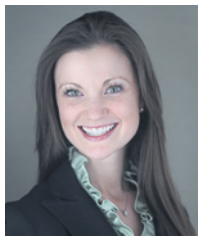
Bloomberg BNA

Federal Contracts Report™

DOD

View From Crowell & Moring: Getting Ahead of the DFARS Safeguarding Clause





BY DAVID BODENHEIMER, EVAN WOLFF AND KATE GROWLEY

On November 18, 2013, the Department of Defense (''DoD'') finalized DFARS 252.204-7012, Safeguarding of Unclassified Controlled Technical Information (''Safeguarding Clause'' or ''rule''). Stemming from the DoD's determination that unclassified but controlled technical information (''UCTI'') is vital to national security and must be protected, the Safeguarding Clause is now mandatory in all DoD-funded contracts awarded and solicitations issued. Generally speaking, the objectives of the rule are straightforward: first, require defense contractors handling UCTI to implement certain security controls for their information systems; and, second, further require these defense contractors to notify the DoD if those systems have nonetheless been compromised. The experience over the past eight months, however, has shown that the implementation may raise more questions than answers. For those grappling with the new rule, some key challenges and preliminary practical pointers are summarized below.

The co-authors of this article are Government Contracts Group attorneys in the Washington, D.C. office of Crowell & Moring LLP. David Bodenheimer is a partner and focuses his practice on government contracts, False Claims Act, privacy, and cybersecurity matters. Evan Wolff is a partner and co-leads the Privacy & Cybersecurity Practice, where he focuses on homeland security, privacy, and data security matters. Kate Growley is an associate whom focuses her practice on the intersection between national security and private industry.

Applicability. When approaching the Safeguarding Clause, the initial question is whether it applies at all. Although *every* DoD contract will include the new rule's language, not every contract will trigger its requirements. UCTI must either ''reside on'' or ''transit through'' a contractor's information system to invoke the rule's security and reporting requirements. Identifying UCTI thus represents a crucial first step.

The Safeguarding Clause defines UCTI in two steps:

- ''Technical information'' is ''technical data or computer software,'' as defined separately in DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items. This includes recorded information of a scientific or technical nature, as well as any materials that would enable software to be reproduced, recreated, or recompiled. As such, engineering drawings, specifications, standards, process sheets, manuals, technical reports, and source code are all examples of common technical information under the rule.

- Technical information becomes ''controlled'' if it has a military or space application, and is also subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dis-

 ISSN 0014-9063

semination. Accordingly, UCTI excludes that which is lawfully publicly available without restrictions.

As one challenge to implementing the requirements, the Safeguarding Clause does not distinguish between UCTI that a covered contractor receives pursuant to its contract, versus that which it may generate or otherwise use in order to fulfill its contractual obligations. Just because an award or solicitation does not refer to UCTI does not mean it – and the Safeguarding Clause – is inapplicable. For this reason, contractors need to focus on the nature of the data itself, rather than what, if anything, the contract says about it.

In addition, the safeguarding rule is a mandatory flowdown provision. Consequently, subcontractors should be asking these same questions. Again, the key will be whether, under their contract, UCTI resides on or transits through their information systems, regardless of the UCTI's source.

'Adequate Security'. Once a defense contractor (or subcontractor) has determined that its DoD contracts may involve housing UCTI on its information systems, the next question is the applicable standard. The Safeguarding Clause generally applies a standard of ''adequate security.'' At a minimum, ''adequate security'' includes the adoption of 51 specific security controls listed in NIST Special Publication 800-53. Covered contractors may propose a different standard, such as ISO 27002, provided that they can persuade the DoD that such alternative controls achieve equivalent protection as that provided by the NIST standards.

Furthermore, maintaining ''adequate security'' may also include the adoption of any additional controls that the contractor deems necessary to provide security commensurate with known risks. For example, a covered contractor who receives threat intelligence through an information sharing program may need to go above and beyond the specified NIST controls to address a specific vulnerability.

Here, too, lies another word of caution: implementing the minimum security controls specified in the Safeguarding Clause is not a ''check the box'' exercise. Instead, it contemplates a dynamic, thoughtful response to a changing threat environment. In such cases, covered contractors would be well served by documenting their risk assessments justifying the proposed controls.

Defining Reportable Incidents. The second primary component of the Safeguarding Clause provides for contractors to report certain ''cyber incidents'' to the DoD – and in a rather tight timeframe. The rule describes two kinds of ''reportable'' cyber incidents:

- Those involving the possible exfiltration, manipulation, or other loss or compromise of any UCTI resident on or transiting through a covered contractor's unclassified information systems; and
- ''Any other activities'' that allow unauthorized access to the covered contractor's unclassified information systems on which UCTI is resident or transiting.

While perhaps counterintuitive, not every ''reportable'' cyber incident must actually be reported. The Safeguarding Clause explains that a covered contractor only needs to report such an incident if it ''affects'' UCTI on its unclassified information systems. The challenge is determining what this means, given that the Safeguarding Clause does not provide further guidance on this standard.

Covered contractors may consider engaging the DoD about its understanding of the reporting triggers. The Department has been internally crafting guidance for its Contracting Officers (''COs'') so that they can help direct covered contractors through the rule's maze of security and reporting requirements. For instance, contractors may seek answers by submitting pre-bid questions, or inquiring with their CO. In light of the short window in which a covered contractor must notify the DoD of a reportable cyber incident, a prepared contractor would want such advice well in advance.

Reporting Requirements. Once a covered contractor has discovered a reportable cyber incident that affects its UCTI, the Safeguarding Clause gives only 72 hours to provide the DoD with specific information related to incident. This may include logistical and administrative information related to the affected systems and data, as well as certain information related to the incident itself, including the type of compromise and a description of the technical information actually or potentially compromised.

In this scenario, a contractor may need to be prepared to collect, analyze, and produce over a dozen specific items within three *calendar* days of an incident's discovery. To be better prepared, defense contractors should take a close look at their incident response plans to confirm that they address the basic reporting items and are practiced enough to react within the short period provided. As a best practice, a prepared contractor will want to address its response plans and execute tabletop exercises well before accepting a contract that contemplates UCTI.

Conclusion. The DFARS Safeguarding Clause has been a long time in the making. Its focus on unclassified technical information echoes the DoD's concern that technology losses pose a serious national security threat to the United States. In today's world, that compromise often comes in the form of a cyber incident. The rule is thus an understandable step towards better securing military technology and secrets. Although its development reflects a number of compromises and challenges that will drive how both the DoD and contractors interpret and implement the rule, it remains mandatory. Contractors will do well by getting ahead of its requirements and developing sound information security programs, not only to comply with the rule but also to safeguard their own technology and intellectual property.

  FCR ISSN 0014-9063