Raytheon Company
Global Business Services
880 Technology Park Drive
Billerica, MA 01821
US

February 11, 2016

Defense Acquisition Regulations System
Attn: Mr. Dustin Pitsch
OUSD (AT&L) DPAP/DARS
Room 3B941
3060 Defense Pentagon
Washington, DC 20301-3060

Subject: DFARS Case 2013-D018, "Network Penetration Reporting and Contracting for Cloud Services (Dec 2015)"

Dear Mr. Pitsch:

Raytheon Company has reviewed the DFARS interim rule on Network Penetration Reporting and Contracting for Cloud Services (Dec 2015) (DFARS Case 2013-D018) and is pleased to provide feedback regarding its content and proposed requirements.

The update in late December of the DFARS governing cybersecurity formally recognized the implementation challenges faced by the defense industrial base. There still are concerns regarding the significant increase in the depth and breadth of government oversight into contractor networks without the benefit of the close and cooperative collaboration between industry and the government that has served us well to date. We believe many of our concerns about the interim rule could be addressed by such collaboration going forward.

Versions

Following the December 2015 interim rule, the industry is faced with three different versions of DFARS 252.204-7012 across existing contracts. This complicates a given Contractor's ability to perform against the myriad of conflicting requirements. Once feedback below has been incorporated, Raytheon recommends ACOs / PCOs issue a block mod for all existing contracts to include the latest version and allowing for equitable adjustment to the contract price to reflect the increase in the number of NIST requirements and the broader definition of CDI.

Definitions

The development of the Covered Defense Information (CDI) classification with Subpart 204.7301 expands the scope of information covered too far beyond the already wide scope defined in the 2013 rule as Unclassified Controlled Technical Information (UCTI). The CDI definition is open-ended but specifically includes privacy and export controlled information. We recommend that covered data be limited to the UCTI covered in the predecessor DFARS rule. The interim rule's expanded definitions of data types covered--sweeping in personally identifiable information and export-import controlled information, for example--detract from the primary goal of protecting defense information and will result in increased internal and supplied part costs and duplicative regulation. The existing privacy and trade laws already govern the reporting of breaches or loss of these data types. A redundant requirement to report separately to DoD will increase administrative overhead without apparent value.

In the alternative, if the scope is not focused back to the UCTI definition, we recommend that the rule define CDI to specifically exclude the contractor's own information that is not delivered to the government. Such a carve out would add clearer scoping to potentially very broad categories such as export-controlled information.

Similarly, the Operations Security process through which "critical information" is determined needs to be properly defined and documented. Contracting officers are already struggling to adequately identify Controlled Technical Information (CTI). A process that lacks any formality for identifying additional instances of information within this CDI sub-category only results in additional confusion and waste during the acquisition process.

Marking

Under Subpart 204.7301, the definition of covered information is not limited to information that is so marked (either by DoD or by the contractor pursuant to explicit DoD instructions). The rule instead relies on criteria for categorization, which introduces subjectivity, variability, and uncertainty. This approach contrasts unfavorably with the predecessor rule and guidance, issued in November 2013, which clearly required CTI be marked as such. With contractors left to decide whether unmarked information on their systems qualifies as CDI, we are experiencing confusion, divergent results, and increased costs. This problem emerged through experience in which PCOs suggest the extremes of classifying all program data as CDI or providing no guidance at all. Due to their inability to address CDI, we recommend reversion back to the original requirement for data marking promulgated in 2013.

Applicability

It is unclear whether the clause applies to CDI resident on Contractor classified information systems. While the CDI itself has been explicitly defined as unclassified, covered contractor systems are not specified as such. There is a general acceptance within industry that systems accredited/authorized under NISPOM or similar customer requirements exceed those set forth in NIST SP 800-171. However, a formal declaration on this matter would remove the doubt.

Process

The December 2015 interim rule introduces the requirement that the contractor provide notification to the DoD CIO within 30 days of contract award listing the unmet NIST SP 800-171 security requirements. The benefit derived from this requirement is unclear. DoD will likely be overwhelmed by tens of thousands of programs and, absent an even more burdensome requirement on the contractor to report progress, the value DoD CIO will accrue from these assessments is not obvious. Furthermore, for new programs, compliance would be built into the proposal. Full compliance or gap documentation would be achieved with the standup of any program environments, which rarely happens within 30 days, thus making a 30 day analysis premature. For current programs, our experience already has shown that the complexity of their longstanding environments will make it difficult to conduct a thorough gap analysis in 30 days. This may often result in an incomplete picture simply to satisfy contractual requirements. In neither situation does the security posture of the program directly benefit from the activity. Where a program is at the 30 day mark becomes irrelevant when the mandate is to be 100% compliant by the end of 2017 regardless of the starting point. Therefore, the 30 day assessment requirement should be deleted.

If the 30 day assessment requirement remains, it contains several ambiguous aspects that call for clarification. For example, is the 30-day deadline for the Prime Contractor's response only, or also for the Prime's entire supply base? Raytheon recommends the -7012 clause specify the 30-day deadline after the government's contract award applies only to the Prime's report of its own control implementation, while a supplier's 30-day window (or more) opens upon the award of its subcontract.

Clarification is also required on what is required for the 30 day assessment if the contract in question ends prior to the 31 December 2017 compliance date.

With respect to seeking DoD approval for a contractor's compensating controls, a well-defined process workflow would be beneficial for all parties. This process would clarify whether the Prime submits the request only for itself or also includes that of its suppliers. Also, should the request be sent to the PCO or direct to the DoD CIO? At the DoD Industry Day, officials mentioned that contractors may bypass their Prime when submitting in order to safeguard any proprietary information, and the -7012 clause should specifically allow for this.

Security Controls

NIST SP 800-171's intent to reduce the burden of implementing security controls on non-federal systems is appreciated although we believe the increased number of controls will be too burdensome on small to medium-sized companies throughout the DoD supply base. We recommend DoD establish a collaborative working group with industry with the goal of removing controls that may represent best practices but not materially move the needle in a company's security.

The DFARS interim rule requires compliance with NIST 800-171 controls in their entirety. This creates a binary pass/fail compliance test that will be unachievable by most companies. While a purely technical analysis might conclude the number of inherent tasks (as opposed to controls) is reduced by the 2015 interim rule, the burden is, in fact, greater. Several of the new controls greatly exceed those of the earlier NIST 800-53 controls in their complexity and cost implications. As such, many companies will find it difficult to become compliant even by December 2017. Raytheon advocates a tiered approach to implementing controls specified by the new rule. A tiered construct would reward a company for incremental improvements while providing an incentive to achieve the next higher tier.

We recommend large companies be allowed to certify at the company level. The requirement to certify each program individually creates an insurmountable burden for both the company and DoD when the prime contractors alone have thousands of programs. This will create a tremendous amount of redundant work for both when the vast majority of programs are relying on corporate-level controls that will be identical in every case.

The security requirement of multifactor authentication for all network connections is onerous. The October 2015 class deviation appears to acknowledge the burden of this requirement; however, it is not sufficient considering the impact to larger contractors and their complex computing environments, let alone the sheer cost of such an endeavor. The requirement for multifactor authentication should be limited to remote access, system administrators, and externally facing systems. This would be a level of effort that would be achievable by all companies and result in most of the practical benefit of multifactor authentication at a fraction of the cost.

Suppliers

The cost impact of levying these security controls on the internal systems of small to medium subcontractors and suppliers cannot be overstated. The success of major programs is built on such companies that could potentially be put out of business due to the sheer cost of control implementation. Many suppliers will be unlikely to afford the investment required to meet these requirements, nor will the skilled labor force required to manage the controls be readily available. As a result, Raytheon expects a non-trivial surge of supplier exceptions with respect to these DFARS cybersecurity requirements that will likely impact subcontracting cycles and deliveries throughout the DoD supply chain.

Incident Reporting

The requirements have increased incident reporting to also include potentially adverse effects on an information system regardless of an actual compromise to CDI. This requirement should be deleted, as too burdensome to industry for little apparent benefit, or reverted to the 2013 version of reporting only detection of actual compromise. Otherwise, the provision amounts to a requirement for contractors to submit their daily cybersecurity operations report to the government. Raytheon recommends the guidance

make clear the cyber incident reporting requirements apply only to CDI that is marked by the government or should be marked by contractors pursuant to clear government instructions in the contract.

The rule as written requires subcontractors to report incidents directly to the government and the prime contractor. It is not clear what specific information the subcontractor must share with the prime directly, or how much of the DIB submission the prime will receive. This ambiguity will create significant confusion when the government takes action on a compromise about which the subcontractor has not fully briefed the prime. We recommend a subcontractor's reporting responsibility be to the prime contractor, with whom the government has the direct contractual relationship.

Post-incident Investigations

The expectation that contractors provide DOD with access to our systems and personnel used in contract performance, regardless of location, for investigations and evidence preservation during incidents likewise raises concerns. The contractor may have other contracts or non-disclosure agreements that create legal conflict with this requirement, especially those with foreign governments. In addition, the guidance does not address how the Government would protect proprietary and attribution information shared by contractors that report cyber incidents. We recommend that appropriate restrictions and parameters be used to protect unauthorized use or disclosure of such information.

Beyond incident-related investigations, the government stipulates that incident data may also be used for national security purposes. Such a vague justification causes concern that the information contractors provide will be used for tangential purposes. The rule offers no relief to contractors for legal restrictions that might prohibit release of information to government, or even contemplate how to avoid organizational conflicts of interest (OCI) that could arise from contractors assisting with post-incident investigations.

Cost Recovery

The cost recovery model for complying with the interim rule is not well understood. The cost to Raytheon and its supply base will be significant as we expand our capabilities to meet the new controls and absorb the administrative costs to oversee our supply base's compliance. The costs and disruption to our small and medium suppliers will be even greater, given they are starting from a much less mature point. Raytheon recommends that OUSD(AT&L) work with industry to clarify cost recovery options. Absent any further guidance, Raytheon is building the direct costs at the program level into our bids and indirect costs into our rates; our suppliers will bid their proposals accordingly.

Thank you for the opportunity to offer feedback on the interim rule.

Jeffrey C. Brown

Digitally signed by Jeffrey C. Brown
DN: dc=com, dc=raytheon, o=CAs, ou=class3, ou=users, 0.9.2342.19200300.100.1.1=1051954, cn=Jeffrey C. Brown
Date: 2016.02.11 11:51:53 -05'00'

Jeff Brown
Vice President and Chief Information Security Officer
Raytheon Company