Cybersecurity: How to Successfully Navigate CMMC and the DFARS

By Reginald M. Jones & Mary Mikhaeel

Reginald M. Jones

Mary Mikhaeel

The U.S. Department of Defense (DOD) has long been vigilant in maintaining the security of its own internal computer systems and networks. Now, it is requiring DOD contractors to take aggressive steps to secure their information systems that store, transmit, or process government data in the performance of DOD contracts. The big change for federal contractors is the addition of contract requirements designed to protect unclassified, but nonetheless sensitive, government data. Understandably, contractors want to know what is required, how those requirements can be met, how much it will cost, and whether associated costs are reimbursable.

The purpose of this article is to tie all of the seemingly complex and costly requirements together in one, easy-to-follow document. Part II explains the history of the federal regulations that govern cybersecurity because the rules have evolved over nearly 20 years, and without the history it is hard to understand the present. Parts III and IV provide practical guidance on how to navigate the Defense Federal Acquisition Regulation Supplement (DFARS) contract clauses and Cybersecurity Maturity Model Certification (CMMC) Version 1.0 requirements. Parts V and VI explain the consequences of noncompliance and provide a conclusion.

The Federal Cybersecurity Regulatory Framework and History

The purpose of the current DOD regulations is to ensure that unclassified DOD information residing on a contractor's internal information system (i.e., computers, computer networks, and any third-party-provided cloud-based network) is safeguarded from cyber incidents. Simply stated, a "cyber incident" is any action taken through the use of computers or computer networks that compromises or potentially adversely affects an information system or the data residing on that system.[1] The regulations seek to assess and minimize the consequences associated with cyber incidents through reporting and damage assessment processes. While that sounds straightforward, the process to develop coherent regulations has been long and is still evolving. In order to understand how DOD arrived at its current contract requirements, it helps to understand how the federal government has responded legislatively and regulatorily to increasing cyber threats. The following sections address the Federal Information Security Management Act of 2002 (FISMA), subsequent Executive Orders, and efforts by the National Institute of Standards and Technology (NIST), the governing body that produces the detailed technical requirements that DOD later implemented through the DFARS contract clauses.

DOD currently regulates nonfederal (i.e., DOD contractors') information systems security primarily through four DFARS contract clauses:

- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting);
- DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls);
- DFARS 252.239-7009 (Representation of Use of Cloud Computing Services); and
- DFARS 252.239-7010 (Cloud Computing Services).

In addition to the contract clauses, DOD recently introduced the CMMC, which is a certification process that will largely satisfy the DFARS contract requirements but is still a work in progress. CMMC is a verification mechanism under which contractors will have to pass an audit in order to obtain the required certification.

In order to understand how the contract clauses and the CMMC work together, contractors need to understand the history behind the still-evolving standards.

FISMA & Key Cybersecurity-Related Executive Orders

The first statute to attempt to address federal cybersecurity on a government-wide basis was the Federal Information Security Management Act of 2002 (FISMA).[2] Unlike the current DFARS clauses, FISMA applied only to federal government information systems and those maintained by contractors on behalf of the federal government.[3] Implementing regulations were agonizingly slow to follow, and executive orders drove the process more than congressional action. Congress ultimately repealed and replaced FISMA in 2014 with the Federal

continued on page 31

Reginald M. Jones is a partner and Mary Mikhaeel is an associate with Fox Rothschild LLP in Washington, D.C.

continued from page 1

Information Security Modernization Act of 2014, also known as FISMA Reform.[4] Until FISMA Reform, NIST and the Office of Management & Budget were in charge of federal cybersecurity.

In practical terms, the first meaningful guidance federal agencies had to help them manage the security of information systems was Executive Order (E.O.) 13556 (Controlled Unclassified Information), issued by President Obama in 2010.[5] This executive order created the Controlled Unclassified Information (CUI) registry, discussed more fully below, and provided the first and only uniform system for identifying and classifying information that could be subject to cyberattacks.[6] Section 1 of the executive order conceded that "at present, executive departments and agencies employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information [i.e., information that should be protected]. . . . This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents."[7]

That is not to say that federal agencies were not working hard on standards to use to defend against cyber threats; they most certainly were. For example, NIST first issued NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems) in February 2005.[8] Further, the advance notice of proposed rulemaking (ANPR) for DFARS contract clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) was published in March 2010 (the year before E.O. 13556), and the first draft of the clause was issued shortly after the issuance of E.O. 13556.[9] However, specific contract guidance to contractors and vendors was slow to form and uniformity among standards is still an unmet goal.

In order to make sense of the current DFARS requirements, it is helpful to understand three regulatory frameworks—NIST Special Publications, the Federal Acquisition Regulation (FAR), and the Defense Federal Acquisition Regulation Supplement (DFARS)—and how they relate to one another.

The NIST Requirements

The National Institute of Standards and Technology (NIST) is a sub-agency of the U.S. Department of Commerce.[10] NIST "is responsible for developing information security standards and guidelines, including minimum requirements for federal systems."[11] And like every good superhero, NIST has its own unique origin story. Congress created NIST (then known as the National Bureau of Standards) in 1901 to create a uniform metric system.[12] Thus, America's powerhouse of uniform standardization was born. NIST is relevant in cybersecurity today because NIST has established the standards with which the DFARS contract clauses require contractors to comply and the standards by which the agencies must conform.

Relevant to the DFARS contract requirements, there are three NIST special publications (SP) that address privacy of federal information systems specifically:

- NIST SP 800-18 (Guide for Developing Security Plans for Federal Information Systems);
- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations); and
- NIST SP 800-171(Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

NIST SP 800-18 was first published in December 1998.[13] In response to FISMA, NIST SP 800-18 was completely revised and replaced through Revision 1 in February 2005.[14]

The second special publication, NIST SP 800-53, was created in response to FISMA in February 2005 and addressed the government's computer systems and networks.[15] The initial version of DFARS contract clause 252.204-7012, first published in 2013, required contractors to comply with certain portions of this NIST manual.[16]

The third, NIST SP 800-171, unlike the previously mentioned two special publications, governs nonfederal information systems.[17] In other words, it provides guidance for DOD contractors, rather than DOD itself. It was first issued in June 2015 in response to FISMA Reform.[18] NIST issued Revision 1, which is currently in effect, in December 2016.[19] Currently Revision 2 and 800-171B, a supplement that focuses on "Enhanced Security Requirements for Critical Programs and High Value Assets," are currently in draft.[20] DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) and DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) require DOD contractors to comply with NIST SP 800-171 Revision 1.

The FAR Requirements

In 2016, DOD, GSA, and NASA issued a final rule amending the FAR to include FAR contract clause 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).[21] This cybersecurity clause is important for a number of reasons. First, it was the first contract clause to meaningfully address cybersecurity for information systems across all agencies. Second, it was born out of DOD's early attempts to uniformly safeguard unclassified information itself, not just the information systems through which unclassified information flows or is stored.[22] Third, it does not require any training, penetration testing, cyber incident reporting, or cybersecurity

insurance because the rule does not address Controlled Unclassified Information (CUI) or classified federal information systems.[23]

The requirements in FAR 52.204-21 are intended to be "reflective of the actions a prudent business person would employ", and they apply to all federal contractors, not just DOD contractors.[24] The clause contains fifteen basic safeguarding requirements to safeguard contractors' information systems. NIST SP 800-171 defines information system as "a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[25]

The history of FAR 52.204-21 helps contractors understand how the rulemaking process has evolved over time since the enactment of FISMA to protect against cybersecurity threats. FAR 52.204-21 originated in 2010 when DOD published an Advance Notice of Proposed Rulemaking (ANPR) to address basic and enhanced safeguarding procedures to protected unclassified information.[26] The ANPR arose out of DFARS Case 2008-D028, Safeguarding Unclassified Information.[27] The ANPR was one of DOD's earliest attempts to create safeguarding procedures for CUI.[28] Ultimately, no DFARS rule was ever published based on that ANPR, and the FAR Councils[29] published this FAR rule to implement a rule to protect information *systems*, as opposed to information itself—a crawl-before-you-can-walk approach. In response to a question, the FAR Councils stated:

> This rule establishes minimum standards for contractors' information systems that process, store or transmit Federal contract information where the sensitivity/impact level of the Federal contract information being protected does not warrant a level of protection necessitating training, penetration or vulnerability testing, evolution, and reporting, detecting, reporting and responding to security incidents, encryption at rest, or cybersecurity insurance. Such standards would be needed if contract performance involved the contractor accessing CUI or classified Federal information systems.[30]

The Councils' response is telling in that it explains that it is the first step in a series designed to protect the information system and that more controls are required if the contractor's performance requires the contractor to access CUI or classified information. For DOD contractors, the DFARS clauses represent the second step. Looking forward, the DFARS security controls will likely need to apply to all federal contractors in order to combat cyber threats. Oddly, there is currently no specific FAR clause that addresses the security controls required for contractors accessing, creating, or handling CUI.

The DFARS Contract Requirements

Compliance with DFARS contract requirements is a salient and often-challenging issue. A July 2019 audit by DOD's Inspector General (IG) concluded that "DOD contractors did not consistently implement DOD-mandated system security controls for safeguarding Defense information."[31] DOD IG cited examples such as failure to use multifactor authentication or strong passwords, protect sensitive data on removable media such as flash drives, oversee network protection services provided by third-party vendors, implement physical security controls, or grant access based on the user's assigned duties.[32] Given that contractors submit applications for payment that certify that they are compliant with the terms of the contract, failure to comply could turn every pay application into a civil False Claim. Therefore, it is important to be vigilant about implementing each requirement.

Two DFARS contract clauses regulate network security for all DOD contractors that have federal contract information residing in or flowing through their IT systems. DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) gives contractors guidance on cybersecurity requirements, and DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) is the accompanying notice provision, notifying contractors that they must comply with DFARS 252.204-7012 or offer any written explanation of how the contractor has taken measures to achieve an equivalent level of protection.[33]

DFARS 252.204-7012 has gone through quite a few revisions since it was first published as a final rule. That evolution itself has been a huge source of confusion in the industry. The rule began as an ANPR in 2010; it progressed to a proposed rule in 2011, and was issued as a final rule in November 2013.[34] Throughout that process, the biggest difference that emerged is that the current clause requires compliance with NIST Special Publication (SP) 800-171 and the earlier versions instead required compliance with a subset of the security controls identified in NIST SP 800-53 (i.e., the NIST manual applicable to federal agencies).[35] The explanation for their change is simple. The first edition of NIST Special Publication (SP) 800-171 was first published in June 2015 and therefore did not exist when DFARS 252.204-7012 first became a rule.[36] The two contract clauses are not retroactive and do not apply to any contract entered into before 2016.[37]

It is important for both prime contractors and subcontractors to be aware of these requirements because DFARS 252.204-7012 has a mandatory flow-down provision that applies to all subcontracts.[38] And both DFARS clauses require that the contractor comply with NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) Revision 1 (as of December 2016).

A third DFARS clause, DFARS 252.204-7010 (Cloud Computing Services) is, as its title suggests, "applicable when using cloud computing to provide information technology services in the performance of the contract."[39] This clause requires the contractor to (1) maintain all government data not located on DOD premises within the U.S. government unless permission

is granted by the contracting officer; (2) implement administrative, technical, and physical safeguards and controls with the security level and services required in accordance with DOD's Cloud Computing Security Requirements Guide (SRG), which includes ensuring that the contractor's cloud service provider has gone through DOD's standardized assessment and authorization (certification) process; and (3) comply with a specific cyber incident reporting protocol and subsequent cyber incident damage assessment activities.[40]

The Cybersecurity Maturity Model Certification (CMMC)

In September 2019, shortly after the July DOD IG report finding inconsistent and poor contractor cybersecurity compliance, DOD's Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) released its first public, unclassified version of the Cybersecurity Maturity Model Certification (CMMC).[41] According to DOD, "[t]he CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks."[42] In essence, because the Office of the Inspector General (OIG) found that contractors were in compliance with NIST SP 800-171, DOD developed a means for contractors to prove that they are compliant on the front end of a procurement, rather than through post-award compliance audits. As soon as June 2020, sections L and M of DOD requests for proposals will identify a specific "maturity level" that contractors will need to meet. The CMMC accreditation body (CMMCAB) will verify that contractors have met the requisite level. The levels will range from "Basic Cybersecurity Hygiene" to "Advanced" and require contractors to obtain a certification from an accredited third-party vendor to prove that their information systems meet the required level of safeguarding.[43]

The CMMC was created through federal grants in conjunction with Carnegie Mellon University and the Johns Hopkins University Applied Physics Laboratory, LLC (APL).[44] Its stated purpose is to "enhance the protection of sensitive data—namely, Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), within the supply chain."[45] The introduction goes on to cite the economic impact of cyber theft as follows:

> The theft of hundreds of billions of dollars of intellectual property and sensitive information from all industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 [1]. The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017 [2].[46]

The Introduction in Version 0.7 placed the blame squarely on the failure to develop adequate defenses to cyber-attacks and contractors' failure to implement the controls. "The majority of this IP theft is directly attributable to poor cybersecurity maturity and ineffective implementation of controls necessary to protect sensitive data."[47]

The CMMC combines security standards found in FAR 52.204-21, DFARS 252.204-7012, NIST SP 800-171 Revision 1, NIST 800-171B, NIST SP 800-53, ISO 27001 (Information Technology—Security techniques—Information security management systems—Requirements), ISO 27003 (Information Technology—Security techniques—Information security management systems—Guidance), and Aerospace Industrial Association National Aerospace Standards 9933 (Critical Security Controls for Effective Capability in Cyber Defense).[48] The purpose is to create a single "unified standard for cybersecurity" and "measure the maturity of a company's institutionalization of cybersecurity practices and processes."[49] Once the CMMC is implemented, the DFARS contract safeguarding requirements provisions will likely be amended to require some level of CMMC certification.

Navigating DFARS 252.204-7012

Between the two DFARS contract clauses, their incorporation of the latest revision of NIST 800-171, and the more recent CMMC certification requirement, navigating DFARS 252.204-7012 may seem difficult, or at least highly technical. However, contractors can effectively and accurately implement DFARS 252.204-7012 into their systems by following three steps. First, identify the information covered under the DFARS. Second, integrate the cyber incident reporting requirements into your FAR 52.203-13–required code of business ethics and compliance. Third, develop and document a System Security Plan and Plans of Action, as necessary. The following sections explain each of these steps.

Step 1: What Information Is Covered?

The first step in accurately complying with DFARS 252.204-7012 is to identify its scope. The clause applies to "all *covered contractor information systems*" that hold "*covered defense information*."[50] A covered contractor information system is an unclassified information system that is owned or operated by or for a contractor and processes, stores, or transmits covered defense information.[51] The clause does not cover information that is lawfully publicly available without restrictions.[52]

Covered Defense Information

This section explains how to identify covered defense information (CDI). After identifying which systems are covered, contractors must identify what information qualifies as CDI. DFARS 252.204-7012 defines CDI as one of two things: (1) "unclassified controlled technical information" (CTI) "or (2) other information, as described in the Controlled Unclassified Information (CUI) Registry

. . . that requires safeguarding or dissemination controls."[53] In addition, the information (whether CTI or CUI) must (1) be "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) be "[c]ollected, developed, received, transmitted, used, stored by or on behalf of the contractor in support of performance of the contract."[54] In order to determine whether information should be classified as CDI, you must (1) identify any CTI or CUI, (2) determine if the information requires safeguarding or dissemination controls, and (3) identify information that is marked as CDI and information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract. The first category of CDI—marked or otherwise identified—is easy to identify because the burden is on DOD to tell the contractor that the material is CDI. The second category—collected, developed, or stored—is murkier and hence carries more risk because it is up to the contractor to exercise its discretion in identifying the information that requires safeguarding.

• Unclassified Controlled Technical Information (CTI)
While the government contracting community works hard to overuse acronyms and create confusion with homonyms, this article will unpack CDI and attempt to make it easier for contractors to apply. CDI consists of either CTI or CUI. The DFARS defines CTI as:

> Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. . . . The term does not include information that is lawfully publicly available without restrictions.[55]

Technical information as used in the definition means technical data or computer software as those terms are defined in DFARS 252.227-7013 (Rights to technical data—Noncommercial items).[56] CTI's complicated definition can be simplified into three parts: (1) technical information that (2) has military/space application and (3) is subject to some form of controls.[57] Examples of such data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.[58]

• Controlled Unclassified Information (CUI)
Turning to controlled unclassified information, or CUI, 32 C.F.R. § 2002.4(h) defines CUI as any information that "a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls," but it does not include information that is formally classified as Confidential, Secret, Top Secret, or Sensitive Compartmentalized Information.[59] It can include information marked as For Official Use Only (FOUO) or information identified by the Department of Energy as Unclassified Controlled Nuclear Information (UCNI). References to CUI go beyond DOD and extend to cybersecurity regulations for other agencies as well. This is why the FAR references CUI, rather than the specific scope found in the DFARS. The easiest way to identify exactly what constitutes controlled unclassified information is to reference the online CUI registry.[60] The CUI registry applies to all agencies and indicates what information is controlled or sensitive.[61]

One particularly common CUI category to watch out for is "export controlled."[62] This category applies to all information marked or identified in the contract as CDI *or* that is collected, developed, etc. on behalf of the contractor in support of performance on the contract.[63] Information is considered CUI if its "export could reasonably be expected to adversely affect the United States' national security and nonproliferation objectives."[64] It may be difficult to determine what does and does not constitute CUI, especially for contractors who generate business from sources other than DOD. Although only covered contractor information systems are subject to these regulations, businesses may find themselves in the position of needing to create security plans on all of their systems if the covered contractor information systems are not separated. DOD regulations only require contractors to protect federal information systems. Therefore, if the federal systems are separated from commercial ones, contractors can save themselves time and money by implementing the required information systems safeguards on fewer systems and information. Therefore, we recommend putting CDI on a separate internal network. This may be difficult in situations where contractors have numerous offices in which they conduct both commercial and federal business because the requirements will only apply to federal systems. However, ultimately, it will be necessary and can potentially save time and money in the long run because it will mean that contractors can focus on creating a security system plan for CDI alone, without overextending their resources to cover other information that is not regulated.

Is It CTI or CUI?
To complicate matters, the CUI Registry lists CTI as a category of CUI. In other words, CTI is also CUI. DOD has done very little by way of describing how CDI differs from CUI or why the definition of CDI separates CTI from CUI. In many ways, the differences may be negligible. The differing definitions may simply come from DOD's unilateral attempt to regulate information security independently from other agencies. The only language that appears in CDI's definition that distinguishes it from CUI is that CDI can be "collected, developed, received, transmitted, used, stored, etc. by the contractor." Generally, CUI must also be marked as such. However, by adding this second clause, DOD expanded CDI

to cover information not only marked as CUI, but also collected, developed, received, transmitted, used, stored, etc. by the contractor in relation to the contract. As discussed below, the CMMC, covering only DOD contractors, applies only to CUI, meaning the difference between CDI and CUI may be trivial.[65]

The question is not whether a DOD contractor has CDI, but whether the information it possesses constitutes CDI. Virtually anyone doing DOD contracting will have CDI. In practice, DOD contractors should keep track of all the information provided to them by DOD as well as information developed in connection with a DOD contract and determine if it fits into one of the CUI registry categories, including controlled technical information.[66] Different types of contractors are likely to have most of their information fall into different categories. For example, construction contractors should put their focus on the "Critical Infrastructure" categories, which are Ammonium Nitrate, Chemical-terrorism Vulnerability Information, Critical Energy Infrastructure Information, Emergency Management, General Critical Infrastructure Information, Information Systems Vulnerability Information, Physical Security, Protected Critical Infrastructure Information, SAFETY Act Information, Toxic Substances, and Water Assessments.[67] On the other hand, an IT contractor may want to be most aware of the Privacy Information and Sensitive Personally Identifiable Information categories.[68]

Other CDI Requirements

If you have determined that the information is CUI (as opposed to CTI), you must then determine whether the information is controlled. CDI is information that "requires safeguarding or dissemination controls." DoD expanded on this by saying that CDI is information "that requires safeguarding or dissemination controls *pursuant to and consistent with law, regulations, and Government wide policies*."[69] Essentially, any information that is regulated or controlled meets this part of the definition.

Finally, you must identify whether the information is either (1) marked or otherwise identified or (2) collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract. Identifying CDI that is marked is rather simple. In this case, DOD is simply telling a contractor when information is CDI. The second category is what causes confusion for many contractors. This second category "recogniz[es] the shared obligation of the contractor to recognize and protect covered defense information that the contractor is developing during contract performance."[70] This second category puts contractors on alert that they may hold or develop CDI throughout the course of contract performance, even if the CDI was not originally either given to them or marked by DOD as CDI.

Step 2: What Are the Cyber Incident Reporting Requirements

Once you determine what information is covered, it is important to put a system in place to report cyber incidents to DOD. DFARS 252.204-7012 defines a "cyber incident" as "actions taken through the use of computer networks that result in a compromise or an actual or potential adverse effect on an information system and/or the information residing therein."[71] For example, discovering malware on your system or discovering that information has been "exfiltrated" or taken from your system are both reportable cyber incidents.[72]

Establishing a system for compliance with reporting requirements should be a priority because DOD requires that contractors "rapidly report" cyber incidents, meaning "within 72 hours of discovery of any cyber incident."[73] The 72-hour reporting requirement is one of the most troubling parts of the regulation for contractors because it is much faster than the disclosures required under FAR 52.203-13 (Contractor Code of Business Ethics and Compliance), which permit time to conduct an internal investigation, which in turn can take weeks. FAR 52.203-13 requires timely disclosure of evidence of a violation of the civil False Claims Act or Title 18 of the U.S. Code but does not require a specific time period, implying that a reasonable time to investigate is allowed.[74] Under the DFARS clause, by contrast, contractors are required to report "whatever information is available" within the 72-hour period, but also "should submit a follow-on report when additional information becomes available."[75] Although the initial time period for disclosure is starkly different from that of FAR 52.203-13, as we have discussed, both clauses contain a continuing obligation to disclose.

It is difficult to meet the tight deadline without, first, a comprehensive understanding of what systems/information you have that are covered under the clause, and, second, having a system already in place to quickly identify cyber incidents and respond in compliance with DFARS 252.204-7012. DOD takes the timely reporting of incidents very seriously. In its answers to comments, DOD stated that timely reporting is "a key element" in protecting DOD's information and "provides the clearest understanding" of what cyber information is being targeted.[76]

To summarize, your cyber incident reporting system should consist of three steps. First, it should establish a system for reviewing compromised CDI. Second, it should trigger reporting to DOD within 72 hours of an incident.[77] Third, it should ensure that all information is preserved and protected for 90 days following the incident.[78] DOD may require access to this information and, in some cases, may even require physical access to your technical systems.[79]

Step 3: Develop a System Security Plan and a Plan of Action

Next, the DFARS clauses require you to ensure that your technical systems are secure enough to withstand cyberattacks.[80] To accomplish this, contractors are required to develop a System Security Plan (SSP) and encouraged to develop Plans of Action (POAs) to help implement the

SSP.[81] Until CMMC is required, SSPs and POAs are perhaps the most important evidence a contractor can produce in an investigation to prove that it has thoughtfully considered and taken steps to implement its safeguarding requirements. Their importance cannot be overstated, as mitigation efforts are essential in negotiating down potential suspensions and debarments and the severity of any penalty for a potential civil False Claims Act violation.

An SSP requires the contractor to develop and regularly update a plan that will describe its system, how it operates, its relationship with other systems, and its security controls.[82] The goal of an SSP is "to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements."[83] Developing an accurate and detailed SSP is important because it will allow DOD to assess the overall risk of hosting CDI on your system.[84] DFARS clause 252.204-7012 requires contractors to implement NIST 800-171 standards into their system security plan and to comply with its guidelines.[85] Neither the DFARS clause nor NIST requires an SSP to take on any particular format, but NIST provides a helpful template in NIST 800-18 Revision 1 Chapter 3.[86] Your SSP must describe how the NIST security requirements are to be met.[87] DFARS clause 252.204-7012 makes it a requirement for contractors to comply with the guidelines in NIST 800-171. NIST 800-18 Revision 1 provides cybersecurity requirements that the federal government must follow.[88] Although contractors are not bound by NIST 800-18 Revision 1, it can be helpful in informing contractors on how to adequately create an SSP.[89]

The question that plagues many contractors is how to implement over 100 pages of NIST SP 800-171's highly technical language into their SSP. First, start with NIST 800-171 Chapter 3. Chapter 3 lays out the requirements of each part of the SSP. It contains eight pages of guidance and is easy to follow. Many contractors get bogged down with the highly technical language and mapping requirements set forth in Appendix D. However, Appendix D is intended to be a tool to help contractors navigate the requirements listed in Chapter 3. Therefore, contractors should focus first on Chapter 3 and then turn to Appendix D if they need clarification.

In June 2019, NIST published a draft of NIST 800-171 Revision 2. NIST has made it clear that "there are no changes to the basic and derived security requirements in Chapter Three."[90] When the final Revision 2 hits, the steps for compliance will likely be the same. For manufacturers, NIST has also developed the NIST MEP (Manufacturing Extension Partnership) program to help small and medium-size manufacturing businesses comply with cybersecurity requirements and has provided a guide for manufacturers to help them assess their SSP.[91]

Although not expressly required, NIST strongly recommends using a plan of action (POA) to enable ongoing real-time updates to your SSP and help you work towards implementing all NIST requirements.[92] NIST describes a POA as a "key document" to "describe how any unimplemented security requirements will be met."[93] A POA may be its own separate document or may be combined with an SSP. A POA "identifies tasks needing to be accomplished" in order to reach certain milestones on your way to NIST compliance.[94] POAs also serve to "correct deficiencies and reduce or eliminate vulnerabilities" in a contractor's technical system.[95] Further, SSPs require periodic review and modification to ensure they are up to date.[96] Having a POA will help you make sure your SSP is up to date. Keeping up with your SSP and POA is also good practice because those are the tools by which DOD will measure your compliance, particularly in the event that a cyber-incident occurs. Outdated or vague documents could potentially be problematic.

Understanding the CMMC, Version 1.0, Requirements

The DOD Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)) released CMMC Version 1.0 on January 30, 2020.[97] Version 1.0 represents years of work to address the fact that DOD's "supply chain currently consists of about 300,000 companies and about 290,000 of those have no cybersecurity requirements whatsoever."[98] The CMMC "framework consists of five maturity processes and 171 cybersecurity best practices progressing across five maturity levels."[99] While the terms, processes, practices, and maturity levels can be confusing, the CMMC essentially consists of steps contractors can take to protect against the risk of cyber-attacks beginning "with basic safeguarding at Level 1, moving to the broad protection of Controlled Unclassified Information (CUI) at Level 3."[100] DOD anticipates that the framework will continue to be updated to address evolving threats such as the potential of quantum computing to decode encrypted digital information.[101]

The Five Maturity Levels

The CMMC model has five ascending levels of cybersecurity practices (i.e., five levels of certification):

- Level 5—Advanced/Progressive
- Level 4—Proactive
- Level 3—Good Cyber Hygiene
- Level 2—Intermediate Cyber Hygiene
- Level 1—Basic Cyber Hygiene[102]

In simple terms, federal contractors with federal, but no DOD, contracts must comply with FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).[103] Level 1 CMMC certification (Basic Cyber Hygiene) is geared towards FAR 52.204-21, and contractors that receive a Level 1 will be well on the road towards satisfying their FAR cybersecurity contract requirements. By contrast, Level 3 certification (Good Cyber Hygiene) is based upon NIST 800-171 Revision 1 and 800-171B, meaning that contractors that receive a Level

3 certification will meet the technical requirements set forth in DFARS 252.204-7012.[104] Currently, all contractors, including small business subcontractors, will need to be Level 3 certified to be awarded a DOD contract. However, a revised DFARS 252.204-7012 is scheduled to come out in the spring and will likely allow DOD small business subcontractors to be Level 1 certified so long as they do not possess any CUI because, as Katie Arrington stated, "cybersecurity is not one size fits all."[105] While DOD talks about exceptions for small business concerns, the reality will likely be quite different. A prime contractor on an unrestricted procurement with a Level 3 or 4 requirement is not likely to accept that the small business subcontractor is not certified at the same level.

The CMMC notes that the DFARS requirements do not end with Level 3 certification. DOD contractors must still separately meet the System Security Plan (SSP) and the rapid reporting requirements.[106] Eventually, Requests for Proposals (RFPs) will identify which level is required for each contract.[107] The requisite CMMC level will be in sections L and M and used as a "go/no go decision."[108]

Version 1.0 states that "Level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats."[109] The definition of Level 3 from the Version 0.7 definition is more detailed and hence insightful:

> An organization assessed at CMMC Level 3 will have demonstrated good cyber hygiene and effective implementation of controls that meet the security requirements of NIST SP 800-171 Revision 1. Organizations that require access to CUI should achieve CMMC Level 3. CMMC Level 3 indicates a basic ability to protect and sustain an organization's assets and CUI; however, at CMMC Level 3, organizations will have challenges defending against advanced persistent threats (APTs). Note that organizations subject to DFARS clause 252.204-7012 will have to meet additional requirements such as incident reporting.[110]

Unpacking CMMC levels

As we've mentioned earlier, CMMC has five levels. However, each of these levels is composed of numerous requirements. In this section, we will unpack how following the requirements in each CMMC Level works. The five CMMC levels collectively contain 17 Security Domains. Version 1 simply takes the 14 "families of security requirements" or the broad list of security control categories from Chapter 3 (The Requirements) of NIST 800-171 Revision 1 and adds three more: "Asset Management," "Recovery," and "Situational Awareness."[111] Each level of certification requires contractors to comply with a unique number of Security Domains. Additionally, there are 171 Best Practices nested within the 17 Security Domains. For each ascending level of certification, the contractor must demonstrate its ability to satisfy a greater number of Best Practices. For example, in order to obtain a Level 1 certification under the domain "Access Control," a contractor must adhere to the following Best Practices:

1. limit information system access to authorized users,
2. limit access to the types of transactions and functions that authorized users are permitted to execute,
3. verify and control/limit connections to and use of external information systems, and
4. control information posted or processed on publicly accessible information systems.[112]

By contrast, in order to meet the higher Level 3 requirements, a contractor must follow such additional cybersecurity Best Practices as:

5. separate the duties of individuals to reduce the risk of malevolent activity without collusion,
6. prevent nonprivileged users from executing privileged functions and capture the execution of such functions to audit logs,
7. terminate (automatically) user sessions after a defined condition,
8. protect wireless access using authentication and encryption, and
9. encrypt CUI on mobile devices and mobile computing platforms.[113]

Ultimately, a Level 1 certification requires the contractor to satisfy 17 cybersecurity Best Practices, whereas a Level 3 requires the contractor to satisfy 58 Best Practices.[114]

Appendices A and B of CMMC 1.0 contain the model in table format by level with references and discussions, clarifications, and examples of each of the requirements for each certification level. Appendices are helpful to determine specific requirements.[115] For example, among the Level 3 Asset Management security controls is the requirement that the contractor "define procedures for handling of CUI data."[116] Appendix D clarifies that the procedures should include how to receive, transmit, store, and destroy CUI information."[117]

Like NIST SP 800-171, the appendices in CMMC are only helpful to supplement the body of the CMMC, which describes the levels. However, the appendices are not intended to serve as specific guidelines on complying with each level.

Who Pays for Certification?

Without question, the cost to obtain CMMC Level 3 or higher certification will be significant, and it is unclear whether or to what extent contractors will be able to seek reimbursement for those costs. According to the DOD Office of the Under Secretary of Defense for Acquisition & Sustainment's CMMC website, "[t]he cost of certification will be considered an allowable,

reimbursable cost and will not be prohibitive."[118] Whether that refers to just the cost of the third-party certification or the work required to get to a Level 3 certification is unclear. DOD's Chief Information Security Officer, Katie Arrington, has also stated publicly that "security is an allowable cost."[119]

Further guidance may be found by looking further back. In 2013, when DFARS 252.204-7012 was first issued as a final rule, the FAR Councils stated in response to the question of whether "the cost associated with compliance to the DFARS changes is allowable under CAS" that "[t]here is nothing in FAR 31 or DFARS 231 that would make the costs of compliance unallowable if the costs are incurred in accordance with FAR 31.201-2 [Determining Allowability]."[120] The take-away is that, if compliance is allowable, allocable, and reasonable under FAR Part 31, it may be reimbursable. The FAR Councils further explained in response to another question that "[i]n many cases, this contract requirement will be spread across and benefiting multiple contracts—costs associated with implementation will be allowable and chargeable to indirect cost pools. The Government does not intend to directly pay for the operating costs associated with the rule."[121] In plain speak, until there is a more clear answer from DOD, contractors will likely have to bear the full brunt of the cost of compliance and then build the cost into their proposals over time as overhead and hope that the increased price does not make their proposal uncompetitive.

Cloud Computing Services: CMMC vs. FedRAMP

One unanswered question is whether cloud computing services (covered under DFARS 252.239-7009 and 252.204-7010) will be addressed in future versions of the CMMC. Version 1.0 of the CMMC only vaguely addresses cloud computing services. An appendix explaining level 1 certification states that level 1 certification addressed cloud computing service, but it does not lay out specific security requirements for cloud computing services.[122]

The CMMC may never fully address cloud computing services, however, because DOD addresses them separately in the Department of Defense Cloud Computing Security Requirements Guide (SRG), which is developed by the Defense Information Systems Agency, Department of Defense.[123] The SRG requires contractors to be certified under FedRAMP.[124] FedRAMP is a cloud services security certification program administered by GSA and applies to all federal contractors. Additionally, SRG points DOD contractors to DoD FedRAMP+, which imposes supplemental security requirements in addition to FedRAMP requirements.[125] DOD classifies information systems into four different levels based on the level of sensitive information they contain.[126] Contractors will have to comply with the appropriate FedRAMP and DoD FedRAMP+ level based on those requirements.[127]

Potential Consequences of Noncompliance

Failure to comply with these regulations can lead to serious consequences, including False Claims Act liability.[128] For example, in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, the Eastern District of California refused to dismiss a qui tam case where an employee of Aerojet Rocketdyne Holdings claimed that his employer repeatedly made false cybersecurity certifications to the government.[129] We anticipate that courts will continue to find civil False Claims Act violations for not complying with cybersecurity requirements. Additionally, contractors face potential suspension and debarment for not complying with DFARS regulations.

Conclusion

The January release of CMMC Version 1 demonstrates DOD's long-standing efforts to ensure its contractors have implemented effective information systems safeguarding measures. As cybersecurity issues become more and more prevalent, DOD has made it clear it will require more safeguarding measures from its contractors and will strictly enforce those requirements. While the requirements may seem daunting and complicated at first, this guide seeks to break down DOD's regulatory framework into easy-to-follow steps.

Ultimately, a contractor's compliance with the regulations will be based upon CMMC. While NIST SP 800-171 and DFARS 252.204-7012 create the basis for information system security regulations, CMMC gives a more comprehensive set of requirements that encompasses the full set of requirements found in both the DFARS and NIST. Not only must contractors comply with all of these regulatory frameworks, but if they wish to stay competitive in today's market, contractors will need to take cybersecurity seriously or risk getting left in the dust. Your attorney can help you conduct due diligence to make sure you are compliant with these regulations. This will help ensure you are up to date on cybersecurity regulations. It is important to make sure these new cybersecurity regulations are implemented into your code of business ethics and conduct.[130] Further, if an issue or cyber threat arises, the system will allow you to inform the office of the Inspector General and the contracting officer of any credible evidence of a cyber-threat or regulatory violation. Additionally, your attorney can assist you in achieving the appropriate level of CMMC compliance so that CMMCAB will find you to be certified at that level. Although navigating the evolving cybersecurity regulations may seem complicated, this article is intended to make the daunting world of cybersecurity understandable and to give practical guidance on how to ensure your information systems are compliant. PL

Endnotes

1. DFARS 252.204-7012(a); Cyber Incident Reporting and Cloud Computing, 84 Fed. Reg. 36,905 (July 30, 2019).

2. Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002) (formerly 44 U.S.C. §§ 3531–3549 prior to repeal).

3. Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69,273, 69,277 (Nov. 18, 2013).

4. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014); 44 U.S.C. §§ 3551–3559.

5. Exec. Order No. 13556, 3 C.F.R. § 13556 (Nov. 4, 2010).

6. *See generally* 32 C.F.R. § 2002 (2016).

7. Exec. Order No. 13556.

8. Nat'l Inst. of Standards & Tech., NIST SP 800-53, Information Security (2005).

9. Safeguarding Unclassified Information, 75 Fed. Reg. 9,563 (Mar. 3, 2010); Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089, 38,090 (June 29, 2011) ("This rule addresses the safeguarding requirements specified in Executive Order 13556, Controlled Unclassified Information.").

10. *About NIST*, Nat'l Inst. of Standards & Tech., https://www.nist.gov/about-nist (last visited Dec. 30, 2019).

11. Nat'l Inst. of Standards and Tech., NIST SP 800-171 Rev. 1, ch. 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (2016) [hereinafter NIST SP 800-171 Rev. 1].

12. John Perry, *The Story of Standards*, *in* Funk & Wagnalls 123 (1953) (Library of Congress Cat. No. 55-11094).

13. Nat'l Inst. of Standards & Tech., NIST SP 800-18, Information Security (1998) [hereinafter NIST SP 800-18].

14. Nat'l Inst. of Standards & Tech., NIST SP 800-18 Rev. 1, Information Security (2005) [hereinafter NIST SP 800-18 Rev. 1].

15. Nat'l Inst. of Standards & Tech., NIST SP 800-53, Information Security (2005).

16. Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69,273, 69,280 (Nov. 13, 2013).

17. NIST SP 800-171 Rev. 1, *supra* note 11.

18. Nat'l Inst. of Standards & Tech., NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (2015) [hereinafter NIST SP 800-171].

19. NIST SP 800-171 Rev. 1, *supra* note 11.

20. Nat'l Inst. of Standards & Tech., NIST 800-171 Rev. 2 DRAFT, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (2019) [hereinafter NIST SP 800-171 Rev. 2 DRAFT].

21. Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30,439 (May 16, 2016).

22. Basic Safeguarding of Contractor Information Systems, 77 Fed. Reg. 51,496 (Aug. 24, 2012).

23. 81 Fed. Reg. at 30,444.

24. *Id.* at 30,440.

25. NIST SP 800-171 Rev. 1, *supra* note 11, ch. 1.

26. 81 Fed. Reg. at 30,440.

27. *Id.* at 30,439.

28. *Id.*

29. The Civilian Agency Acquisition Council and the Defense Acquisition Regulation Council.

30. 81 Fed. Reg. at 30,439.

31. Inspector Gen., Dep't of Def., Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, Rep. No. DODIG-2019-105, at i (July 23, 2019).

32. *Id.* at i–ii.

33. Cyber Incident Reporting and Cloud Computing, 84 Fed. Reg. 23,532 (July 22, 2019).

34. Safeguarding Unclassified Information, 75 Fed. Reg. 9,563 (Mar. 3, 2010); Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089 (June 29, 2011); Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69,273 (Nov. 18, 2013).

35. *Compare* 78 Fed. Reg. 69,273, *with* Network Penetration Reporting and Contracting for Cloud Services, 80 Fed. Reg. 51,739, 51,746 (Aug. 26, 2015).

36. NIST SP 800-171 Rev. 1, *supra* note 11.

37. *Cybersecurity FAQs*, Dep't of Def. Procurement Toolbox, https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity-faqs (last visited Dec. 24, 2019).

38. *Id.*

39. DFARS 252.204-7010 (codified at 80 Fed. Reg. 51,747 (Aug. 26, 2015)), *as amended by* Technical Amendments, 80 Fed. Reg. 74,695 (Nov. 20, 2015).

40. DFARS 252.204-7010(b), (d), (h); *see also DoD Cloud Computing Security*, DoD Cyber Exchange Pub., https://public.cyber.mil/dccs/ (last visited Jan. 29, 2020).

41. Carnegie Mellon Univ. & Johns Hopkins Univ. Applied Physics Lab. LLC, Cybersecurity Maturity Model Certification (CMMC) Draft Version 0.4 (2019) [hereinafter CMMC Version 0.4].

42. *CMMC FAQ's*, Office of Under Sec'y of Def. for Acquisition & Sustainment, Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/faq.html (last visited Jan. 20, 2020) (FAQ No. 5).

43. *Id.* at FAQ Nos. 4 & 10.

44. Carnegie Mellon Univ. & Johns Hopkins Univ. Applied Physics Lab. LLC, Cybersecurity Maturity Model Certification (CMMC) Draft Version 0.7 (2019) [hereinafter CMMC Version 0.7].

45. *Id.* at 1.

46. Carnegie Mellon Univ. & Johns Hopkins Univ. Applied Physics Lab. LLC, Cybersecurity Maturity Model Certification (CMMC) Version 1.0 (2020) [hereinafter CMMC Version 1.0] (citing Council of Econ, Advisors, The Cost of Malicious Cyber Activity to the U.S. Economy (2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; Ctr. for Strategic & Int'l Studies (CSIS) & McAfee, Economic Impact of Cybercrime—No Slowing Down (2018) (emphasis added)).

47. CMMC Version 0.7, *supra* note 44, at 1.

48. *Id.* at 1.

49. *CMMC FAQ's*, *supra* note 42, at FAQ No. 8.

50. DFARS 252.204-7008(b) (codified at 81 Fed. Reg. 72,986 (Oct. 21, 2016)); DFARS 252.204-7012(b) (codified at 81 Fed. Reg. 72,986 (Oct. 21, 2016)).

51. DFARS 252.204-7012(a) (codified at 81 Fed. Reg. 72,986).

52. DFARS 204.73.

53. DFARS 252.204-7012(a) (codified at 81 Fed. Reg. 72,986).

54. *Id.*

55. *Id.*

56. 32 C.F.R. § 236.2.

57. DFARS 204.7301.

58. Susan B. Cassidy, Melinda Lewis & Weiss Nusraty, *DoD Announces the Cybersecurity Maturity Model Certification (CMMC) Initiative* National Archives, Inside Gov't Contracts (July 16, 2019), https://www.insidegovernmentcontracts.com/2019/07/dod-announces-the-cybersecurity-maturity-model-certification-cmmc-initiative/.

59. 32 C.F.R. § 2002.4(h).

60. *See CUI Registry: CUI Glossary*, Nat'l Archives, https://www.archives.gov/cui/registry/cui-glossary.html (last visited Dec. 30, 2019).

61. *CUI Registry*, Nat'l Archives, https://www.archives.gov/cui (last visited Jan. 6, 2020).

62. *CUI Category: Export Controlled*, Nat'l Archives, https://www.archives.gov/cui/registry/category-detail/export-control.html (last visited Dec. 20, 2019).

63. *Id.*
64. *Id.*
65. CMMC Version 0.7, *supra* note 44, at app. D.
66. The definition of controlled technical information found in the CUI registry is identical to the one found in the DFARS.
67. *See CUI Categories*, Nat'l Archives, https://www.archives.gov/cui/registry/category-list (last visited Jan. 6, 2020).
68. *Id.*
69. Network Penetration Reporting and Contracting for Cloud Services, 81 Fed. Reg. 72,986 (Oct. 21, 2016) (emphasis added).
70. *Id.*
71. DFARS 252.204-7012(a)(2) (codified at 81 Fed. Reg. 72,986 (Oct. 21, 2016)).
72. *Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73*, Dep't of Def. Procurement Toolbox (Apr. 2, 2018), https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-11/POSTED%20Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018%20rev%201.pdf (last visited Dec. 24, 2019).
73. DFARS 252.204-7012(a) (codified at 81 Fed. Reg. 72,986).
74. FAR 52.2013-13(c)(ii)(F) (codified at 80 Fed. Reg. 38,293 (July 2, 2015)).
75. *Frequently Asked Questions*, *supra* note 72.
76. Cyber Incident Reporting and Cloud Computing, 84 Fed. Reg. 36,905 (July 30, 2019).
77. DFARS 252.204-7012.
78. *Cybersecurity*, Office of Small Bus. Programs (Dec. 20, 2018), https://business.defense.gov/Small-Business/Cybersecurity/.
79. 84 Fed. Reg. 36,905.
80. *See* DFARS 252.204-7012.
81. NIST SP 800-171 Rev. 1, *supra* note 11, ch. 3.
82. *Id.* ch. 3.21.4.
83. NIST SP 800-18 Rev. 1, *supra* note 14, ch. 1, at vii.
84. Memorandum from Office of Under Sec'y of Def., Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Sept. 21, 2017), https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.
85. Office of Under Sec'y of Def., Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (2018).
86. Memorandum from Office of Under Sec'y of Def., *supra* note 84.
87. NIST 800-171 Rev. 1, *supra* note 11, ch. 3.
88. *See* NIST 800-18 Rev. 1, *supra* note 14, at iii ("This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright.").
89. *See id.* ch. 3.
90. NIS TSP 800-171 Rev. 2 DRAFT, *supra* note 20.
91. *Cybersecurity Assessment Tool*, MEP Nat'l Network, https://www.surveymonkey.com/r/Z7RVFWV (last visited Dec. 30, 2019).
92. NIST 800-171 Rev. 1, *supra* note 11, ch. 3.12.2.
93. *Id.* app. F, at 99.
94. *Id.* app. B, at 36.
95. Dep't of Def., *Cybersecurity Challenges: Protecting DoD's Unclassified Information: Implementing DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting* (2018), https://www.nist.gov/system/files/documents/2018/10/18/cui18oct2018-104501145-dod_dfars-michetti-thomas.pdf.
96. NIST 800-18 Rev. 1, *supra* note 14, ch. 1, at vii.
97. CMMC Version 1.0, *supra* note 46.
98. Connie Lee, *Small Business Concerned About New Cybersecurity Certification*, Nat'l Def. (2020) (referencing DOD Chief Info. Sec. Officer Katie Arrington).
99. CMMC Version 1.0, *supra* note 46, at 23.
100. *Id.*
101. Lee, *supra* note 98 (referencing interview comments of DOD Chief Info. Sec. Officer Katie Arrington).
102. CMMC Version 1.0, *supra* note 46, at 3–4.
103. *Id.* at 5.
104. *Id.* at 6.
105. Interview with Katie Arrington, Special Assist. to Sec'y of Def. for Acquisition for Cyber, Arlington, VA (Jan. 31, 2020).
106. *Id.*
107. *Cybersecurity FAQs*, *supra* note 37.
108. *Id.*
109. CMMC Version 1.0, *supra* note 46, at 6.
110. CMMC Version 0.7, *supra* note 44, at 3.
111. CMMC Version 1.0, *supra* note 46, at 7.
112. *Id.* at A-3–A-6.
113. *Id.* at A-4–A-5.
114. *Id.* at 3.
115. *Id.* apps. A & B.
116. *Id.* app. B, at B-43.
117. *Id.* app. D.
118. CMMC *FAQ's*, *supra* note 42, Response to Question 19.
119. Daniel Wilson, *DOD Official Says Cyber Is an Allowable Contractor Cost*, Law360 (June 14, 2019).
120. Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69,273, 69,274 (Nov. 18, 2013).
121. *Id.* at 69,275.
122. CMMC Version 1, *supra* note 46.
123. DFARS 252.239-7010(b)(2) (stating that contractors "shall implement and maintain . . . services required in accordance with the Cloud Computing Security Requirements Guide").
124. Def. Info. Sys. Agency for Dep't of Def., Department of Defense Cloud Computing Security Requirements Guide (2017).
125. *Id.*
126. *Id.*
127. *Id.*
128. *See* FAR 52.203-13.
129. 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
130. *See* FAR 52.203-13 (requiring contractors to create a code of business ethics and conduct).