to unclassified information technology resources. That regulation specifies several aspects of IT security for which contractors are responsible and requires preparation, submission, and accreditation of an IT Security Plan that explains how compliance with applicable laws and regulations will be achieved.[177]

In January 2017, DHS proposed a series of additional regulations explaining cybersecurity measures to be followed by contractors working with the Department. The proposed regulations would amend the Homeland Security Acquisition Regulation to (1) add a contract clause and make changes to several existing requirements for safeguarding CUI,[178] (2) add a contract clause to standardize IT security awareness training and "DHS Rules of Behavior requirements for contractor and subcontractor employees,"[179] and (3) add a new subpart and update existing clauses to require contractors to complete training that addresses the protection of privacy and safeguarding of personally identifiable information.[180] These proposed regulations would alter numerous requirements for safeguarding and maintaining Government information, reporting threats and intrusions, and training the contractor workforce.

National Aeronautics And Space Administration

The NASA FAR Supplement includes a relatively short contract clause that similarly addresses "Security Requirements for Unclassified Information Technology Resources."[181] After defining several general terms applicable to many Government contractors (*e.g.*, "security management plan"), the contract clause specifies that contractors working with NASA (and whose contracts contain this provision) must submit a security plan specific to its IT system to the CO within 30 days of contract award.[182] The contract clause also provides information regarding a NASA webpage with resources needed to satisfy contractors' cybersecurity obligations.[183]

Department Of Commerce

The Department of Commerce Acquisition Regulation contains a "Security Requirements for Information Technology Resources" clause to be inserted into contracts awarded by the Department.[184] The Commerce Department regulations contain security plan submission and approval rules, as well as inspection requirements, that are similar to the other agencies discussed above, *e.g.*, the Department of State and NASA. Notably, the Commerce regulations mandate that, within five days of contract award, the contractor must certify that its employees have satisfied the IT security orientation training.[185] Other dates by which contractors must complete cybersecurity related requirements are similarly accelerated in the Commerce regulations, *e.g.*, submission of a "System Certification Work Plan" is required within 14 days of award.[186] The contract clause also mandates that contractors "comply with the requirements in the Department of Commerce Information Technology Management Handbook.[187]

Other Departments And Agencies

Many federal departments and agencies that have not implemented separate cybersecurity regulations nevertheless have published policy manuals, handbooks, and web-based training information. For example, the Department of Transportation (DOT) issued Order 1351.37 in June 2011, explaining "Departmental Cybersecurity Policy" and laying out "processes, procedures, and standards" applicable to contractors that provide services involving information systems.[188] And a DOT component, the Federal Highway Administration, has issued its own Cybersecurity Program Handbook.[189] Similarly, the Department of Energy publishes a manual titled Cybersecurity Framework Implementation Guidance[190] and maintains webpages regarding "Cybersecurity Training and Education" and "Cybersecurity for Critical Energy Infrastructure."[191] The Department of Education publishes a similar handbook.[192]

Classified Contracts

Government contractors with access to, or that possess, classified information must comply with the requirements of the National Industrial Security Program (NISP), which was established in January 1993 by Executive Order 12829.[193] The NISP is administered by the Defense Security Service (DSS), and its rules are set forth in the National Industrial Security Program Operating Manual (NISPOM).[194] In May 2016, DSS issued "Change 2" to the NISPOM that added several important cybersecurity-related requirements applicable to cleared contractors. Those revisions are discussed below, in conjunction with certain related requirements.

Establishment And Implementation Of An Insider Threat Program

Contractors subject to the NISPOM must "establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat" that is consistent with Executive Order 13587.[195] To satisfy those requirements, contractors must perform "self-inspections . . . related to the activity, information, information systems (ISs), and conditions of the overall security program, to include the insider threat program."[196] The contractors' self-inspections must be designed to obtain information related to cyber threats and incidents, as discussed below. Further, the contractor must prepare a formal report "describing [each] self-inspection, its findings, and resolution of issues found," and a "senior management official" at each cleared facility must certify in writing, on an annual basis, that the self-inspection was conducted and that any required corrective action has been taken.[197]

Mandatory Reporting Of Cyber Incidents On Cleared Systems

The NISPOM requires cleared contractors to "report immediately to DOD any cyber incident on a classified covered IS."[198] The report must include at least the following information:

(1) A description of the technique or method used in the cyber incident.

(2) A sample of the malicious software, if discovered and isolated by the [cleared defense contractor] , involved in the cyber incident.

(3) A summary of information in connection with any DOD program that has been potentially compromised due to the cyber incident.[199]

The NISPOM's chapter regarding contractors' "Security Responsibilities and Duties" related to ISs contains important provisions applicable to cyber incident reporting. For example, paragraph 8-100(d) requires that contractors "implement protection measures. . ., including tools or capabilities required by the [agency] to monitor user activity on classified ISs in order to detect activity indicative of insider threat behavior." Thus, the NISPOM mandates that contractors install applications allowing them to obtain records of, and analyze users' access to, classified information.

In addition, contractors with access to classified information must implement "a risk-based set of management, operational and technical controls" that facilitate detection and intervention of cyber incidents and threats. These include training (discussed below); testing and evaluation procedures to detect threats; processes for responding to security incidents; plans for maintaining continuity of IS operations; and implementing any necessary remedial measures to address deficiencies.[200]

After a cyber incident, the NISPOM requires that contractors with classified information systems provide DOD with "access to equipment or information . . . that is necessary to conduct forensic analysis in addition to any analysis conducted" by the contractors.[201] Contractors are "only required to provide access to equipment or information . . . to determine whether information was successfully exfiltrated from [the contractor's] classified covered IS and if so, what information was exfiltrated."[202] Given the strict Governmental oversight of IS systems with classified information, the Government is likely to perform an invasive analysis of any system that is the subject of a cyber incident.

Needless to say, a contractor's ability to provide immediate reporting of any cyber incident requires diligent monitoring of its systems. Such monitoring protocols should be set forth in the contractor's insider threat program (as discussed above).

Security Training And Briefings Under The NISPOM

The "Change 2" revisions to the NISPOM also enhanced cleared contractors' obligations for trainings and briefings to be provided to all employees with access to classified information. Personnel with access to classified systems or information must receive instruction regarding cyber threats, including the importance of detecting such threats; methodologies used by adversaries to "collect classified information, in particular within ISs"; and "security reporting requirements."[203] The training also must include explanations of the "security risks associated with their user activities and [their] responsibilities under the NISP."[204]

All cleared employees must be provided initial security briefings before being provided access to classified information. Among other things, that training must explain how the IS users will "[c]omply with the IS[] security program requirements as part of their responsibilities," be accountable for their actions on an IS, and protect authentication mechanisms such as passwords (including at the appropriate classification level).[205] Contractor employees also

should be informed that they are "subject to monitoring of their activity on any classified network and [that] the results of such monitoring could be used against them in a criminal, security, or administrative proceeding."[206]

In addition to the initial training that all cleared contractor employees must receive, the NISPOM mandates that they must receive "refresher training" each year to "reinforce the information provided during the initial security briefing and . . . keep cleared employees informed of appropriate changes in security regulations," including the rapidly changing cybersecurity rules.[207]

Defense Industrial Base Cybersecurity Program

To enhance the ability of DOD contractors (and subcontractors) to deal with cyber attacks, DOD created a voluntary Defense Industrial Base (DIB) Cyber Security (CS) Program with the objective of encouraging information sharing between contractors and the Government. Initiated in a 2008 pilot, the Program was established by an interim final rule in 2012.[208] That rule provided for eligible DIB companies and the Government to share information. The rule added regulations at 32 C.F.R. Part 236 that provided the requirements and framework for the voluntary Program.

The DIB Program changed significantly through an interim rule in October 2015 that was aimed at broadening participation and also included mandatory reporting requirements.[209] The 2015 interim rule included mandatory cyber incident reporting applicable to all types of contracts or any other agreements between DOD and DIB companies.[210] DOD indicated that it was focused on cyber incidents posing a threat to Program information such as technical information subject to restriction under the International Traffic in Arms Regulations or the Export Administration Regulations or technical information otherwise controlled by DOD and operational security information related to DOD activities.[211] (This raises a question whether reporting may be required to the applicable export control authority.) DOD recognized that the information being shared was extremely sensitive, warranting additional protections.[212]

DOD issued a final rule governing DIB Cybersecurity Activities on October 4, 2016, effective November 3, 2016.[213] The commentary explains that the revisions were directed at establishing a single reporting mechanism for cyber incidents on unclassified DOD contractor networks or information systems.[214] (Cyber incident reporting involving classified systems is addressed under the NISPOM.[215]) The regulations require "all DOD contractors" to report cyber incidents involving covered defense information on unclassified contractor information systems or cyber incidents affecting the contractor's ability to provide operationally critical support within 72 hours.[216] The regulations also permit "eligible DIB participants to participate" in the voluntary DIB information sharing program.[217] Contractors "eligible" to participate in the DIB CS program are cleared defense contractors (CDC) that also have an existing Facility Security Clearance at least at the Secret level and that execute the Framework Agreement (FA). [218] This rule, consistent with the approach in the 2015 interim rule, changes the character of the DIB program—information sharing by DIB companies is voluntary, but reporting is extensive and mandatory.

During the comment period, a question was raised regarding the meaning of "operationally critical support." DOD indicated that it will develop procedures to "ensure" that contractors receive notice when they are providing supplies or services that are designated as operationally critical support.[219] The regulations define operationally critical support as "supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency situation."[220] If contractors are unclear whether their activities are operationally critical they are directed to ask for clarification from the Contracting Officer.[221] If you are unsure, you should promptly and in writing seek clarification and recognize that the situation may be fluid such that supplies and services that are not critical one day, may become so the next day. This requirement may be particularly difficult for nontraditional contractors, such as holders of other transaction agreements (OTs), or grant participants, that have sub-agreements and may not be aware that their work could become operationally critical.

Mandatory Reporting

Under the regulations, the requirement to report "shall" be included in "all forms of agreements . . . between the Government and the contractor in which covered defense information resides on, or transits covered contractor information systems or under which a contractor provides operationally critical support."[222] Agreements include contracts, grants, cooperative agreements, OTs, technology investment agreements, and "any other type of legal instru-

ment or agreement."[223] The coverage of the regulations thus is broader than the DFARS clauses because they go well beyond procurement contracts to reach OTs, grants, cooperative agreements, and, although not named, would reach any other form of financial assistance agreement. This portion of the rule may be problematical for subcontractors that are not DIB participants but have subcontracts or sub-agreements under one of these nonprocurement instruments. It is worth noting that OTs, grants, and cooperative agreements are frequently used with small businesses, nonprofit entities, academic institutions, and other entities that may not have experience in traditional defense contracting.

The regulations require that contractors flow down the cyber incident reporting requirements to their subcontractors that are providing "operationally critical support" or "for which subcontract performance will involve a covered contractor information system."[224] Subcontractors must be required to report cyber incidents directly to DOD (at https://dibnet.dod.mil) and to the prime contractor within 72 hours.[225]

To report cyber incidents under this rule, the contractor or subcontractor "shall" have a DOD-approved medium assurance certificate.[226]

"Covered Defense Information" And CUI

The regulations align the definition of "covered defense information" with the definition of "controlled unclassified information." The commentary states that the definitions are intended to be consistent with the Government-wide CUI definition.[227] The final rule provides that CUI means "unclassified controlled technical information or other information (as described in the CUI Registry at http://www.archives.gov/cui/registry/categoy-list.html)" that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies and is (1) marked or identified in an agreement and provided to the contractor by or on behalf of DOD to support performance, or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance.[228] You should note that "on behalf of" could cover service providers or other suppliers that have or use information to support the contractor or subcontractor in connection with performance of the contract/subcontract. The commentary on the rule also notes that it is harmonized with the DFARS Network Penetration and Cloud Services Case 2013-D018 (that resulted in the 2016 final DFARS rule discussed above) and the FAR Case 2011-020 on Basic Safeguarding of Contractor Information Systems (that resulted in the 2016 final FAR rule discussed above).[229] In the context of procurement contracts, the requirements of this rule are to be implemented through the DFARS, *i.e.*, DOD contractors report cyber incidents in accordance with the clause at DFARS 252.204-7012.[230]

Government Use Of Incident Reports

The Government may use and disclose information received in connection with incident reports for Government purposes. With respect to "contractor attributional/proprietary" information, the Government "shall" protect such information against "unauthorized use or release."[231] Contractors are required to identify and mark attributional/proprietary information.[232] The Government commits in the regulations to implement procedures that will seek to minimize the contractor attributional/proprietary information that is released to only that which is necessary for authorized purposes.[233] The regulations are clear that contractor attributional/proprietary information (*i.e.*, information obtained from the contractor) that is not created by or for DOD *is* authorized to be released outside of DOD.[234] Authorized purposes for release include, among others, release to entities assisting in diagnosis, detection, or mitigation of cyber incidents; release to support services contractors supporting the Government in this mission that have signed nondisclosure agreements (NDAs);[235] and release for national security purposes.[236] The regulations require the NDA to contain certain terms to protect the contractor that filed the incident report.[237] You must take steps to mark your information and to ensure that the Government and any party to whom it releases information about the incident comply with the requirements for a robust NDA.

Contractor attributional/proprietary information that is created "by or for" DOD is authorized to be used and released outside of DOD for purposes authorized by the regulations and for any other lawful Government purpose—subject to all applicable statutory, regulatory, and policy restrictions.[238] DOD commits to complying with the Freedom of Information Act, including informing a contractor of requests to allow the contractor to challenge release.[239]

Information Sharing Regarding Threats And Security Practices

The commentary to the 2016 final rule states that the DOD objective is to enable greater participation in the voluntary cybersecurity Program,[240] which is viewed as integral to a comprehensive approach to counter cyber threats

through information sharing between the Government and DIB participants. DOD states that the Program has substantial benefits because it allows "eligible" DIB participants to receive Government furnished information and cyber threat information from other DIB participants, which allows all involved to gain greater insight into adversarial activity that is targeting defense contractors.[241] The Program is intended to create a collaborative environment to share actionable unclassified cyber threat information that can improve cybersecurity for the DIB.[242] Significantly, the Program provides access to Government classified threat information—with appropriate clearance—that allows companies to better understand threats, as well as allowing technical assistance from the DOD Cyber Crime Center (DC3). Information sharing of this nature allows both DOD and the DIB participants to understand adversary actions and the impact on warfighting capabilities.[243]

To participate in the DIB voluntary CS Program, a contractor must be a Cleared Defense Contractor (CDC), *i.e.*, granted clearance at least at the Secret level, to access, receive, or store classified information, and execute the standard FA with the Government.[244] The FA allows the CDC to determine its level of participation in the voluntary DIB CS Program. As a CDC, you elect the level of participation with which you are comfortable. The FA is tailored to implement the voluntary information sharing with each participant.[245]

DOD's DIB CS Program Office is the point of contact for this Program. However, the DC3 managed DOD DIB Collaborative Information Sharing Environment is the *operational* focal point for cyber threat information and incident reporting, *i.e.*, operational issues are the responsibility of DC3.[246]

Confidentiality of information that is exchanged in the voluntary Program is protected to the maximum extent authorized by law, regulation, and policy.[247] The regulations make clear that each participant is responsible for its own actions, *i.e.*, appropriate compliance mechanisms must be in place to protect information.[248] DIB participants and the Government may limit or terminate their participation in the Program at any time—it is voluntary. However, termination does not relieve the contractor of responsibility to protect information that was exchanged under the Program as required by law or the FA.[249] You should consider carefully whether to participate in the Program and whether you can manage the compliance requirements.

Under the regulations, the Government "shall" share Government Furnished Information (GFI) with Program participants, depending upon their level of participation. [250] GFI is defined as information provided by the Government under the voluntary DIB CS program, including, but not limited to, cyber threat information and cybersecurity practices.[251] GFI also may be shared with a designated Service Provider (SP).[252] Receipt of GFI is subject to significant restrictions:

- Prior to receiving GFI, the participant (or designated SP) must identify the individuals who will be receiving the information, to include security clearance and citizenship information. The Government will verify the eligibility of the individuals to receive the information.[253]

- GFI can be used only on U.S.-based covered contractor information systems, or U.S.-based networks for information systems used to provide operationally critical support.[254]

- GFI may only be shared within an organization on a "need-to-know" basis, with distribution restricted to U.S. citizens.[255] No sharing outside the participant's organization is permitted without advance approval—regardless of clearance level; provided that if the contractor uses an SP for information system security services, the contractor may share GFI with that SP as approved by the Government.[256]

- GFI may be shared by the Government by means of both unclassified and classified means; participants must comply with NISPOM requirements.[257] Note that in order for participating CDCs to receive classified threat information electronically, they must (1) have a Communication Security (COMSEC) account as provided for in the NISPOM, (2) have approval for safeguarding information at least at the Secret level, and (3) obtain access to DOD's secure voice and data transmission systems that support the voluntary DIB CS Program.[258]

Participation in the voluntary Program requires careful planning, assessment of risks of participation, and a compliance program. It is up to the contractor to determine whether the benefits of participation are meaningful and worth the cost for its operations.

Liability Protection—No Regulations

In connection with the issuance of the 2016 final rule, a

commenter recommended that the rule include provisions for liability protection.[259] Section 1641 of the National Defense Authorization Act for Fiscal Year 2016 (FY 2016 NDAA) contains provisions providing protection from liability for "operationally critical contractors" pursuant to 10 U.S.C.A. § 391 and "cleared defense contractors" pursuant to 10 U.S.C.A. § 393.[260] The liability protections are the same in each provision and include the protection that no cause of action may be maintained in any court against the identified types of contractors for compliance with procedures required to be established by DOD requiring (1) operationally critical contractors to report cyber incidents and (2) cleared defense contractors to report penetrations of the contractor's network of information systems. In response to the referenced comment regarding liability protection, DOD noted that the liability protections established by 10 U.S.C.A. §§ 391 and 393 became effective after the date of the October 2015 interim final rule. DOD then stated that the regulatory implementation of these new statutory provisions would be addressed through a future rulemaking with the opportunity for public comment.[261] Similarly, the commentary accompanying the 2016 DFARS final rule indicates that DOD received a recommendation that the rule include the liability protections provided for in the § 1641 of the FY 2016 NDAA.[262] In response to that inquiry, DOD noted that "DFARS case 2016-D025, Liability Protections when reporting Cyber Incidents, was opened on April 20, 2016 to implement section 1641 of the FY 2016 NDAA."[263] Consistent with the scope of the NDAA, that DFARS Case indicated that it was limited to amending the DFARS to specify liability protections for cleared defense contractors and operationally critical contractors when reporting cyber incidents and network penetrations.[264] DOD subsequently closed the DFARS liability protection case without comment.

Supply Chain Management

A key element of cyber risk is the supply chain. Supply chain attacks primarily arise from (1) malicious insertion of a defect or malware and (2) exploitation of latent vulnerabilities.[265] There are at least two challenges faced in addressing cybersecurity in the supply chain. First, due to the long development period, it is common for many electronic parts to become obsolete between the time a system is designed and fielded.[266] Second, industry increasingly relies on commercial products as DOD becomes a less prominent consumer of complex electronics.[267]

DOD instructions emphasize the importance of guarding against cyber risk in the supply chain. DOD Instruction 5000.02 states that when a "DOD capability advantage derives from the integration of commercially available or custom-developed components, program protection manages the risk that design vulnerabilities or supply chains will be exploited to destroy, modify, or exfiltrate critical data, degrade system performance, or decrease confidence in a system."[268] Enclosure 14 to the Instruction addresses responsibilities for assessment of cyber risks. The enclosure emphasizes that Government Program Managers must assess risks and implement safeguards in every phase of a program.[269] The Program Protection Plan should guide the program and be included in solicitations.[270] Program Managers are required to derive cybersecurity requirements into system specifications.[271]

NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," specifically addresses supply chain risk management. It explains that supply chain risks "include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware (*e.g.*, GPS tracking devices, computer chips, etc.), as well as poor manufacturing and development practices in the [information and communications technology] supply chain."[272]

Government contractors procure a wide range of IT products and services as well as electronic parts that can pose cyber threats due to the use of counterfeit parts or other vulnerabilities. In addition to complying with the DOD counterfeit parts rule,[273] companies must be attentive to cyber risks in their supply chains.

Government contractors (and companies that frequently obtain subcontracts under Government contracts) are accustomed to the process of negotiating appropriate flow-down clauses for inclusion in subcontracts and other supply agreements. These negotiations can be straightforward at times, but difficult at others. Negotiations can be difficult for the prime contractor when a clause itself does not include an express flow down requirement that the prime contractor can cite during negotiations, but the prime wishes to include the clause to mitigate its risk or to make its procurement approach more uniform. The negotiations can be difficult for a subcontractor or supplier if the high-tier contractor insists on boilerplate terms that do not appear to be tailored to the unique circumstances or application of a particular purchase.

Flow-Down Clauses

The FAR requires contractors to include the substance of

the FAR cyber clause, including the flow-down requirement, in "subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system."[274] The flow-down thus extends past the first tier of subcontractors, although COTS items are excepted.[275]

As noted above, the clause at DFARS 252.204-7012 also has flow-down requirements that apply to commercial items. The DFARS clause itself is not to be included in solicitations and contracts that are solely for the acquisition of COTS.[276] The contractor must include the clause (including the flow-down requirement) in "subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration."[277]

As noted, the clause must be flowed down to subcontracts for which performance will involve CDI. The contractor must make an assessment if the information required for performance by its subcontractor(s) retains its identity as "covered defense information."[278] The contractor may consult with the CO "if necessary," [279] but the DFARS clause does not state that the CO is required to provide direction or expressly confer any safe harbor for relying on the CO's views.

RFP Terms

In addition to the standard FAR and DFARS clauses discussed above, solicitations may include program or project-specific security requirements that implicate cyber protections or practices. Therefore, you should carefully review solicitations for cybersecurity requirements that the agency may have included beyond clauses required by regulations.

Practical Considerations For Flow-Down

In light of the potential uncertainty as to whether a subcontract will involve federal contract information (FAR clause) or CDI (DFARS clause) and the application of the flow-down requirement to commercial items, some prime contractors (or larger subcontractors) may flow down the cyber clause as a matter of course as a standard term and insist on its inclusion. Prospective subcontractors thus may need to seek and obtain greater clarification from the prime contractors to avoid unnecessary inclusion of the clauses in subcontracts. Although the lack of privity between an agency and a subcontractor normally would weigh against Government involvement in this process, the DFARS cyber rule is somewhat unique in that it calls for direct communications between the agency and a subcontractor notwithstanding the lack of privity in the context of reporting a cyber incident to DOD.

As is typical for flow-down requirements, neither the FAR nor DFARS provides guidance regarding what to do if a prospective subcontractor refuses to accept a flow-down clause. However, in the commentary accompanying the 2016 rule, DOD stated that if a subcontractor does not agree to comply with the terms of DFARS 252.204-7012, then CDI "shall not be on that subcontractor's information system."[280]

The DFARS clause does not specify what, if anything, a prime contractor (or next higher-tier subcontractor) should do if it suspects a covered subcontractor has failed to report an incident. Some contractors may feel obligated to report such failures under the FAR mandatory disclosure rule.[281]

Diligence

For regular suppliers, a prime contractor or high-tier subcontractor might consider requesting or requiring periodic audits or assessments for cyber risk. These assessments can gauge vulnerabilities or security gaps in the subject's operations.

Indemnification

To mitigate its exposure, a prime contractor may wish to include cyber indemnification clauses in subcontracts and supply agreements. At a minimum, a prime contractor (or higher-tier subcontractor) might require a supplier to indemnify it with regard to the costs associated with any cyber incident that has been (or should have been) reported.

DOD Evaluations And Exclusions Of Sources

Supply chain risk also may lead to the denial of DOD business for prime contractors and their subcontractors and suppliers. For certain procurements, supply chain risk must be included as an evaluation factor and use of that factor can lead to the exclusion of sources. Specifically, such a factor must be applied to relevant purchases of enterprise software agreements under the Multiple Award Schedule,[282] acquisition of other commercial items under FAR Part 12,[283] and FAR Part 14[284] and FAR Part 15[285] procurements of covered systems. The rule implements a statutory mandate for DOD

to consider supply chain risk posed by hardware and software.[286]

DFARS Subpart 239.73 sets forth requirements for information relating to supply chain risk. The DFARS specifies supply chain protections to be taken with regard to certain information systems, including telecommunications systems.[287] These rules apply to IT (whether acquired as a service or supply) that is a "covered system." A "covered system" is "any information system" that is "used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency" that involves "intelligence activities," "cryptologic activities related to national security," "command and control of military forces," or "equipment that is an integral part of a weapon or weapons system" or that is "critical to the direct fulfillment of military or intelligence missions."[288] A covered system includes an information system that is protected by procedures established for information that is to be kept classified in the interest of national defense or foreign policy.[289] A covered system does not include a system used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management applications.[290]

The rules at DFARS Part 239 are intended to guard against "supply chain risk," which is "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system" so as to "surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[291]

The rules at DFARS Part 239 confer considerable discretion on the Government to assess supply chain risk and to take action to protect the Government. The rules permit certain designated officials to exclude sources from procurements for covered systems due to the supply chain risk they pose. The agency may (1) exclude a source that fails to meet qualification standards established to reduce supply chain risk in the acquisition of covered systems; (2) exclude a source that fails to achieve an acceptable rating for a supply chain risk evaluation factor for the award of a contract or task or delivery order; or (3) withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.[292] The agency may consider information, public and nonpublic, including all-source intelligence, relating to the offeror and its supply chain in making its decision.[293] Although the rules contemplate the possibility (as noted above) of exclusions based on failure to meet qualification standards, DOD has not yet developed such standards and would publish them prior to use.[294]

The agency is supposed to advise prospective offerors through the inclusion of a FAR clause[295] in the solicitation and contract that supply chain risk will be assessed. The specific parameters of the evaluation factor are not defined and instead are left to agencies to craft for specific solicitations. That raises the prospect that the factors used may vary—possibly to a significant degree—by solicitation.

Review Of A DOD Supply Chain Risk Exclusion Decision

An agency decision to exclude a source under the authority discussed above is not reviewable in a bid protest.[296] DFARS 239.7305 does not state that the exclusion is unreviewable in any respect, which raises the prospect that a contractor might be able to challenge the action in district court. Any such challenge, however, is likely to face a motion to dismiss by the Government on the basis of lack of jurisdiction or justiciability.

When it excludes a source, the agency is required to give notice of the exclusion and its basis "only to the extent necessary to effectuate the action."[297] The agency may limit the information to be disclosed, notwithstanding any other provision of law (such as the Freedom of Information Act or the Privacy Act).[298] The official who makes the exclusion decision is required to notify other DOD components or other federal agencies responsible for procurements that may be subject to the same or similar supply chain risk, in a manner that is consistent with the requirements of national security.[299] A supplier thus may be given very limited information regarding the perceived risk and little insight as to how to address it to avoid future exclusions.

In sum, DOD may exclude a source and a contractor may be unable to challenge such an exclusion. Posing a further challenge, the information justifying the exclusion can be shared with other agencies (which may result in findings of nonresponsibility for a given procurement or other adverse consequences).

On The Horizon

As shown above, cybersecurity has been a key area of focus for DOD and civilian agencies over the last half decade. Contractors can expect that emphasis to continue.

What is next for cybersecurity? As of this writing, and as mentioned previously, there is a new CUI rule in the works, FAR Case 2017-016, to ensure uniform implementation of the CUI Program across the Government. The rule reportedly will feature a FAR clause that will apply the requirements of the federal CUI regulations and NIST Special Publication 800-171 to contractors.[300] An internal report on the rule is due in early November 2017.[301] Regardless of whether (and when) this rule is issued, contractors can expect ongoing developments in the area of cyber safeguards and reporting. At a minimum, contractors can expect the security requirements in NIST Special Publication 800-171 to be referenced in federal contracts and solicitations.[302]

Conclusion

Cyber attacks, including the Equifax data breach and reports of Russian election hacking, continue to make front page news. The Federal Government has responded—and continues to respond—with extensive cybersecurity efforts and vast amounts of information that are difficult if not impossible to digest fully. As discussed above, the Government has significantly stepped up its cybersecurity efforts with respect to federal contracts and subcontracts, issuing substantial regulations in 2016. These regulations, and those to come, represent a notable expansion of Government contracts law that is still in its infancy—as of this writing, there are no reported cases dealing with the 2016 regulations. The Government and its contractors are grappling with many aspects of the regulations, which undoubtedly will lead to numerous communications between agencies and industry, bid protests, and other litigation that may clarify many aspects of the rules.

For now, you should concentrate on understanding the cybersecurity rules that are in your contracts and subcontracts. The Government has provided resources to assist your understanding, including commentary in the Federal Register accompanying the promulgation of regulations. Take advantage of these resources and, when in doubt, reach out to your COs or other appropriate Government officials for guidance. As mentioned previously, compliance with the new rules will not only help you avoid negative consequences such as poor past performance ratings, but also can bolster your defenses against costly attacks on your information systems—attacks that are all too prevalent in today's world.

Guidelines

These *Guidelines* are intended to assist you in providing advice regarding Government contracting cybersecurity requirements. They are not, however, a substitute for professional representation in any specific situation.

1. As part of your efforts to understand contract provisions and take steps to achieve and maintain compliance, you should consult with IT professionals. These can be your in-house professionals or third-party consultants.

2. Document in writing steps you take to ensure compliance with cybersecurity requirements. This should include, but not be limited to, system security plans if you are subject to NIST SP-800-171. Be sure to update this written documentation as you make ongoing changes to your information systems and other aspects of your cyber defenses to keep up with new requirements in your contracts and subcontracts.

3. By sure that all employees are familiar with cybersecurity requirements that are relevant to their responsibilities. Consider preparing and circulating written procedures implementing requirements and providing periodic training. For example, if you are subject to DFARS 252.204-7012, make sure that your IT personnel and other relevant personnel are familiar with the broad definitions of "cyber incident" (which includes the term "actual or potential adverse effect") and "compromise" (which includes the term "may have occurred").

4. If you have different versions of requirements in your contracts, such as different versions of the clause at DFARS 252.204-7012, or different versions of NIST SP 800-171 that apply, you should work with your COs to amend your contracts to include the latest versions of the requirements. This will eliminate the need to monitor compliance of different requirements impacting the same information systems.

5. Carefully review solicitations and proposed agreements for cybersecurity provisions. Take issue with provisions you conclude are not required or are otherwise inappropriate. Also take steps to ensure that you can comply with provisions that are appropriate.

6. Follow regulatory developments, including the pending FAR CUI rule, Case 2017-016, which reportedly will ensure uniform implementation of the CUI Program across the Government and create one or more FAR clauses. Individual agencies also may promulgate cybersecurity requirements and clauses.

7. For companies doing business with DOD, consider

participating in the DIB voluntary Cybersecurity Program to gain the benefits of shared information (including Government information) about threats and technical assistances from DC3. Because participation is voluntary, you can tailor your level of participation to your needs.

8. Prime contractors and higher-tier subcontractors should consider requesting or requiring periodic audits or assessments of common suppliers for cybersecurity risk. Prime contractors also should include cybersecurity indemnification clauses in subcontracts and supply agreements and ensure teaming agreements include an exception for any supplier exclusion or failure to consent due to supply chain risk.

9. Prospective subcontractors should ensure that the work scope is clearly defined to avoid unnecessary flow down of cybersecurity clauses.

ENDNOTES:

[1]Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," N.Y. Times, July 9, 2015.

[2]H.R. Comm. on Oversight and Gov't Reform, 114th Cong., The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation vii (Sept. 7, 2016).

[3]Comm'n on Enhancing National Cybersecurity, Report On Securing and Growing The Digital Economy 9 (Dec. 1, 2016).

[4]DOD, Cybersecurity Challenges: Protecting DoD's Unclassified Information 3, available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-08/DFARS%20252.204-7012%20%20%20Dec%2031%202017.pdf.

[5]Exec. Office of the President, Annual Report to Congress: Federal Information Security Modernization Act of 2014, at 3 (Mar. 10, 2017).

[6]81 Fed. Reg. 30,439 (May 16, 2016).

[7]81 Fed. Reg. 72,986 (Oct. 21, 2016).

[8]81 Fed. Reg. 63,324 (Sept. 14, 2016).

[9]78 Fed. Reg. 69,273 (Nov. 18, 2013).

[10]80 Fed. Reg. 51,739 (Aug. 26, 2015); 80 Fed. Reg. 81,472 (Dec. 30, 2015).

[11]E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat 2899, 2946 (2002).

[12]U.S. Gov't Accountability Office, GAO-16-294, Information Security: DHS Needs To Enhance Capabilities, Improve Planning, and Support Greater Adoption of its National Cybersecurity Protection System (Jan. 28, 2016).

[13]See 31 U.S.C.A. §§ 3729–3733.

[14]The E-Government Act of 2002 is at Pub. L. No. 107-347, 116 Stat. 2899 (2002). The FISMA of 2002 is at Title III of the E-Government Act of 2002.

[15]Pub. L. No. 107-347, § 301, 116 Stat. 2899, 2946 (2002).

[16]Pub. L. No. 107-347, § 301, 116 Stat. 2899, 2950 (2002).

[17]Pub. L. No. 107-347, § 302, 116 Stat. 2899, 2957 (2002).

[18]Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075–76 (2014) (codified as amended at 44 U.S.C.A. §§ 3551–3558).

[19]Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3074–76 (2014).

[20]Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3077 (2014).

[21]Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3085 (2014).

[22]81 Fed. Reg. 30,439 (May 16, 2016).

[23]81 Fed. Reg. at 30,440.

[24]81 Fed. Reg. 30,439.

[25]81 Fed. Reg. at 30,440.

[26]FAR 4.1902.

[27]FAR 4.1901.

[28]FAR 4.1903, 52.204-21(c).

[29]NIST SP 800-171, Rev. 1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (Dec. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[30]FAR 52.204-21(a).

[31]77 Fed. Reg. 51,496 (Aug. 24, 2012).

[32]81 Fed. Reg. at 30,441.

[33]FAR 52.204-21(a).

[34]81 Fed. Reg. at 30,441.

[35]81 Fed. Reg. at 30,441.

[36]81 Fed. Reg. at 30,441.

[37]81 Fed. Reg. at 30,445.

[38] 81 Fed. Reg. at 30,444.

[39]FAR 42.1501(a).

[40]See FAR 49.401(a) ("Termination for Default," "General"); FAR 49.402 ("Termination of fixed-price contracts for default").

[41]See FAR 52.212-4(m) ("Termination for cause" provision in clause in commercial item contracts).

[42]31 U.S.C.A. §§ 3729–3733.

[43]81 Fed. Reg. 72,986 (Oct. 21, 2016).

[44]78 Fed. Reg. 69,273 (Nov. 18, 2013).

[45]80 Fed. Reg. 51,739 (Aug. 26, 2015); 80 Fed. Reg. 81,472 (Dec. 30, 2015).

[46]81 Fed. Reg. at 72,997.

[47]See 82 Fed. Reg. 16,577 (Apr. 5, 2017).

[48]See http://dodcio.defense.gov/IID.aspx (recording of Industry Information Day (June 23, 2017)).

[49]81 Fed. Reg. 30,439 (May 16, 2016).

[50]DFARS 204.7300.

[51]DFARS 204.7304(c).

[52]DFARS 252.204-7012(m).

[53]DFARS 252.204-7012(a).

[54] DFARS 204.7301, 252.204-7012(a).

[55]81 Fed. Reg. 72,986, 72988 (Oct. 21, 2016).

[56]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, at 8–9 (Jan. 27, 2017), available at http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf [hereinafter 'FAQs"].

[57]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 25 (slides from DOD's Industry Information Day (June 23, 2017)).

[58]DFARS 204.7300.

[59]DFARS 204.7301, 252.204-7012(a).

[60]DFARS 252.204-7012(a).

[61]DFARS 252.204-7012(b)(1).

[62]DFARS 252.204-7012(b)(2)(i).

[63]DFARS 252.204-7012(b)(2)(ii)(A).

[64]DFARS 252.204-7012(b)(3).

[65]Memorandum from Shay D. Assad, Dir., Defense Pricing/Defense Procurement & Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" 3 (Sept. 21, 2017), available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf.

[66]NIST SP 800-171, Rev. 1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," at i (Dec. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[67]NIST SP 800-171, Rev. 1, at 8 (Dec. 2016).

[68]NIST SP 800-171, Rev. 1, at 10–16 (Dec. 2016).

[69]See NIST SP 800-171, Rev. 1, at 7 (Dec. 2016).

[70] NIST SP 800-171, Rev. 1, at 13 (Dec. 2016) (footnote omitted).

[71]NIST SP 800-171, Rev. 1, at 10 (Dec. 2016).

[72]NIST SP 800-171, Rev. 1, at 11 (Dec. 2016).

[73]NIST SP 800-171, Rev. 1, at 14 (Dec. 2016).

[74]NIST SP 800-171, Rev. 1, at 20–27 (Dec. 2016).

[75]See, e.g., Memorandum from Shay D. Assad, Dir., Defense Pricing/Defense Procurement & Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" (Sept. 21, 2017), available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf; DOD, Cybersecurity Challenges: Protecting DOD's Unclassified Information 14-17, available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-08/DFARS%20252.204-7012%20%20%20Dec%2031%202017.pdf; http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 40, 46, 57, 59, 61–63 (slides from DOD's Industry Information Day (June 23, 2017)).

[76]NIST SP 800-171, Rev. 1, at 14 (Dec. 2016).

[77]Memorandum from Shay D. Assad, Dir., Defense Pricing/Defense Procurement & Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" 3 (Sept. 21, 2017), available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf.

[78]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 59 (slides from DOD's Industry Information Day (June 23, 2017)).

[79] NIST SP 800-171, Rev. 1, at 4 (Dec. 2016).

[80]DFARS 252.204-7012(b)(2)(ii)(B), (C); 81 Fed. Reg. 72,986, 72991 (Oct. 21, 2016).

[81]DFARS 252.204-7012(b)(2)(ii)(B).

[82]FAQs at 14.

[83]FAQs at 12–13.

[84]FAQs at 13.

[85]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 42 (slides from DOD's Industry Information Day (June 23, 2017)).

[86]Memorandum from Shay D. Assad, Dir., Defense Pricing/Defense Procurement & Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" 6 (Sept. 21, 2017), available at http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf.

[87]81 Fed. Reg. 72,986, 72,997.

[88]FAQs at 6.

[89]DFARS 204.7304(a).

[90]DFARS 252.204-7008(c)(1).

[91]DFARS 252.204-7008(b)(2).

[92]DFARS 204.7302(b), 252.204-7012(c)(1).

[93]DFARS 204.7301, 252.204-7012(a).

[94]DFARS 252.204-7012(a).

[95]DFARS 252.204-7012(a) (emphasis added).

[96]DFARS 204.7302(b).

[97]DFARS 204.7302((b), 252.204-7012(m)(2)(ii).

[98]DFARS 252.204-7012(c)(1).

[99]DFARS 252.204-7012(c)(1)(i) (emphasis added).

[100]DFARS 252.204-7012(c)(2). Note that the citation in the regulation is http://dibnet.dod.mil; that has been updated to include an "s" after "http."

[101] See https://dibnet.dod.mil/portal/intranet/Splashpage/ReportCyberIncident.

[102]81 Fed. Reg. 72,986, 72,991 (Oct. 21, 2016).

[103]81 Fed. Reg. at 72,998.

[104]See DFARS 252.204-7012(c)(3).

[105]See https://iase.disa.mil/pki/eca/Pages/certificate.aspx.

[106]DFARS 252.204-7012(d).

[107]DFARS 252.204-7012(a).

[108]DFARS 252.204-7012(e).

[109]DFARS 252.204-7012(g).

[110]DFARS 252.204-7012(f).

[111]DFARS 252.204-7012(a).

[112]DFARS 252.204-7012(h).

[113]DFARS 252.204-7012(a).

[114]DFARS 252.204-7012(h).

[115]DFARS 252.204-7012(i).

[116]DFARS 252.204-7012(j).

[117]DFARS 252.204-7012(i).

[118]DFARS 252.204-7009(b).

[119]DFARS 252.204-7012(i)(2).

[120]DFARS 252.204-7012(c)(2), (j).

[121]DFARS 252.204-7012(j).

[122]See DFARS 252.204-7012(m)1); 81 Fed. Reg. 72,986 (Oct. 21, 2016).

[123]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 33 (slides from DOD's Industry Information Day (June 23, 2017)).

[124]DFARS 204.7302(d).

[125]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 49 (slides from DOD's Industry Information Day (June 23, 2017)).

[126]DFARS 239.7604.

[127]DFARS 239.7604(a).

[128] DFARS 252.239-7009(a).

[129]DFARS 252.239-7009(c).

[130]DFARS 239.7604(b).

[131]DFARS 252.239-7010(b)(2).

[132]DFARS 252.239-7010(d).

[133]DFARS 252.239-7010(e).

[134]DFARS 252.239-7010(f).

[135]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 49 (slides from DOD's Industry Information Day (June 23, 2017)).

[136]DFARS 252.204-7012(b)(2)(ii)(D).

[137]See http://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940, at 8 (slides from DOD's Industry Information Day (June 23, 2017)).

[138]DFARS 252.204-7012(b)(2)(ii)(D).

[139]FAQs at 25.

[140]75 Fed. Reg. 68,675 (Nov. 4, 2010).

[141]75 Fed. Reg. 68,675 (Nov. 4, 2010).

[142]81 Fed. Reg. 63,324 (Sept. 14, 2016).

[143]FAQs at 7.

[144]32 C.F.R. § 2002.4(y), (gg).

[145]32 C.F.R. § 2002.1(f).

[146]32 C.F.R. § 2002.16(a)(5)(iii).

[147]See 32 C.F.R. § 2002.4(c).

[148]32 C.F.R. § 2002.16(a)(6).

[149]32 C.F.R. §§ 2002.8(b)(2), 2002.16(a)(6).

[150]See, e.g., Office of Management and Budget, Office of Information and Regulatory Affairs, RIN 9000-AN56, "Federal Acquisition Regulation (FAR), FAR Case 2017-016, Controlled Unclassified Information (CUI)," available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN56.

[151]Memorandum from Mark A. Bradley, Dir., Information Security Oversight Office, NARA, to Heads of Executive Departments and Agencies, "Annual Report to the President on Agency Implementation of the Controlled Unclassified Information (CUI) Program for FY 2017" (Aug. 17, 2017), available at https://www.archives.gov/files/cui/documents/20170817-annual-reporting-fy2017.pdf.

[152]CUI Notice 2017-01, "Implementation Recommendations for the Controlled Unclassified Information Program" 9 (June 12, 2017), available at https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/2017-cui-notice-2017-01-implementation-recommendations.pdf.

[153]32 C.F.R. § 2002.14(b).

[154]32 C.F.R. § 2002.4(j).

[155]81 Fed. Reg. 63,324, 63,327 (Sept. 14, 2016).

[156]32 C.F.R. § 2002.4(j).

[157]32 C.F.R. § 2002.4(r).

[158]32 C.F.R. § 2002.4(p).

[159]32 C.F.R. § 2002.4(k).

[160]32 C.F.R. § 2002.14(h).

[161] 32 C.F.R. § 2002.14(h).

[162]See 81 Fed. Reg. at 63,325–26.

[163]81 Fed. Reg. at 63,327.

[164]32 C.F.R. § 2002.16(a)(6)(ii).

[165]81 Fed. Reg. at 63,332.

[166]81 Fed. Reg. at 63,333.

[167]32 C.F.R. § 2002.20(a)(7).

[168] 81 Fed. Reg. at 63,333 (emphasis added).

[169]81 Fed. Reg. at 63,333 (emphasis added).

[170]32 C.F.R. § 2002.50(a).

[171]48 C.F.R. § 652.239-71.

[172]48 C.F.R. § 652.239-71.

[173]48 C.F.R. § 652.239-71(a).

[174]48 C.F.R. § 652.239-71(a).

[175]48 C.F.R. § 652.239-71(b)–(e) (citing OMB Circular A-130, Appendix III (Security of Federal Automated Information Resources), available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf, and NIST SP 800-37, available at https://www.fismacenter.com/SP800-37-final.pdf.

[176]48 C.F.R. § 552.239-71.

[177]48 C.F.R. § 3052.204-70.

[178]Homeland Security Acquisition Regulation; Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001), 82 Fed. Reg. 6429 (Jan. 19, 2017).

[179]Homeland Security Acquisition Regulation; Information Technology Awareness Training (HSAR Case 2015-002), 82 Fed. Reg. 6446 (Jan. 19, 2017).

[180]Homeland Security Acquisition Regulation; Privacy Training (HSAR Case 2015-003), 82 Fed. Reg. 6425 (Jan. 19, 2017).

[181]48 C.F.R. § 1852.204-76.

[182]48 C.F.R. § 1852.204-76(c)(4).

[183]48 C.F.R. § 1852.204-76(c)(4); see https://itsecurity.nasa.gov/policies/index.html.

[184]48 C.F.R. § 1352.239-72.

[185]48 C.F.R. § 1352.239-72(f).

[186]48 C.F.R. § 1352.239-72(i).

[187]48 C.F.R. § 1352.239-72(d); see http://www.osec.doc.gov/opog/dmp/daos/dao200_0.html.

[188]See https://www.transportation.gov/sites/dot.gov/files/docs/DOT%20Order%201351.37%2C%20Departmental%20Cybersecurity%20Policy.pdf.

[189]See https://www.fhwa.dot.gov/legsregs/directives/orders/csp_handbook.pdf.

[190]See https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[191]See https://energy.gov/cio/training/cybersecurity-awareness-training-warehouse/doe-cybersecurity-training-and-education; https://energy.gov/oe/activities/cybersecurity-critical-energy-infrastructure.

[192]See https://www2.ed.gov/fund/contract/about/acs/ocio15.doc.

[193]See https://www.archives.gov/files/isoo/policy-documents/eo-12829.pdf.

[194]See http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf (current version, incorporating changes discussed below).

[195]NISPOM ¶ 1-202; see Exec. Order No. 13857, 76 Fed. Reg. 63811 (Oct. 7, 2011) (imposing requirements related to "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information").

[196]NISPOM ¶ 1-207(b)(1).

[197]NISPOM ¶ 1-207(b)(2), (3).

[198]NISPOM ¶ 1-401(a).

[199]NISPOM ¶ 1-401(b)(1)–(3).

[200]NISPOM ¶ 8-101(a)–(g).

[201]NISPOM ¶ 1-402(a).

[202]NISPOM ¶ 1-402(b).

[203]NISPOM ¶ 3-103.

[204]NISPOM ¶ 8-101(c).

[205]NISPOM ¶ 8-103(c).

[206]NISPOM ¶ 8-103(c).

[207]NISPOM ¶ 3-308.

[208]77 Fed. Reg. 27,615 (May 11, 2012).

[209]80 Fed. Reg. 59,581 (Oct. 2, 2015).

[210]80 Fed. Reg. at 59,582.

[211]80 Fed. Reg. at 59,582.

[212]80 Fed. Reg. at 59,582.

[213]81 Fed. Reg. 68,312 (Oct. 4, 2016) (amending 32 C.F.R. pt. 236).

[214]81 Fed. Reg. 68,312.

[215]81 Fed. Reg. 68,312.

[216]32 C.F.R. §§ 236.1, 236.2.

[217]32 C.F.R. § 236.1.

[218]32 C.F.R. § 236.7.

[219]81 Fed. Reg. at 68,314.

[220]32 C.F.R. § 236.2.

[221]81 Fed. Reg. at 68,314.

[222]32 C.F.R. § 236.4(a).

[223]32 C.F.R. § 236.4(a).

[224]32 C.F.R. § 236.4(d).

[225]32 C.F.R. § 236.4(d); see 32 C.F.R. § 236.2.

[226]32 C.F.R. § 236.4(e).

[227]81 Fed. Reg. at 68313.

[228]32 C.F.R. § 236.2.

[229]81 Fed. Reg. at 68,313.

[230]81 Fed. Reg. at 68314. See DOD's Defense Industrial Base Cybersecurity (DIB CS) Program, "A Public-Private Cybersecurity Partnership" 12 (Aug. 24, 2016), available at https://www.fbcinc.com/e/cybertexas/presentations/Room_302_Wed_1-145PM_Vicki_Michetti_DIB_101_Cyber_Texas_Aug15.pdf.

[231]32 C.F.R. § 236.4(l).

[232]32 C.F.R. § 236.4(l).

[233]32 C.F.R. § 236.4(l).

[234]32 C.F.R. § 236.4(m).

[235]32 C.F.R. § 236.4(m)(5)(iii), (iv).

[236]32 C.F.R. § 236.4(m) (2), (4), (5).

[237]32 C.F.R. § 236.4(m)(5).

[238]32 C.F.R. § 236.4(n).

[239]32 C.F.R. § 236.4(p).

[240]81 Fed. Reg. 68,312.

[241]81 Fed. Reg. 68,312.

[242]81 Fed. Reg. 68,312.

[243]81 Fed. Reg. at 68,313.

[244]32 C.F.R. §§ 236.5, 236.7.

[245]32 C.F.R. § 236.5(c).

[246]32 C.F.R. § 235(d).

[247]32 C.F.R. § 236.6(a).

[248]32 C.F.R. § 236.6(a).

[249]32 C.F.R. § 236.6(e).

[250]32 C.F.R. § 236.5(f), (h).

[251]32 C.F.R. § 236.2.

[252]32 C.F.R. 236.5(f).

[253]32 C.F.R. §§ 236.5(f), (g).

[254]32 C.F. R. 236.5(i)(1).

[255]32 C.F.R. § 236.5(i)(2) (exceptions are permitted with Government preapproval).

[256]32 C.F.R. §§ 236.5(l), (m).

[257]32 C.F.R. § 236.5(h).

[258]32 C.F.R. § 236.7(a).

[259]81 Fed. Reg. 68,312, 68,316 (Oct. 4, 2016).

[260]National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 1641, 129 Stat. 726, 1114 (2015).

[261]81 Fed. Reg. at 68,316.

[262]81 Fed. Reg. 72,986, 72,993 (Oct. 21, 2016).

[263]81 Fed. Reg. at, 72,993.

[264]81 Fed. Reg. at 72,993.

[265]Defense Science Board, DSB Task Force on Cyber Supply Chain 2-3(Apr. 2017), available http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF.

[266]See Defense Science Board, DSB Task Force on Cyber Supply Chain 5 (Apr. 2017), available http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF.

[267]See Defense Science Board, DSB Task Force on Cyber Supply Chain 2 (Apr. 2017), available http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF.

[268]DOD Instruction 5000.02, Encl. 3, at 92 (Aug. 10, 2017).

[269]See DOD Instruction 5000.02, Encl. 14, at 161, 164–68 (Aug. 10, 2017).

[270]DOD Instruction 5000.02, Encl. 14, at 163–64 (Aug. 10, 2017).

[271]DOD Instruction 5000.02, Encl. 14, at 158 (Aug. 10, 2017).

[272]NIST SP 800-161, at 7 (Apr. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[273]See, e.g., DFARS 252.246-7008 (clause focusing on risk posed by procuring electronic parts from sources other than original equipment manufacturer (OEM) or a supplier authorized by OEM to manufacture or sell the item).

[274]FAR 52.204-21(c).

[275]See FAR 52.204-21(c).

[276]See DFARS 204.7304(c).

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

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

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

[280]81 Fed. Reg. 72,986, 72,993 (Oct. 21, 2016).

[281]See FAR 52.203-13.

[282]DFARS 208.7402(2).

[283]DFARS 212.301(c).

[284]DFARS 214.201-5(c).

[285]DFARS 215.304(c)(v).

[286]See National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 806, 124 Stat. 4137, 4255 (2011), as amended by National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 806, 126 Stat. 1632, 1827 (2013).

[287]See DFARS 239.7300.

[288]DFARS 239.7301.

[289]DFARS 239.7301.

[290]See DFARS 239.7301.

[291]DFARS 239.7301.

[292]DFARS 239.7305(a), (b), (c).

[293]See DFARS 252.239-7017(b), 252.239-7018(c).

[294]See 80 Fed. Reg. 67244, 67249 (Oct. 30, 2015).

[295]See DFARS 252.239-7017, 252.239-7018.

[296]DFARS 239.7305(d)(1).

[297]DFARS 239.7305(d)(2)(i).

[298]DFARS 239.7305(d).

[299]DFARS 239.7305(d)(2)(ii).

[300]See NIST SP 800-171, Rev. 1, at 3 n.9 (Dec. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[301]See http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf at 3 (addressing FAR Case 2017-016).

[302]See NIST SP 800-171, Rev. 1, at 3 n.9 (Dec. 2016), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

NOTES:

NOTES:

BRIEFING PAPERS