DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
www.dlapiper.com

Sam Knowles
sam.knowles@dlapiper.com
T 202.799.4404
F 202.799.5404

July 11, 2019

SUBMITTED VIA WWW.REGULATIONS.GOV

Defense Acquisition Regulations System
Attn: Kimberly Ziegler
OUSD(A&S)DPC(DARS)
3060 Defense Pentagon
Room 3B941
Washington, DC 20301-3060

Re: Docket Number DARS-2019-0020; OMB Control No. 0704-0478: Information Collection Requirement; Defense Federal Acquisition Regulation Supplement (DFARS); Cyber Incident Reporting and Cloud Computing

Dear Ms. Ziegler:

On behalf of our client, a Fortune 100 company and government contractor, we respectfully submit the following comments on the proposed rule cited above. In sum, as reflected in our comments below, we are concerned that the current information collection and incident-reporting requirements are overly burdensome – particularly on commercial item contractors.

In the case of our client, and many similarly-situated contractors, revenue from government agencies represents a very small percentage of overall revenue. Indeed, the value of our client's services and the benefits that the government receives are derived, in large part, from economies of scale and from the operation of an international commercial business. However, the unique government requirements that require contractors, like our client, to deviate from standard commercial practices, are increasingly burdensome and inefficient. The cybersecurity, reporting, and record-keeping requirements that are the subject of the proposed rule are no exception. To be clear, companies like our client understand the importance of information security and employ robust measures to protect customer data. However, these companies take a comprehensive approach to protecting information across the company's entire business and generally do not tailor their cybersecurity and privacy practices to address unique requirements of any one customer. Accordingly, satisfying the government-specific cybersecurity, recordkeeping, and reporting obligations set forth in DFARS 252.204-7012 are overly burdensome to commercial item contractors.

Importantly, the Federal Acquisition Regulation provides that agencies shall include only those terms and conditions "[d]etermined to be consistent with customary commercial practice." FAR 12.301(a)(2). The imposition of onerous government-specific cybersecurity requirements, combined with the Government's reluctance to grant waivers for systems that already maintain robust security controls, runs contrary to this policy. As a result, placing these regulatory burdens on commercial item vendors creates a disincentive for

those vendors to stay in the defense market and erects barriers to new entrants, which stifles competition and conflicts with many of the Department's commercial item outreach initiatives.

Moreover, the applicable requirements can be ambiguous, particularly where the Government does not clearly identify CDI being provided under the contract or, alternatively, creates contract-specific obligations that require contractors to satisfy the requirements of DFARS 252.204-7012 for categories of information much broader than those that fall within the definition of CDI. The resulting uncertainty surrounding what information must be protected can create inefficiencies in reporting and implementing compliance systems. We appreciate your time and attention to this important matter.

1. The existing rule, specifically DFARS 252.204-7012(g) – (j), discusses the Government's safeguarding, use, and release of cyber incident information that is reported and collected, including the ability to release information outside of the United States Government, s*ee, e.g.*, DFARS 252.204-7012(i)(1). Other than generally discouraging the release of attributional/proprietary information and urging contractors to mark information as proprietary (a process that could delay reporting when a company is in the midst of responding to a cyber incident), the clause does not specify the process that must be used to prevent against the release of proprietary information. To ensure proper safeguarding of contractors' attributional/proprietary information, we recommend that the contractor submitting the information be afforded an opportunity to review and propose redactions prior to release. Furthermore, contractors should be permitted to apply protective markings to information after its submission to the Government. A reasonable opportunity to correct initial oversights would help protect contractors seeking to comply with prompt reporting requirements and would not create an undue burden or risk for government agencies. In addition, time should be allotted for a contractor to pursue any administrative or legal remedies in the event that the Government plans to disclose information that the contractor has otherwise proposed to be withheld. This process would be similar to that undertaken when the Government plans to release information under the Freedom of Information Act.

2. The current clause's "rapidly reporting" requirement, DFARS 252.204-7012(c)(1)(2), is extremely burdensome on contractors. It is particularly impactful on contractors that have robust IT capabilities and many different systems because they may require more time to fully assess the scope of a cyber event. Moreover, the 72-hour reporting requirement results in significant over-reporting, inefficient use of resources, significant costs incurred on outside consultants, and unwarranted scrutiny on contractors. In particular, contractors are often concerned that they must report even if they do not have sufficient information to assess whether there was a "cyber incident" with an actual or potential impact on a covered contractor information system or CDI. We recommend either extending the period to report or, otherwise, amending the clause to explain that the 72-hour reporting period begins to run once a contractor knows or should have known that CDI was adversely impacted or it is "highly likely" that CDI was adversely impacted. In addition, we

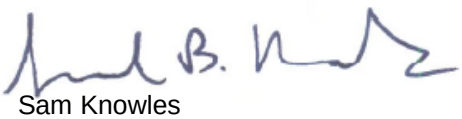
suggest that a medium assurance certificate need not be required for initial reporting. This requirement limits the person(s) within the entity who may report and may impede the ability to report within the requisite time period.

3. DFARS 252.204-7012(c)(1) requires contractors to report cyber incidents that affect "a covered contractor information system or the covered defense information residing therein." However, there is often ambiguity as to what is considered CDI under specific contracts. Any ambiguity ought to be resolved by the Government, as agency personnel are best suited to identify the CDI being provided to a contractor and make appropriate notifications. Unfortunately, in many instances, contracting officers do not know whether, and to what extent, information under a given contract is CDI or, are otherwise reluctant to engage with contractors to reach a mutual agreement regarding what is considered CDI. The result is often significant over-reporting because, in the face of a cyber incident, contractors often take an overly broad view as to whether CDI was impacted. Accordingly, we suggest that DoD develop processes and procedures for engaging with contractors on the designation of information as CDI during the solicitation process or otherwise before the contract is finalized. Such processes and procedures would foster a more efficient use of contractor resources and more certainty with regard to compliance obligations.

4. DFARS 252.204-7012, as drafted, applies to contractors that possess CDI. However, certain commands within the Department have created contract-specific requirements mandating that contractors apply the protections and reporting requirements of DFARS 252.204-7012 – including the reporting and record-keeping obligations – to categories of information much broader than CDI. In some cases DoD agencies impose the DFARS 252.204-7012 requirements on all information generated under the contract. These same commands then place the burden on the contractor to determine what information must be protected and do not engage with the contractor on these issues. Contractors who perform contracts with such contract-specific requirements incur significant time and expense on compliance despite the fact that the regulation was not intended to extend to information under their contract. In order to reduce the already burdensome requirements on these contractors, we recommend that any extension of the record-keeping and reporting obligations expressly exempt commercial-item contractors and contractors that do not possess CDI, regardless of contract-specific cybersecurity requirements. We further suggest that before creating contract-specific requirements, agencies be required to obtain approval from a centralized office within the Department and to explain the basis for requiring protections in excess of what is required by DFARS 252.204-7012. This will enable the Department to better assess the burden of the reporting and record-keeping obligations on contractors that do not possess CDI.

Respectfully submitted,

DLA Piper LLP (US)



Sam Knowles
Partner