PATTON BOGGS LLP

September 4, 2012

New FAR Clause Establishes Minimum Data Security Requirements for Federal Contractors

Government Contracts Law Client Alert

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the author listed below.

Mary Beth Bosco
mbbosco@pattonboggs.com

WWW.PATTONBOGGS.COM

With Congress unable to pass cybersecurity legislation by the August recess, the executive agencies are proceeding to regulate government contractors with access to government information. Specifically, on August 24, 2012, the Federal Acquisition Regulation (FAR) Council proposed a new clause requiring contractors to maintain minimum data protection standards. Comments on the proposal are due October 23, 2012. As explained below, GSA already has in place cybersecurity standards for its contractors, and DoD has proposed its own set of rules. These specific agency rules take precedent over this new FAR clause.

Once final, the new FAR clause will apply to civilian, DoD and NASA contracts exceeding the simplified acquisition threshold ($150,000), including commercial acquisitions. The clause must be flowed down to subcontracts at any tier. The new clause, which will be in FAR Part 52.204, identifies seven basic safeguards for contractor information systems through which nonpublic information generated by or for government either resides or transits. The basic safeguards are:

1. Government information may not be processed on computers without access control or located in public areas. Similarly, government information cannot be posted on a public website. If posted to a web site, the site must control access either through user identification or password, user certificate or other technical means, and must provide protection via use of security technologies.

2. Electronic information may be transmitted only on systems that utilize technologies and processes that provide the best level of security and privacy available, given facilities, conditions and environment.

3. Transmission by voice or fax may only occur when the sender has a reasonable assurance that access is limited to authorized recipients.

4. Systems must be protected by at least one level of physical barrier and one level of electronic barrier, such as lock and key in conjunction with a password, when not in the direct control of the individual user.

5. Media that is being released or discarded must be cleared and sanitized. Overwriting is an acceptable method of sanitizing, and the clause refers to the National Institute of Standards and Testing's (NIST) protocols for clearing computers. NIST Publication 800-88, Guidelines for Media Sanitization.

6. The contractor must provide at least the following means of intrusion protection: Current and regularly updated malware protection, such as anti-virus software and anti-spyware software; and prompt application of security-related upgrades and patches.

7. Information may only be transferred to those subcontractors with a contractual need to have the information and who employ the safeguards described in the clause.

While the clause's requirements are very general, covered contractors will need to review not just their hardware and software systems, but their facilities, employee practices, record-keeping systems, and subcontract relationships in order to ensure compliance. For example, contractors should make sure they have policies in place so that employees working from home comply with the clause's security requirements.

In addition, government contractors must be aware that GSA already has more fulsome cybersecurity regulations in place, and that DOD has proposed a comprehensive set of rules. In brief, GSA's regulations require contractors to have an IT security plan for each contract that is approved by the Contracting Officer. Contractors must also supply evidence of either a self or third-party-certified security authorization, the components of which are defined by GSA's regulations. The regulations also contain notification requirements for cyber breaches and GSA inspection rights.

DOD's proposal mandates reporting of cyber incidents affecting designated DOD information within 72 hours of discovery. In addition to incident reporting, contractors will need to take immediate action to support forensic activities. These actions include an immediate review of the system to identify compromised computers, servers and user accounts; identification of the specific DOD information that has been affected; and preservation of the known affected systems and any corresponding capture data. In the event DOD determines to perform its own damage assessment, the contractor will be required to comply with all information requests and cooperate with DOD's investigation. The DOD regulations are not expected to become final before the end of the year.