PATTON BOGGS LLP

April 12, 2012

Government Contractors Now Subject to Cybersecurity Regulations – And More are on the Way

Government Contracts 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 authors listed below.

Mary Beth Bosco
mbbosco@pattonboggs.com

WWW.PATTONBOGGS.COM

I. INTRODUCTION

Congress currently is considering various cybersecurity bills. While Congress debates cyber legislation, the executive agencies are adopting regulations governing how government contractors handle contract-related information either residing on or transiting through their computer systems.

As described below, if your company contracts with the General Services Administration (GSA), and has access to government information, you may already be required to have an IT security plan and to be a certified provider. Department of Defense (DOD) contractors should expect even more stringent regulations to be finalized in 2012, which could restrict even a company's internal access policies and practices.

This memorandum provides an overview of the regulatory scheme imposed on GSA contractors and previews the requirements expected to be implemented by DOD. If requested, we would be happy to provide additional detail on the regulatory requirements.

II. GSA CURRENT AND DOD PROPOSED REGULATIONS

A. GSA Cybersecurity Regulations

In January of this year, GSA finalized its June 2011 interim cybersecurity rules. These regulations apply to GSA contracts for IT supplies, services or systems which involve physical or electronic access to non-classified government information supporting the mission of GSA. If you have a GSA IT contract, and you are provided information by the agency or have access to GSA information, you are covered by the regulations, as are your subcontractors. The new rules require contractors to maintain government-approved security plans, and to possess a security authorization. These provisions are summarized below.

1. Contractor IT Security Plan

The first GSA requirement is preparation of an IT security plan for each contract. This plan must be submitted to the contracting officer for approval within 30 days of contract award, and must comply with the Federal Information Security Management Act of 2002 and the E-Government Act of 2002. The approved plan will be incorporated as part of the contract.

In addition to the basic IT security plan, GSA contractors are now required to maintain a continuous monitoring strategy. The strategy must provide (a) a configuration management process for the information system and its constituent components; (b) a

means to make determinations of the security impact of changes to the information system and environment of operations; (c) ongoing security control assessments in accordance with the organizational continuous monitoring strategy; (d) regular reporting requirements as to the security state of the information system to designated GSA officials; and (e) a description of the continuous monitoring support systems and applications.

2. Security Authorization

Within six months of receipt of a covered contract, GSA contractors must submit proof of IT security authorization in accordance with National Institute of Standards and Testing (NIST) Special Publication 800-37. Contractors can "self" authorize or use a third-party verifier. The authorization document must include a final security plan, risk assessment plan, security test and evaluation plan, and a disaster recovery and continuity of operations plan. Once approved by the contracting officer, the security authorization document becomes part of the contract requirements, and contractors will be required to submit annual verifications of compliance.

3. Notice and Access Requirements

Under the new GSA regulations, contractors must notify GSA each time an employee with access to GSA information systems or data leaves or is hired. Contractors are also required to have procedures in place for immediate cancellation of system access rights for terminated employees. Finally, the regulations provide for GSA access to contractor and subcontractor personnel, operations, and IT systems for the purpose of inspection, investigation or audit relating to compliance with the cyber regulations.

B. DOD's Proposed Cybersecurity Regulations

In June of 2011, DOD published a proposal for cybersecurity regulation. DOD accepted comments on its proposal through November 2011, but has not yet issued final regulations. They are expected to come out later this year. The DOD proposal covers non-public, non-classified DOD information resident on or transitioning through a contractor's information systems. The proposed rules divide this information into two subsets, with different security measures applicable to each.

1. "Basic" Information Covered by DOD's Proposed Regulations

The first category of information is "basic" DOD information, which is defined as information that has been provided by DOD or is used or generated in support of a DOD activity. The information must be "nonpublic," which means (a) it is either exempt from disclosure under the Freedom of Information Act (FOIA), or (b) it has not been disseminated to the general public and DOD has not made a determination that the information is releaseable. In other words, unless DOD has specifically authorized a contractor to release information, or the information would not be protected by FOIA, the contractor will be required to treat the information in accordance with DOD's rules.

2. Safeguarding "Basic" Information

Absent DOD's determination that information is releasable, and with certain exceptions for audits and investigations, the proposed rules preclude contractors from releasing even basic level information outside of their organizations or to employees who do not have a right to know the information. Subcontractors will also be subject to these same

restrictions. This general prohibition has the potential to result in costly changes to the structure of company email, intranet, and other data sharing systems. The proposed regulations further contain these specific mandates:

a. Contractors cannot process government information on publicly-accessible computers or on company computers that do not have access control.

b. Contractors' electronic transmission systems must provide "the best level of security and privacy available, given facilities, conditions, and environment."

c. Voice data may only be transmitted when the user has reasonable assurance that access is limited only to authorized recipients.

d. When information is not being accessed, it must be protected by at least one physical barrier (e.g., lock or password).

e. Contractors must have procedures to clear information from devices before they are released or discarded.

f. Contractors must have minimum intrusion protections, including regularly updated malware and prompt application of security-related patches and upgrades.

g. Finally, contractors may only transfer covered data to subcontractors with a need to know the information and who employ the safeguards listed above.

3. "Enhanced" Information

The second category of information is "enhanced" information, which includes information designated by DOD as critical, information subject to the export control laws, information subject to DOD-specific FOIA directives, information designated as controlled information (such as "Official Use Only"), personal identification information, and certain technical data. If data falls within these categories, contractors must implement enhanced security requirements in addition to those described above for basic data. To constitute enhanced protection, a contractor's security program will need to comply with the standards set forth in NIST Special Publication 800-53. In the alternative, a contractor may prepare a written submission describing either why the NIST standard is inapplicable or how the contractor's systems meet the NIST requirements through other means. Additionally, contractors handling enhanced data will be required to use DOD-approved identity credentials for accessing the information.

4. Cyber Incident Reporting for Enhanced Information

DOD's proposal mandates reporting of cyber incidents affecting DOD information within 72 hours of discovery. Cyber incidents include data exfiltration or manipulation or other loss or compromise, or unauthorized access to a system on which DOD data resides or is transiting. 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.

III. CONCLUSION

At a minimum, GSA's cyber regulations and DOD's proposal will require affected contractors to review their IT security procedures to ensure they match the respective agency's requirements. In some cases, these rules may result in substantial changes to company IT policies and operations. While the DOD regulations are not yet final, proactive review of contractor IT policies and procedures may be warranted in order to accomplish a more orderly and less compressed path towards compliance once the rules are published.