Bloomberg BNA

Federal Contracts Report™

Cybersecurity

View From RJO: DOD's Cybersecurity Initiative—What the Unclassified Controlled Technical Information Rule Informs Public Contractors About the New Minimums in Today's Cyber-Contested Environment

BY ROBERT S. METZGER AND LUCAS T. HANBACK

On November 18, 2013, the Department of Defense (DOD) finalized its rule governing Unclassified Controlled Technical Information (UCTI). Since then, it has included DFARS clause 252.204-7012, which implements the rule, in all new solicitations and contracts. On December 16, 2014, DOD revised DFARS Subpart 204.73. 79 Fed. Reg. 74652. The changes indicate that DOD will assess contractor compliance with the UCTI regulations in accordance with Procedures, Guidance and Information (PGI) which DOD issued on December 12, 2014. (The pointer to access both the revised DFARS and the PGI is available through http://www.acq.osd.mil/dpap/dars/change_notices.html.)[1]

The importance of the UCTI rule to the entire DOD supply chain has not been well understood. The new PGI and FAQs help to explain what DOD seeks to accomplish, how it is to be achieved, and how this rule will affect defense suppliers at all tiers.

DOD's UCTI regulations are likely a precursor to other pending initiatives to apply similar minimum cyber assurance standards to all federal acquisitions. Companies that adopt cyber controls and reporting protocols that meet or exceed the DFARS UCTI rule will be well positioned to comply with comparable rules as they emerge from other federal agencies. Strong cyber assurance measures are likely to emerge as an important and favorable competitive discriminator.

Objectives of the UCTI Rule. Fundamentally, the UCTI rule imposes minimum cybersecurity standards and practices upon DOD's supply chain. There are several principal objectives. One is to protect DOD's sensitive but unclassified information, where it resides or passes through information systems operated by DOD contractors, from exfiltration (theft) or manipulation. Protecting this information should deny rival nations and unauthorized competitors the ability to learn sensitive information or exploit U.S. technologies. A collateral benefit is that improvements that better defend contractor systems against cyber attacks will protect company-owned intellectual property and proprietary information, and therefore enhance the security of the U.S. industrial base. Another principal objective is to require more DOD contractors to promptly report cyber incidents and to improve contractor responses to such events. Timely receipt of information on cyber attacks has many benefits. National counter-intelligence resources and cyber specialists can recognize attack vectors as well as new or varied means of cyber attack. Alerts can be communicated within the federal supply chain or more broadly. Defenses and countermeasures can be organized and disseminated more quickly. Improved reporting of cyber events also informs DOD owners of UCTI where an attack has caused compromise of information security. This is necessary to mitigate potential adverse consequences and to restore information systems functionality after attacks.

The UCTI rule does not cover classified information. Though it applies to DOD's larger contractors, its focus is not upon them – because larger DOD contractors, especially if they perform classified work, already will have systems and procedures in place that exceed the

[1] Further explanation is provided by a document presenting "Safeguarding Unclassified Controlled Technical Information (CTI), Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73," available at http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf.

Rogers Joseph O'Donnell, P.C., is a boutique law firm that has specialized in public contracts for more than 33 years. Robert Metzger is a Shareholder and heads the Washington, D.C. office of the firm. Lucas Hanback is an associate in the firm's Washington, D.C. office. This article presents the individual views of Mr. Metzger and Mr. Hanback and should not be attributed to any client of Rogers Joseph O'Donnell, P.C.

 ISSN 0014-9063

baseline standards of the UCTI rule. Instead, the focus is upon the many thousands of smaller companies who participate in DOD's supply chain, who may host or transport sensitive DOD CTI, but may not have minimally sufficient cyber protection or operative reporting protocols. From a threat perspective, improved protection of the cyber assurance of these companies is important to national security.

The Cyber Threat to DOD's Supply Chain. The cyber threat environment is characterized by diverse, determined and resourceful adversaries. They may include nation states, sophisticated non-state actors enjoying state sponsorship or tolerance, terrorist organizations, as well as smaller subversive elements and individual hackers. Foreign business rivals also can employ cyber assault methods purely for commercial gain, and sometimes do so with state support. The impact of attacks also varies greatly. Some attacks, as evident from the Sony Pictures hack, appear to be politically motivated but have largely a disruptive intent. Many attacks seek to deny or disrupt service. Of greatest concern to DOD are cyber attacks that seek to find or create information system vulnerabilities and to extract or subvert sensitive information and steal intellectual property.

Larger and more sophisticated U.S. defense contractors may be resistant to most attacks. They can be expected, already, to have robust cyber defenses and to be vigilant in responding to the rapid dynamics of changing cyber threat. Smaller companies, as a generalization, have greater vulnerability. Yet important and sensitive DOD information may be used routinely by these companies, for design and development, in services they supply or products they deliver, and in the tools and methods they employ. Adversarial access to this information, through cyber attack, can injure both national and commercial interests. For illustration, adversaries may be able to find vulnerabilities in the network system of smaller companies that they can exploit to provide gateways to illegal access to other connected networks. Hostile actors may steal device technology from unprotected contractor systems and use it to create hard-to-identify counterfeit parts or even ''clones'' of electronic parts that harbor tampered code or malicious firmware. Again for illustration, a hacker might exfiltrate a contractor's software code to create counterfeit software or even to insert, surreptitiously, corrupt code sequences in the ''original'' code that remains on the contractor's system.

These threats are very real, even if rarely disclosed publicly. The UCTI rule recognizes that adversaries are all too likely to exploit those areas of the U.S. defense industrial base which are less protected and where responses to cyber attacks are slow or incomplete. That is why, as shown below, the rule has such broad applicability.

The UCTI Rule is Broadly Applicable. The UCTI rule applies to contracts and subcontracts requiring safeguarding of UCTI on non-federal contractor information systems. As confirmed by the newly published FAQs, the contract clause at DFARS 252.204-7012 is to be included in *all* solicitations and contracts, including solicitations and contracts using FAR Part 12 procedures for acquisition of commercial items. While the DFARS clause does not apply retroactively, contracting officers are permitted to apply it by modification to an existing contract.

Smaller companies may figure their contribution to a delivered military system is ''minimal'' and therefore may suppose this rule is irrelevant to them. They would be wrong. There are no exceptions for small business. The UCTI rule applies to every company, irrespective of size, that makes use of, hosts or transmits UCTI. This is made clear by the very broad flowdown requirements of DFARS 252.204-7012(g), which reach ''all subcontracts, including subcontracts for commercial items.'' As explained in the promulgation comments that accompanied publication of the final rule, ''the prime contractor is required to include the substance of this clause *in all subcontracts, and each subcontractor must flow the clause down to the next tier*.'' 78 Fed. Reg. 69277 (emphasis added).

Higher tier contractors cannot rely upon the formality of flow down in contract boilerplate to satisfy their obligations under the clause. The obligations of a contractor covered by the clause include reporting of cyber incidents that occur not only on UCTI on its own system but also UCTI on ''its subcontractors' unclassified information systems.'' DFARS 252.204-7012(d)(2)(i).

Implementation of Measures to Protect 'Controlled Technical Information.' If a contractor receives a contract subject to DFARS 252.204-7012, it must implement the requirements of the clause when ''controlled technical information'' is present on the contractor's information system. ''Controlled technical information,'' defined at DFARS 204.7301k includes technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Examples could include technical data, computer software including executable code and source code, engineering data, drawings, associated specifications, data sets, and studies and analyses. The FAQs explain that the government often equates technical information with intellectual property. DOD takes a very broad view of what is to be protected; as stated in the FAQs:

> The government views technical information as any technical data or computer software that can be used in the design, production, manufacture, development, testing, operation, or maintenance process of goods or materiel; or any technology that advances the state of the art in an area of significant military applicability to the United States. Defense contractors view any such data or software created by them as intellectual property. Defense contractors should be willing to take the steps necessary to protect their own intellectual property which will ultimately mean better protection of technical information.

This elaborates upon and underscores the previous point. DOD sees a convergence of its interest and the business interests of its contractors in improving basic cybersecurity. DOD is using the UCTI rule to protect not only DOD's CTI but also the valuable IP of its contractors. The FAQs also show that it is DOD's intent to protect its supply chain from ''end to end,'' i.e., from design through manufacture. These propositions should be considered carefully by *every* contractor in the defense supply chain.

Identification of 'Controlled Technical Information.' Ordinarily, CTI is to be ''marked with one of the ''distribution statements B-through-F,'' in accordance with DOD Instruction 5230.24, Distribution Statements on Technical Documents.'' This refers to five categories of permitted distribution, namely to U.S. government agencies

  FCR ISSN 0014-9063

only (B), to U.S. government agencies and their contractors (C), to DOD and U.S. DOD contractors only (D), to DOD Components only (E) or ''only as directed'' by the controlling DOD office or higher authority (F).

After promulgation last November, some analysts were unsure of whether *all* CTI must be designated with a distribution statement as determined by a DOD component or whether a contractor might have independent responsibility to so designate. This has been clarified by the FAQs. The ''controlling DOD office'' (in most cases the requiring activity) is responsible to determine whether information furnished to the contractor by the Government is CTI. This means that, in most cases, contractors will be informed specifically by their customer (or the prime) when CTI is present that requires protection. However, the FAQs also recognize that under many contracts, the *contractor* will develop unclassified CTI in the performance of the contract. In this situation, the requiring activity and Contracting Officer are to include in the Statement of Work specific requirements as to the marking of technical data and the application of distribution statements. These obligations can extend both to contractual deliverables (e.g., specifications and engineering documents) as well as to ''internal'' work product of contractors (such as test plans and reports).

Strictly speaking, the UCTI requirements apply only to contractor systems that host or transmit information that is designated as CTI. A contractor, in theory, could have one network system that employs the necessary cyber controls, while not applying similar measures to other enterprise systems. Caution is in order, however. If an enterprise network enables users to retrieve UCTI from one system and communicate it to recipients on another system, then the minimum cyber measures would apply to both systems. Similarly, care must be taken to prevent inadvertent extraction of UCTI information and use outside protected systems – as could occur, for illustration, if a company employee downloads UCTI to a memory stick and then works with that data on a home computer. Access through mobile devices also must be assessed from a security standpoint.

Safeguarding UCTI. The security controls required by DFARS 252.204-7012(b) are taken from NIST Special Pub. 800-53. These controls are designed to be ''policy and technology-neutral'' and ''focus on the fundamental safeguards and countermeasures necessary to protect information.'' NIST 800-53 states more than 300 potentially applicable security controls, allocated to fourteen functional areas (e.g., ''Access Control,'' ''Audit and Accountability,'' ''Incident Response,'' ''Risk Assessment,'' etc.). Reflecting the proposition that the UCTI regulations impose a basic level of cyber assurance, only 51 of the NIST controls are required to satisfy the ''minimum security controls for safeguarding'' under the UCTI rule. *See* Table 1 to DFARS 252.204-7012(b). DOD's contractors are to provide ''adequate security'' to safeguard UCTI, which is defined as ''protective measures that are commensurate with the consequence and probability of loss, misuse, or unauthorized access to, or modification of information.'' DFARS 252.204-7012(a) (emphasis in original).

The FAQs make clear that ''a degree of flexibility is provided'' to contractors in defining how to implement the controls. In fact, the regulation, while it encouraged adoption of the listed controls, explicitly recognizes that some controls may be inapplicable and enables contractors to adopt alternative protective measures. *Id.* at 7012(b)(1)(ii). At the same time, contractors are cautioned not to believe their obligations are necessarily limited to initial implementation of minimally sufficient measures. The regulation obligates contractors to apply other (i.e., additional) information systems security requirements if reasonably necessary in a ''dynamic environment based on an assessed risk or vulnerability.'' *Id.* at 7012(b)(2). While this will implies continuing uncertainty as to what level of controls are sufficient, it corresponds to real world experience that shows, time and again, the shifting and unpredictable nature of cyber threats and constantly changing particulars of cyber defenses.

The DFARS rule makes provision of ''adequate security'' a contract requirement. But there is no obligation imposed on any contractor to submit its system controls for review or seek or receive CO approval. Indeed, there is no oversight mechanism, as such. Consequently, it is sufficient for contractors to engage in good faith efforts to implement the minimum controls, or adopt and be prepared to justify alternate methods. In the event of a cyber incident, however, they should expect scrutiny of their controls. Contractors should know of the consequences of failure to implement the required controls, apart from the loss or compromise of CTI and contractor IP. As stated in the FAQs:

> The DFARS rule did not add any additional requirement for the Government to monitor contractor implementation on the required security controls because this is a decision that should be made at the agency level. *Failure to implement the controls to protect CTI that is resident on or transiting through contractor unclassified information systems would be a breach of contract*.

(Emphasis added.) The consequences of such a breach, conceivably, could include liability to the Government (or a higher tier contractor) for damages, termination for default, or even (potentially) exposure to an action under the False Claims Act.

Reporting Cyber Incidents. DFARS 252.204-7012(d)(1) require reporting within 72 hours of discovery of a cyber incident. It will be critical for a contractor to have in place protocols and procedures that enable it to quickly compile and organize information once a cyber incident has been detected. The FAQs inform DOD contractors of the expected reporting mechanism. A cyber incident is to be reported by an ''Incident Collection Form'' (ICF) submitted by the DIBNet portal at http://dibnet.dod.mil. In order to access this form, a contractor must have a DOD-approved medium assurance public key infrastructure (PKI) certificate, as can be obtained by contacting the DOD Cyber Crime Center (DC3). Contractors are instructed to report what they know within 72 hours of the event, even if the information is incomplete. Contractors also are responsible to assure that their subcontractors report incidents *to the prime* as it is the prime's responsibility to submit an incident to DOD within 72 hours of receiving notice of any cyber incident. DOD's DC3 unit is designated as being the ''DOD operational focal point'' receiving cyber threat and incident reporting from contractors subject to this DFARS contractual requirement.

Proper reporting does not create a ''safe harbor'' as to cyber incidents, although the rule provides that proper reporting of such an incident shall not, by itself,

be interpreted as evidence that the contractor failed to provide adequate information safeguards. DFARS 204.7302(b)(2). Compliance will be measured at the time that a cyber incident is reported. *Id*. Accordingly, this regulation is not one where contractors are assured of any ability to obtain ''pre-clearance'' or other advance approval. Nor can they anticipate routine oversight. Scrutiny will be event-driven – but the likelihood of a cyber incident must be regarded as high in the contemporary environment. Accordingly, every company that is or plans to be in the defense supply chain, and that knows or expects it will receive, use or transmit CTI, is well advised to: (i) implement at least the basic NIST 800-53 controls, or equivalent; (ii) take measures to be informed continuously of changes to cyber threats; (iii) regularly update firewalls and other defenses; and (iv) have in place protocols and procedures to report any incident. The UCTI rule seeks to improve the minimum security measures of DOD's entire supply chain, and to improve reporting of threats and events, but DOD authorities are well aware that it is all but impossible to completely eliminate the risk of cyber attack or compromise.

Extension of Minimum Cybersecurity Measures to Other Federal Agencies. The UCTI regulations apply only to DOD contracts and the DOD supply chain. Other federal agencies soon may employ similar requirements in their acquisition regulations. Executive Order 13556, issued on November 4, 2010, sought to establish a ''uniform program for managing information that requires safeguarding or dissemination controls.'' Executive Order 13636, issued on February 12, 2013, directed federal agencies to provide stronger protections for public and private sector cyber-based systems that are critical to national and economic security. Under Section 8(e) of EO 13636, GSA and DOD established a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition.

On November 18, 2014, the National Institute of Standards and Technology (NIST), a unit of the Department of Commerce, released for comment a draft of Special Publication 800-171 (''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations''). SP 800-171 is available at http://csrc.nist.gov/publications/drafts/800-171/sp800_171_draft.pdf. SP 800-171 states that the protection of sensitive unclassified federal information, while residing in ''nonfederal information systems,'' is ''of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its operations.'' ''Nonfederal information systems'' include those operated by federal contractors to process, store and transmit sensitive federal information to support the delivery of products and services to federal customers.

SP 800-171 seeks to clarify identification of ''controlled unclassified information'' and relies upon NIST 800-53 both for security assessment and for basic controls as well as more elaborate ''derived security requirements.'' A purpose of SP 800-171 is to achieve consistent use of these controls throughout the Executive branch, and the ''Executive Agent'' responsible for controlled unclassified information anticipates establishing a single FAR clause that, among other attributes, will apply the requirements of NIST 800-171 ''to the contractor environment.''

While only proposed, and while the related FAR clause has not yet been released for comment, NIST 800-171 is a clear signal that the Executive branch intends to apply a minimum set of cybersecurity controls broadly to all acquisition requirements. As is true of the DFARS rule, the stated purpose of the NIST initiative is to protect sensitive federal information, while a collateral purpose, albeit unstated, is to elevate the minimum cyber assurance of thousands of companies that furnish supplies and services to federal customers.

Conclusion. There are some companies and some industries that believe that the free market should be trusted to take adequate measures to protect against cyber threats. Recent events, such as the hack of Sony Pictures, remind us of the potentially devastating impact of cyber attacks on commercial enterprises. The federal government has vital interests to protect the national infrastructure and the U.S. industrial base. When controlled technical information is resident on contractor information systems, the federal government has interests that justify insistence that its contractors apply at least minimum cyber assurance controls. Use of acquisition measures to elevate cyber assurance among government contractors will come at a cost, but events prove there is no room for argument that vigilant cybersecurity is necessary to protect the public interest in the operation of federal systems. Companies have a choice to make. Those who intend to continue as federal contractors will find they must adopt basic cyber controls, improve these continuously as threats and defenses evolve, and that they must participate in federally organized reporting of cyber events.

  FCR ISSN 0014-9063