PATTON BOGGS LLP

May 16, 2012

DoD Implements Broad Cybersecurity Information–Sharing Program

Cybersecurity 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

On May 11, 2012, the Department of Defense (DoD) published an interim final rule expanding its pilot program institutionalizing the sharing of cyber threat information between DoD and its contractors. Comments on the rule are due on July 10, 2012. The following description of the rule outlines the basics of the program, the benefits of participation, the eligibility requirements, and the program mechanics.

What is the Basic Purpose of the Program?

DoD's program establishes a bilateral cybersecurity information sharing activity among Defense Industrial Base (DIB) government and industry stakeholders. As part of the program, DoD will provide cyber threat information and information security best practices to participating companies in order to improve their abilities to safeguard information. For their part, participating companies are to report cyber intrusion incidents to the Defense Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment (DCIS). DCISE will analyze these reports to accumulate information regarding cyber threats and vulnerabilities, and develop effective response measures which DCISE will share with participating companies. In addition to this initial reporting and analysis, DoD and the reporting company may pursue, on a voluntary basis, more detailed, digital forensics analysis or damage assessments of individual incidents.

What are the Benefits of Participation?

Participation in the program is voluntary. Large defense contractors, such as Lockheed Martin, participated in the smaller, pilot DoD program and have announced they will participate in the expanded program.

A DIB program participant will have access to DoD's experience in and resources for predicting and countering cyber attacks and to industry lessons learned. The rule sets out procedures for protecting contractor data on cyber breaches, thus allowing DoD to share on a non-attribution basis the experiences of other contractors, and best practices for detecting, preventing, and minimizing the risks and damage from cyber attacks. Accordingly, the most obvious benefit of program participation is access to both DoD and industry cyber threat assessment, prevention, and mitigation information. This benefit, however, will come with a cost of implementation and a reporting requirement. There is also the open question of potential liability or claims based on a participating company's determination not to implement best practices which it becomes aware of through the program.

Who is Eligible and What Information is Covered?

To be eligible for the program, a company must have a facility clearance approved to handle at least secret information. The DIB company also must possess two or more DoD-approved assurance certificates to allow the sharing of unclassified data with the government, obtain a DoD Communications Security (COMSEC) account, and follow other protocols to be able to access and share data with the government.

The data covered by the program includes technical information as designated by DoD, export-controlled information, critical program information, personally identifiable information, information that could be assembled by hostile intelligence systems, nonclassified controlled information (such as information marked as "For Official Use Only"), and information protected from release by the Freedom of Information Act. If your company's IT system collects, develops, receives, transmits, uses or stores this type of information, and you meet the other criteria described above, you are eligible for the DIB program.

How Does the Program Work?

Once accepted in the program, contractors will be required to report cyber incidents to DoD within 72 hours of their occurrence. Once advised of the incident, DoD may choose to perform a cyber damage assessment report and work to develop the means to minimize the damage and prevent future similar incidents. On a non-attribution basis, DoD may also provide the information it develops concerning the nature, scope, prevention and mitigation of the cyber attack to other program participants ("Government Furnished Information" or "GFI").

Because the DIB program is premised on the exchange of information between DoD and its contractors, DoD's interim final regulations focus on data protection. First, DIB contractors may only use GFI to safeguard information on covered DIB systems that are U.S.-based and may only share GFI with U.S. citizens within their organization. If a DIB contractor uses a third-party service provider (SP) for information system security systems, DoD must approve the SP. The approved SP will be required to enter into an agreement with the DIB contractor to be bound by all applicable DIB program requirements.

Second, the government acknowledges that information shared by DIB participants may include extremely sensitive proprietary, commercial, or operational information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the DIB participant that reported that information. Accordingly, the government commits to restrict its internal use and disclosure of attribution information to government personnel and government support contractors that are bound by appropriate confidentiality obligations and restrictions relating to the handling of the sensitive information.

In further recognition of the protections to be given the shared information, DoD and each DIB participant must enter into a Standardized Framework Agreement (FA) which will memorialize the procedures set forth in the new rule and the means of protecting the exchanged information.

Participation in the DIB program is voluntary and does not obligate the participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Thus, there is no requirement for a DIB contractor to change its IT systems based on information concerning threat protection it receives under the program. This discretion raises an interesting question: If a cyber breach occurs after a participating company receives GFI containing best practices for breach protection and chooses not to implement the best practices, will any third-parties – such as employees, consumers, or shareholders – be able to use the non-implementation choice against the company? This is an open question, and one which should be weighed when a company considers whether to participate in the DIB cyber program.