COVINGTON

DoD Issues Interim Rule Addressing New Requirements for Cyber Incidents and Cloud Computing Services

August 27, 2015

Government Contracts

Overview

On August 26, 2015, the Department of Defense (DoD) issued an interim rule that expands the obligations imposed on defense contractors and subcontractors to safeguard "covered defense information" and for reporting cyber incidents on unclassified information systems that contain such information. The interim rule revises the Defense Federal Acquisition Regulation Supplement (DFARS) to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 and section 1632 of the NDAA for FY 2015. In addition, the interim rule implements DoD policies and procedures for safeguarding data and reporting cyber incidents when contracting for cloud computing services.

Section 941, which applies to "cleared defense contractors," and Section 1632, which applies to contractors designated as "operationally critical," impose certain reporting requirements on federal contractors with regard to cyber incidents involving networks that contain DoD information. In addition to reporting a cyber incident, both Sections include requirements for contractors to permit DoD access to their systems to allow the Department to assess the incident. Similarly, both Sections contain provisions requiring DoD to provide "reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person." The interim rule expands these and other cybersecurity requirements to all DoD contractors and subcontractors, not just to the "cleared contractors" and "operationally critical contractors" referenced in the 2013 and 2015 NDAAs.

As to the cloud computing requirements, the interim rule states that it is implementing existing policies and procedures including a DoD Chief Information Officer (CIO) memorandum dated December 15, 2014 ("Updated Guidance on the Acquisition and Use of Commercial Cloud services") and the DoD Cloud Computing Security Requirements Guide from January 2015. Consistent with this guidance, the interim rule imposes security requirements and limitations on access and disclosure of government data and government-related data maintained by the contractor pursuant to a cloud computing services contract.

Now, almost three years after section 941 was passed, DoD has issued an interim rule – effectively immediately − that:

- Adds new definitions for "compromise," "cyber incident," and "media" to be used across the DFARS.

- Modifies DFARS 204.73 to expand safeguarding requirements beyond unclassified controlled technical information (UCTI) to those involving covered defense information, a broader category of information than UCTI. The interim rule also addresses requirements for reporting cyber incidents involving covered defense information, information systems that contain covered defense information, and any cyber incidents that may affect a contractor's ability to provide operationally critical support.
- Renames DFARS Clause 252.204-7012 to "Safeguarding Covered Defense Information and Cyber Incident Reporting," specifies new security controls, and expands the scope of the clause consistent with the changes to DFARS 204.73.
- Adds new clause DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," which allows contractors to explain how "alternative, but equally effective" security measures can be substituted for the ones specified in DFARS 252.204-7012.
- Adds new DFARS clause 252.204-7009, "Limitations on the Use and Disclosure of Third Party Contractor Reported Cyber Incident Information," which prohibits third party contractors who are assisting with assessments of cyber incidents from unauthorized release or disclosure.
- Adds new DFARS subpart 239.76, which addresses the acquisition of cloud computing services consistent with the DoD CIO memo dated December 15, 2014 ("Updated Guidance on the Acquisition and Use of Commercial Cloud services") and the DoD Cloud Computing Security Requirements Guide from January 2015.
- Adds new DFARS clause 252.239-7009, "Use of Cloud Computing," which requires offerors to state whether they "anticipate" using cloud computing services in the performance of a particular government contract.
- Adds new DFARS provision 252.239-7010, "Cloud Computing Services," which imposes security requirements and limitations on access and disclosure of government data and government-related data maintained by the contractor pursuant to a cloud computing services contract.

The Interim Rule Expands the Scope of DFARS 252.204-7012 and Imposes New Cyber Incident Reporting and Safeguarding Requirements

New DFARS Definitions

The interim rule adds definitions for "compromise," "cyber incident," and "media" to DFARS part 202. From a harmonization standpoint, this is a positive change, as any future DoD cybersecurity regulations likely will be based on the same definitions. The interim rule defines these terms as follows:

- Compromise: disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

- Cyber Incident: actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
- Media: physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

A key point is that a "compromise" not only includes actions with objectively verifiable consequences, but also actions that *may* have occurred. Similarly, the definition of "cyber incident" includes *potentially* adverse effects, not only confirmed adverse effects.

Modification and Expansion of DFARS 204.73 and DFARS Clause 252.204-7012

At their core, the intent of DFARS 204.73 and 252.204-7012 remain the same. They (i) establish a set of security requirements to be implemented when handling unclassified DoD information, (ii) impose a 72-hour reporting requirement upon discovery of a cyber incident, and (iii) require cooperation with any post-report investigations.

DFARS 252.204-7012, however, has been appreciably expanded beyond UCTI to encompass "covered defense information," which (1) includes any DoD information provided to the contractor or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of a government contract; and (2) falls into one of the following categories (defined below): (a) controlled technical information, (b) critical information, an/or (c) export control information.

- Controlled Technical Information: technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.[1]
- Critical Information: specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).[2]
- Export Control Information: unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably

[1] "Controlled Technical Information" is defined essentially the same as UCTI in the prior version of 252.204-7012. Note, however, that the interim rule does not impose an explicit marking requirement for this information.
[2] Note that the interim rule does not define "Operations Security" or the "Operations Security process," so it is unclear how items will be identified as "critical information." Although unclear, it may relate to OpSec Security Programs as described in DoD Directive No. 5205.02. That Directive defines OPSEC Indicators to include "[f]riendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information."

be expected to adversely affect the United States national security and nonproliferation objectives.

Contractors also must safeguard any "other information, marked or otherwise identified in the contract, that requires safeguarding dissemination controls pursuant to and consistent with law, regulation, and Governmentwide policies." The interim rule thus greatly increases the scope of information subject to safeguarding.

But, the type of information subject to safeguarding and the additional reporting obligations are not the interim rule's only material changes. Under the previous regime, contractors were only required to report cyber incidents affecting UCTI. The interim rule, on the other hand, requires contractors to report any cyber incidents affecting (i) covered defense information (a broader category of data than UCTI), (ii) contractor information systems that contain covered defense information, and/or (iii) information that affects the contractor's ability to provide operationally critical support. For example, under the interim rule, the reporting requirement would be triggered by a cyber incident that affects the contractor's information system housing covered defense information, even if the information itself was not affected.

The chart below provides a more detailed comparison of the November 2013 and the August 2015 versions of DFARS 252.204-7012 and highlights key differences between the two.

Requirement	252.204-7012 - Safeguarding Unclassified Controlled Technical Information (Nov 2013)	252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting (Aug 2015)	Key Differences
Applicability	Required in all DoD solicitations and contracts, including those for the acquisition of commercial items. The safeguarding requirements applied only if a contractor had UCTI resident on or transiting through its information systems.	Applies to DoD solicitations and contracts and subcontracts, including those for the acquisition of commercial items. The safeguarding requirements apply to "covered defense information" residing in or transiting through covered contractor information systems.	The interim rule applies to all contracts that include "covered defense information," not just UCTI, so the applicability is broader.
Scope	Applied to UCTI, which was defined 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 UCTI may have needed to originate from or have been delivered to DoD to be covered by DFARS 252.204-7012. UCTI was required to be marked by the DoD, bearing the legends B through F as prescribed under DoD Instruction 5230.24.	Applies to "covered defense information" (discussed above), which includes information provided to the contractor by or on behalf of DoD or "collected, developed, received, used or stored" in support of contract performance, which also falls within one of these four categories: (i) controlled technical information, (ii) critical information, (iii) export control information, as well as (iv) any additional information marked or otherwise identified in the contract that is subject to controls imposed by law, regulation, or government-wide policy.	The interim rule expands scope to include information well beyond UCTI and provides only narrow exceptions for information not marked, not identified in the contract and which does not fit in one of the four enumerated categories. The interim rule allows the government to avoid the marking requirement that had applied to UCTI. Critical information is not clearly defined.
Adequate Security	Required contractors to implement a security program that, at a minimum, met 51 specified security controls from NIST SP 800-53. Contractors who did not implement all 51 controls were required to provide the CO with a written explanation that either explained why such controls were not	For systems operated on behalf of the USG: • Computing cloud services are subject to the requirements in clause 252.239.7010 (discussed below); and • IT services other than cloud	The interim rule divides covered information systems into two categories: (1) systems part of an IT service or system operated on behalf of the USG, and (2) internal contractor systems. Changes security control requirements from NIST SP 800-53 to NIST SP 800-171. Requires the DoD CIO to approve any

	required or specified alternative controls or protective measures that achieved the same level of protection. Contractors also were required to implement any other security measures that they reasonably determined were necessary to provide "adequate security" for UCTI resident on or transiting through its unclassified information systems.	computing are subject to "security requirements specified elsewhere in [the contract]." For systems not operated on behalf of the USG, contractors must implement: • The security requirements in NIST SP 800-171; or • "Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement" approved in writing by the DoD CIO. The contractor is also required to apply other security measures it deems necessary.	alternative security controls prior to contract award.
Cyber Incident Reporting	A reportable incident was defined as one that affects UCTI resident on or transiting through the contractor's unclassified information systems. A reporting obligation was triggered upon discovery of a reportable cyber incident, and contractors had 72 hours to report via http://dibnet.dod.mil. The report was required to include 13 enumerated pieces of information, such as contract numbers and a description of technical information compromised.	Must "rapidly report" a cyber incident to http://dibnet.dod.mil within 72 hours of discovery. A reportable cyber incident is one that "affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support." Upon discovery of such an incident, the contractor must:	Under the original regime, a reportable cyber incident was one that affected UCTI. The interim rule includes incidents affecting a contractor's information systems, as well as the contractor's ability to perform operationally critical contract requirements. In both cases, the key is that the incident has to "affect" (vice potentially affect) the system or information.

		• Conduct a review for evidence of compromise of covered defense information, including identifying compromised computers, servers, data, and user accounts. The review should include an analysis of the covered information system as well as any other information systems on the contractor's network that may have been compromised. • "Rapidly report" a cyber incident to http://dibnet.dod.mil within 72 hours of discovery.	
Post-incident Investigation	Following a report, a contractor was required to: • review its entire unclassified network for evidence of compromise resulting from the cyber incident, including identifying compromised computers, servers, specific data, and user accounts as well as analyzing any information systems on the network that were accessed as a result of the cyber incident; • review the accessed information to determine the specific UCTI documents, DoD programs, and DoD contracts compromised; and • preserve and protect images of the known affected unclassified	Contractors must preserve and protect images of all known affected information and systems for at least 90 days from reporting to allow DoD to determine whether it will conduct a damage assessment. Contractors must provide DoD access to additional information or equipment necessary to conduct a forensic analysis. Contractors must submit to DoD any malicious software connected to the incident that was discovered and isolated.	The original rule did not require the submission of malicious software to DoD. Under the previous rule, the contractor was required to collect specifically identified information and "comply with damage assessment information requests." The interim rule states that "[u]pon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct an forensic analysis." This is potentially a much broader scope of access. The interim rule also contains language that could be interpreted to give the Government the ability to use data provided by contractors for purposes other than the assessment of the incident.

	information systems impacting UCTI and all relevant monitoring/packet capture data for at least ninety (90) days to allow DoD the opportunity to review.		
Subcontractors	Contractors were required to flow down the substance of the clause in all subcontracts (including for commercial items). Subcontractors were required to report cyber incidents to higher tier contractors.	Contractors are required to flow down the substance of the clause in all subcontracts (including for commercial items). Contractors must require subcontractors to rapidly report cyber incidents directly to DoD via http://dibnet.dod.mil and to any higher tier contractor (including the prime).	Subcontractors were originally required to report directly to the higher tier contractor who would report up the chain until the report reached the prime contractor, who would then report to the DoD. The interim rule adds a direct report to DoD for all subcontractors in addition to any reporting to higher tier contractors.

New clause DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls"

The revised DFARS Clause 252.204-7012 also specifies new security controls for contractors that house covered defense information on nonfederal systems. Consistent with the Office of Management and Budget cybersecurity guidance issued in early August, DFARS Clause 252.204-7012 replaces the subset of required controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 with NIST SP 800-171 as the baseline security standard for protecting covered defense information. Ironically, although one of the stated directives of the Cybersecurity Executive Order was to "harmonize and make consistent existing procurement requirements related to cybersecurity,"[3] this interim rule leaves defense contractors potentially subject to differing security standards for the same information systems depending on which version of 252.204-7012 appears in their contracts and subcontracts.[4] Nonetheless, this change may provide clarity to contractors that have struggled to translate SP 800-53's federal system guidance to their own systems, as SP 800-171 was specifically tailored for protecting information stored on contractor systems. However, certain SP 800-171 security controls, such as the implementation of segregated networks or the requirement for multifactor authentication, could still prove costly or simply impractical to implement. Contractors should, therefore, engage with their technical experts to review their current security controls against SP 800-171, identify unmet requirements, and begin assessing how these requirements can be met.

Contractors that cannot meet the specific requirements of SP 800-171 may nonetheless be able to meet the security requirements of the interim rule. The interim rule added a new DFARS Clause 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," which pulls from the prior version of 252.204-7012 the concept that contractors can propose alternatives to the SP 800-171 security measures if those measures provide equally effective protection. Such proposals must be submitted in writing to the Contracting Officer and will then be reviewed and either approved or disapproved by the DoD CIO or the DoD CIO's authorized representative. This procedure provides potential relief from the more stringent requirements of SP 800-171, but the degree of such relief ultimately may be limited. The contractor still bears the burden of demonstrating that its approach will be equally effective, and, short of a bid protest or lawsuit challenging the government's determination as arbitrary and capricious, there is no apparent method for challenging a decision by the DoD CIO. For the time being, it is therefore difficult to tell whether contractors will be able to successfully convince DoD to accept alternatives to the SP 800-171 requirements.

New DFARS Clause 252.204-7009, "Limitations on the Use and Disclosure of Third Party Contractor Reported Cyber Incident Information"

The interim rule also adds DFARS Clause 252.204-7009, "Limitations on the Use and Disclosure of Third Party Contractor Reported Cyber Incident Information." This new clause provides added protection to contractors and subcontractors that are required to disclose

---

[3] Exec. Order No. 13636, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013).

[4] Indeed, the interim rule explicitly notes that the requirements of the revised DFARS safeguarding clause "in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements."

potentially proprietary information under DFARS Clause 252.204-7012. These protections include:

- prohibiting third party contractors assisting with assessments of cyber incidents from making unauthorized release or disclosure of information provided by a reporting contractor;
- subjecting third party contractors assisting with assessments to both criminal and civil actions for violations of the above prohibition; and
- designating the reporting contractor as a third-party beneficiary to any agreement between the Government and a contractor assisting in the assessment of the cyber incident.

These are all substantial protections for contractors reporting cyber incidents, but they still may not be sufficient. Attacks on contractor systems often target a company's crown jewels, and any disclosure of such information, no matter how well protected, could put a contractor at substantial risk. Accordingly, contractors must carefully review the information being disclosed and track to whom it is provided. This is especially true for lower tier subcontractors, whose information will be provided not only to the Government but to the prime contractor and each tier of subcontractor above the company.[5]

Moreover, missing from the new clause is any guidance or requirements as to how to handle organizational conflicts of interest (OCI) that may result from the disclosure of proprietary or program information to contractors assisting in the assessment of a cyber incident. Contractors should be attuned to this potential when bidding on opportunities to provide the assessment assistance to the Government and when choosing teammates who could conflict a contractor out of a particular procurement.

The Interim Rule Implements DoD Policies and Procedures for Use When Contracting for Cloud Computing Services

The interim rule also imposes substantial information security and cyber-incident reporting requirements on cloud service providers (CSPs) that deliver commercial cloud services in connection with DoD contracts. These new requirements apply to all DoD contracts, including commercial items contracts, for "information technology services." They are intended to implement two policies recently issued by the DoD CIO: (1) the December 15, 2014 memorandum titled "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," and (2) the January 13, 2015 "Cloud Computing Security Requirements Guide (SRG)," Version 1, Release 1. For ease of reference, we have underlined the key defined terms in the new rule.

[5] Moreover, the interim rule fails to adopt the language in the previous version of the DFARS rule that recognized that there could be "legal restrictions" on certain information related to the assessment that could not be produced to the Government.

Overview

DoD's interim rule introduces three major changes in the area of cloud computing:

First, the rule adds Subpart 239.76−Cloud Computing to the DFARS, which prescribes policies and procedures for the acquisition of cloud computing services by DoD. Specifically, the new subpart requires DoD to acquire cloud computing services "using commercial terms and conditions" typically found in commercial license agreements, End User License Agreements (EULAs), and Terms of Service (TOS), provided that such terms and conditions are consistent with applicable Federal laws and regulations and the agency's needs. The subpart also makes clear that DoD may only acquire cloud services from CSPs that have been granted an appropriate level of "provisional authorization" by the Defense Information Systems Agency (DISA). To obtain provisional authorization, a CSP must demonstrate that it can provide the relevant cloud services in accordance with the DoD Cloud Computing SRG.

Subpart 239.76 also requires DoD to provide CSPs with certain information in connection with a request for cloud services, including:

- Descriptions of the Government data and Government-related data that will be managed under the contract;
- Any relevant conditions or limitations that may apply to the subject data, including data ownership, licensing, or delivery and disposition instructions;
- Any applicable limitations and requirements regarding access to, and use and disclosure of, the subject data;
- Any applicable requirements regarding inspections, audits, investigations involving the subject data or the cloud services being acquired;
- Any applicable requirements to "support and cooperate" with searches of and access to the subject data in connection with authorized agency activities (e.g., inspections, audits, investigations, litigation, eDiscovery, records management); and
- Any requirement for the CSP to cooperate with the agency "to respond to any spillage" that occurs in connection with the cloud services being provided.

In addition, the new subpart requires that CSPs maintain "all Government data that is not physically located on DoD premises" within the "50 states, the District of Columbia, or outlying areas[6] of the United States." This requirement may be waived by the "authoriz[ing] official" described in DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology. Notably, the interim rule does not define "DoD premises," and it is unclear whether DoD installations or other DoD real property located outside the United States or its outlying areas are considered "DoD premises." It also is unclear whether this requirement applies only to the physical computing infrastructure that is used to deliver cloud services (e.g., networks, servers, storage, applications) or whether it also applies to all CSP employees who provide services under the contract.

[6] FAR 2.101 defines "Outlying areas" as (1) Commonwealths (Puerto Rico, The Northern Mariana Islands); (2) Territories (American Samoa, Guam, U.S. Virgin Islands), and (3) Minor outlying islands (Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll).

Second, the interim rule creates a new DFARS clause, 252.239-7009, "Representation of Use of Cloud Computing," which requires prospective offerors on covered DoD contracts to indicate whether they anticipate using "cloud computing" services in the performance of the contract or any subcontract awarded at any tier thereunder. The clause defines "cloud computing" as:

> [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 commercials offerings for a software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

Third, the interim rule also introduces a new clause at DFARS 252.239-7010, "Cloud Computing Services," which, as described below (i) establishes the minimum security requirements that apply to DoD cloud services contracts, (ii) imposes limitations on, access to, and use and disclosure of, Government data and Government-related data, (iii) creates mandatory procedures for reporting cyber incidents involving cloud services contracts, and (iv) requires CSPs to provide DoD access to information, equipment and facilities in connection with certain authorized Government activities.

Cloud Computing Security Requirements

DFARS 252.239-7010 provides that CSPs delivering cloud services in connection with a covered DoD contract:

- Must "implement and maintain administrative, technical, and physical safeguards and controls" that comply with the requirements of the then-applicable version of the DoD Cloud Computing SRG. The current version of the SRG is available at: https://info.publicintelligence.net/DoD-CloudSecurity.pdf.
- Must, as described above, maintain all "Government data" that is not physically located on "DoD premises" within the United States or its outlying areas. The clause defines "Government data" as "any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official business." This definition is extremely broad, and may, for example, include purely private or commercial/proprietary information, as long as it was "obtained by the Government in the course of official Government business." The clause does not define the term "Government," nor does it describe the types of activities that are considered to be "official Government business."
    - Notably, this requirement does not apply to "Government-related data," which is defined as "any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by a contractor through the storage processing, or communication of Government data." Government-related data does not include contractor's business records (e.g., financial, records, legal records or proprietary data) "that are not uniquely applied to the Government data." The clause does not, however, provide guidance on how to

determine whether a particular record is or is not "uniquely applied to the Government data."

Limitations on Access To and Use and Disclosure of Government Data and Government-Related Data

The clause also imposes the following limitations on access and use of Government data and Government-related data:

- CSPs and their employees may not "access, use, or disclose" Government data unless specifically authorized by the terms of their contracts or orders issued thereunder. According to the clause, these obligations survive the expiration or termination of any contract or subcontract to which they apply. It is unclear whether, after expiration or termination, CSPs and their employees are permitted to access, use or disclose Government data if they do so in compliance with the terms of the expired or terminated contract or subcontract.
- CSPs may only use Government-related data "to manage the operational environment that supports the Government." Any exception to this rule must be authorized in advance and in writing by the cognizant contracting officer. As described above, the clause does not explain how to determine whether a particular record is "uniquely applied to Government data," and, therefore, whether it is "Government-related data" that is subject to the restrictions on access, use, or disclosure. This lack of clarity could cause contracting officers to be inundated with requests for approval to use, access, or disclose information that may not clearly fit within the definition of "Government-related data."

Cloud Computing Cyber Incident Reporting

The new clause requires CSPs to report "cyber incidents" that are "related to the cloud computing service provided" under the subject contract or subcontract. The phrase "related to the cloud computing service provided" is remarkably broad and could be problematic for CSPs that utilize the same resources (e.g., servers, networks) to manage both Government and non-Government data. The breadth of this requirement is compounded by the fact that it adopts the definition of the terms "cyber incident" and "compromise" in DFARS Part 202.101, both of which are very broad, as described above.

- Notably, it does not appear that the "rapid reporting" requirement of revised DFARS 252.204-7012 (i.e., within 72 hours of discovering a cyber incident) applies to contracts or subcontracts for cloud services.

Providing Access to Equipment, Information and Facilities

DFARS 252.239-7010 also contains a number of broadly-worded requirements that allow the Government to gain access to a CSPs' equipment, information, and facilities. For example:

- CSPs are required, "upon request by DoD," to provide DoD with access to "information or equipment" that is deemed "necessary to conduct a forensic analysis." This provision contains no limitations on the types of "information or equipment" that can be accessed by the Government, nor does it describe the potential scope or intended purpose of the "forensic analysis" to which CSPs will be required to submit (*e.g.*, in the event of a cyber incident in which Government data may have been compromised). Further, it provides

no mechanism by which a CSP can refuse or attempt to limit the scope of such a "request by DoD," even if the request is unduly burdensome or otherwise improper.

- CSPs are required to provide the Government, or its "authorized representatives," access to (i) all Government data and Government-related data, (ii) contractor personnel involved in the performance of the contract, and (iii) physical access to "any Contractor facility with Government data," for the purpose of audits, investigations, inspections or other similar activities, as authorized by law or regulation. In responding to such requests for access, CSP contractors must ensure that the Government has clearly articulated the statutory or regulatory basis for the request, particularly if the request will be carried out by an "authorized representative[]" of the Government, which could include other government contractors.

Other Notable Requirements of DFARS 252.239-7010

Additional notable requirements imposed on CSPs by DFARS 252.239-7010 include:

- Third-Party Requests: CSPs are required to "promptly" notify the contracting officer of any third-party request for access to Government data or Government-related data, including any warrants, seizures or subpoenas from any federal, state, or local agency. The term "promptly" is not defined. In addition, the provision requires the CSP contractor to cooperate with the contracting officer "to take all measures to protect Government data and Government-related data from any unauthorized disclosure." It provides no guidance, however, on what CSP contractors should do if the contracting officer does not authorize the release of relevant information in response to a warrant, seizure or subpoena.
- Information Spillage: CSPs must cooperate with the Government to "address" any spillage. The clause defines "spillage" as a "security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (*i.e.*, authorized) for the appropriate security level. It is unclear whether and to what extent CSP contractors will be reimbursed for the cost of addressing a spillage, including a spillage that may have been caused by the Government or its authorized representatives.
- Subcontracts: DFARS 252.239-7010 is a mandatory flow down in all subcontracts "that involve or may involve cloud services," including subcontracts for commercial items.

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

Susan Cassidy	+1 202 662 5348	scassidy@cov.com
Alex Sarria	+1 202 662 5426	asarria@cov.com
Patrick Stanton	+1 202 662 5441	pstanton@cov.com
Catlin Meade	+1 202 662 5889	cmeade@cov.com