



December 16, 2011

Defense Acquisition Regulations System

Attn: Mr. Julian Thrash

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

Defense Procurement and Acquisition Policy, Room 3B855

3060 Defense Pentagon

Washington, DC 20301-3060

Re: DFARS Case 2011-D039; Safeguarding Unclassified DoD Information

Dear Mr. Thrash,

On behalf of The Coalition for Government Procurement, the following comments are provided on the proposed rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and associated contract clauses to address requirements for safeguarding Department of Defense (DoD) unclassified information. The proposed rule was published in the Federal Register on June 29, 2011.

The Coalition for Government Procurement is a non-profit association of approximately 300 firms selling commercial services and products to the Federal Government. Our members collectively account for approximately 70% of the sales generated through the GSA Multiple Award Schedules (MAS) program and about half of the commercial item solutions purchased annually by the Federal Government. Coalition members include small, medium and large business concerns. The Coalition is proud to have worked with Government officials over the past 30 years towards the mutual goal of common sense acquisition.

The Coalition is concerned that the proposed rule will require commercial companies to make costly changes to their internal systems which may inevitably lead to higher costs for commercial items on the part of the American taxpayer. Implementation of many of the proposed security requirements extends far beyond normal corporate practices. In light of the Better Buying initiative and the associated objectives to achieve cost savings, the Coalition recommends that DoD apply an exception for commercial-off-the-shelf products.

Protection of Federal Data

The DFARS proposed requirements do not reference commercial practices in the protection of unclassified DoD information nor has the Department provided their own guidance on a number of issues that require clarification before companies can comply. Service providers need DoD guidance regarding how data that is authorized for public release should be distinguished from data that is not, and how this process should be managed. Further, DoD clarification regarding what constitutes an “enhanced” level of protection and an “advanced persistent threat” is necessary. Without such guidance, it will be difficult for commercial contractors to comply with the proposed rule.

Reporting Cyber Incidents

Again, the Coalition recommends further guidance regarding how contractors should report cyber incidents affecting unclassified DoD information such as where to report, within what period of time, and what types of incidents should be covered. Also, more details explaining how the reported information will be protected is needed for contractors to better understand the ramifications involved and whether any reduction of liability will be considered for intrusions that are voluntarily reported.

Proposed DFARS Language

252.204-70XX(a) and 252.204-70YY

The Coalition requests that the Department define what constitutes an adequate level of security – whether it’s based on a FISMA or a similar federal standard, or adequate commercial controls.

252.204-70XX(b)(1)

The proposed definition of data in the application of this part is overly broad. In order for the contractor to comply, DoD information must be uniquely categorized and tracked. Customized systems would need to be put in place in order to protect information that is not specifically approved for public release. Given the complications and costs involved in developing such a system, contractors are likely to resort to protecting all DoD information rather than adopting a more sophisticated system with various levels of control.

252.204-70XX(b)(2)

The Coalition recommends rephrasing 252.204-70XX(b)(2) by changing “best” to “adequate” so that the language is consistent with other parts of the proposed rule. As new technologies are developed, the “best level of security and privacy available” becomes a constantly evolving and thus moving target. This is also a rather subjective term which does not consider cost. Providing the “best” level of security and privacy available may not be the most cost effective solution from the perspective of the government or the American taxpayer.

252.204-70XX(b)(7)

Reasonable corporate-level intrusion protection based on industry best practices should be acceptable for commercial contractors.

252.204-70YY(d)

Implementation of NIST SP 800-53 within a corporate network is not a commercial practice. Adopting this standard within a corporate IT environment is cost prohibitive and not practical in regular business practice. The Coalition highly recommends that the DoD look to commercial best practices if the proposed rules are intended to cover commercial items.

Consistency Government-wide

If the government is to impose requirements for the protection of unclassified information, the standards to do so should be consistent government-wide. The Coalition is concerned that there are other efforts within the government to provide similar protection as DFARS Case 2011-D039 proposes. The DoD proposed rule appears to be getting ahead of government-wide guidance on this issue. As such, it is possible that the Department will require contractors to make costly changes to their internal IT environments which are later superseded by new requirements. As a result, we highly recommend that the DoD release procedures for protecting unclassified information at a later time when they can be harmonized with similar requirements from civilian federal agencies to ensure consistent application of these protections government-wide.

The Coalition appreciates the opportunity to submit comments on this proposed rule. If you have any questions, please contact me at (202) 331-0975 or rwaldron@thecgp.org.

Regards,

A handwritten signature in black ink, appearing to read 'Roger Waldron', with a long horizontal flourish extending to the right.

Roger Waldron
President