VENABLE LLP

government contracts update

January 2014

Please contact the authors below if you have questions regarding this alert.

Authors:

Rebecca E. Pearson
repearson@Venable.com
202.344.8183

Keir X. Bancroft
kxbancroft@Venable.com
202.344.4826

Anna E. Pulliam
aepulliam@Venable.com
703.905.1457

Time to Comply: New DoD Rules Governing Supply Chain Risk Information and Unclassified Controlled Technical Information

Government contractors should be aware of recent Department of Defense (DoD) rules governing Information Relating to Supply Chain Risk, 78 Fed. Register 69,268 (Nov. 18, 2013) and Unclassified Controlled Technical Information, 78 Fed. Register 69,273 (Nov. 18, 2013). The two key implications of the rules for Government Contractors are:

- Contractors may be removed from information technology procurements supporting national security systems for failure to satisfy standards related to supply chain risk, and in some cases they will be unable to protest their removal; and
- Contractors must safeguard unclassified controlled technical information (UCTI) and take quick action to report and investigate "cyber incidents" having an actual or potential adverse effect on UCTI.

Though contractors **have until January 17, 2014 to comment** on the interim rule on safeguarding UCTI, the rules are presently in effect and apply to procurements of both commercial and noncommercial items. This update gives a summary of the rules and their implications for government contractors.

Supply Chain Risk Information Requirements

Section 806 implementation

The DoD's interim rule, "Requirements for Information Relating to Supply Chain Risk," implements Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year 2011 authorizing DoD officials to restrict certain sources of supply from information technology procurements supporting national security systems if they pose supply chain risk. Section 806 defines supply chain risk as a risk that:

> *"An adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system*."

Authority to exclude sources of supply

Under a DoD pilot program authorized by Section 806, the Secretaries of Defense, the Army, the Navy, the Air Force, or a limited number of designees may mitigate supply chain risk by:

- Excluding sources of supply from covered procurements if they fail to meet qualification standards established in accordance with 10 U.S.C. § 2319;
- Excluding any source of supply that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals; and
- Withholding consent for a contractor to subcontract with a particular source or supply, or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

In determining whether to take these actions, the authorized officials may consider public and non-public information, including all-source intelligence, relating to an offeror and its supply chain.

Information withholding authorized

The interim rule lacks clarity as to what "qualification standards" or "evaluation factor" sources of supply must satisfy to comply with the rule. Contractors may want to consult FAR 9.2, Qualifications Requirements, for details on how agencies currently implement qualifications requirements under Section 2319. However, authorized officials may limit disclosure of information relating to the basis for excluding certain sources of supply from procurements under the interim rule. In such cases, these actions are not subject to review before the Government Accountability Office or any federal court. These officials are also required to communicate with other federal agencies about other procurements that may be subject to the same supply chain risk.

Applicable to IT procurements supporting national security systems

Though the rule will be applied to a specific subset of national security systems, all DoD components are required to incorporate DFARS Clause 252.239-7017, Notice of Supply Chain Risk, *in all solicitations involving the development or delivery of any information technology* – whether acquired as a service or as a supply – including commercial item procurements, falling both above and below the simplified acquisition threshold. The national security systems under the interim rule:

- Support intelligence activities; cryptologic activities related to national security; the command and control of military forces; and equipment integral to weapon or weapons systems;
- Are critical to direct fulfillment of military or intelligence missions (but do not include systems used for routine administrative and business applications);
- Are protected as classified by Executive Order or an Act of Congress in the interest of national defense or foreign policy.

Tips for contractors

Contractors providing information technology supplies or services should consider the following:

- Contractors are required under the interim rule to "maintain controls in the provision of supplies and services to the Government to minimize supply chain risk."
- Agencies may consider all sources of information in determining supply chain risk; contractors should therefore perform diligence to ascertain if they might trigger a supply chain risk.
- Contractors should perform due diligence on supply chain subcontractors, which may be individually excluded from national security system information technology procurements.

Consider submitting written comments on the rule, which are due by January 17, 2014.

Safeguarding Unclassified Controlled Technical Information

Contractors must also comply with the DoD's final rule requiring the safeguarding of unclassified controlled technical information that is either resident on or transiting through contractors' unclassified information systems. DoD defines UCTI as technical data or computer software with military or space application that the Department has marked as controlled in accordance with DoD Instruction 5230.24, which covers Distribution Statements on Technical Documents.

Required preventative security measures

Under the rule, a contractor must enact safeguards to provide "adequate security" to its project, enterprise, or company-wide unclassified information technology systems to prevent compromise of UCTI. The DoD adopts information security controls prescribed by the National Institutes of Standards and Technology (NIST) as a baseline for ensuring adequate security. Under the rule, a contractor can choose from among the following options:

- Implement specific security controls and methodologies set forth in NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations;
- Convince the DoD that some or all of the specified SP 800-53 security controls are inapplicable; or
- Demonstrate that the contractor has applied alternative and equivalent security measures.

To ensure adequate security, DoD requires that contractors use "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." To that end, if a contractor determines additional security measures beyond the SP 800-53 or equivalent controls are necessary, they must be applied.

Cyber incident reporting requirements

The rule requires contractors to report any "cyber incident" that results in an *actual or potentially adverse effect* on an information system or the information residing on it. A cyber incident includes any exfiltration (including the unauthorized release or copying of data), manipulation, other loss or compromise of UCTI on a contractor or its subcontractor's systems. Contractors must also report any unauthorized access to systems on which UCTI resides.

- Within 72 hours of a cyber incident, a contractor must report to DoD a number of details, which include:
- The type of compromise (for example, unauthorized access or inadvertent release);
- Contracts and DoD programs affected;
- Identification of the technical information compromised;
- The name and CAGE code of the subcontractor if this was an incident on a subcontractor network;
- Date and location of the incident; and
- Any additional pertinent information.

It is important to note that the rule mandates reporting regardless of whether a cyber incident has an actual or a possible adverse effect on UCTI. This language indicates contractors will have to submit reports to DoD within the 72 hour window even if they have not been able to confirm whether there was an actual exfiltration or compromise of UCTI.

Damage assessment support

After reporting a cyber incident, the contractor must also support the DoD's damage assessment by identifying the specific computers, information systems, and UCTI compromised. For at least 90 days from the date of the cyber incident, the contractor must preserve and protect images of known affected information systems and all relevant monitoring or packet capture data so the DoD may use it if it elects to conduct a damage assessment.

Subcontractors and outsourced IT infrastructure

The rule applies equally to subcontractors; DoD mandates the substance of the UCTI safeguarding requirements be flowed down to subcontracts, even those involving commercial items. In fact, the DoD clarified when promulgating the final rule that IT infrastructure services such as Internet Service Providers (ISPs) and cloud service providers will count as subcontractors for purposes of compliance with the rule. 78 Fed. Register 69,274.

Assessing compliance; no safe harbor provisions

The rule states that the contracting officer, after consulting with a "security manager" of a requiring activity will assess a contractor's compliance with the rule in the event of a cyber incident. The rule clarifies that though the report of a cyber incident is not enough in itself to constitute evidence that the contractor failed to provide adequate information safeguards for UCTI, or otherwise failed to comply with the rule, it will be considered as part of the contracting officer's overall assessment of the contractor's compliance with safeguarding requirements. DoD also states in the discussion and analysis of the rule that audits or reviews of contract compliance will be conducted at the discretion of the contracting officer in accordance with the terms of the contract. 78 Fed. Register 69,274. The DoD also clarifies that it does not intend the reporting obligation to constitute a safe harbor statement. *Id*. at 69,278.

Defining UCTI and prescribing marking requirements

The DoD re-scoped its rule by focusing on controlled *technical* information. Earlier proposed rules were applicable to the more general category of controlled unclassified information (CUI), but DoD focused on controlled technical information, which it "determined to be of utmost importance and which DoD has existing authority to protect." 78 Fed. Register at 69,274. DoD defines "controlled technical information" as:

> *"Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, or dissemination."*

DoD elaborates in its rule that controlled technical information is marked in accordance with distribution statements B through F under DoD Instruction 5230.24, Distribution Statements on Technical Documents, and expressly excludes from its definition information that is *lawfully publicly available without restrictions*. The rule also further defines the term "technical information" as technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data – Non Commercial Items, and clarifies those definitions apply regardless of whether or not the clause is incorporated in the solicitation or contract. Some examples of technical information include:

- research and engineering data
- engineering drawings and associated lists
- specifications
- standards
- catalog-item identifications
- data sets
- studies
- analyses

- process sheets
- manuals
- technical reports and orders
- computer software executable code
- source code

Applicable to all solicitations and contracts

The requirement at DFARS 204.7303 specifies that the new clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, must be used in all solicitations and contracts, including contracts for commercial items. Thus, contractors should be mindful that any new DoD procurements will include this requirement.

Tips for contractors

Any contractors hosting UCTI on their servers, or that may have UCTI transiting through their servers, or have subcontractors or IT infrastructure providers doing the same, should consider the following:

- The rule applies to information systems at the project, enterprise, or business level. Contractors must accurately assess the scope of systems with which UCTI will have any contact; that will help clarify the information systems against which this rule applies. The scope of information systems in question will likely contribute to the allowability of compliance costs. The DoD stated in its discussion and analysis of the rule that "this contract requirement will be spread across and benefitting multiple contracts" and as a result "costs associated with implementation will be allowable and chargeable to indirect costs pools." 78 Fed. Register at 69,275. That being the case, contractors should consider the cost of project-scoped information systems, as the DoD stated that it "does not intend to directly pay for the operating costs associated with the rule."
- The rule applies to subcontractors and third-party IT infrastructure providers; contractors should be sure their subcontracts and service agreements reflect all of the DoD's UCTI requirements.
- The rule requires reporting cyber incidents that have actual or potential adverse effects on UCTI; contractors must be prepared to notify their clients within 72 hours of a cyber incident, even if they have not confirmed there were actual adverse effects on UCTI.
- The rule requires contractors to provide a significant amount of assistance to DoD in identifying and assessing the effects of a cyber incident; contractors should be sure they have the resources available to satisfy these requirements in the months following a cyber incident.

If there is any doubt, contractors should seek confirmation with a contracting officer as to whether a certain type of information falls within the category of UCTI. A contracting officer, with the assistance of only a "security manager" whose responsibilities and authority are not clarified under the rule, has a great deal of discretion in determining if a contractor complied with the requirements under this rule. Thus, contractors should be proactive with their contracting officer to determine the boundaries of compliance.

For assistance in determining how these regulations might impact your business, please contact **Becky Pearson** at repearson@Venable.com, **Keir Bancroft** at kxbancroft@Venable.com, **Anna Pulliam** at aepulliam@Venable.com, or any of the other attorneys in Venable's **Government Contracts Practice Group**.