wiley

ALERT

DoD Enhances Industrial Base Cybersecurity Information Sharing

May 14, 2012

On Friday, May 11, the Department of Defense (DoD) issued an interim final rule to enhance its defense industrial base (DIB) cybersecurity voluntary disclosure program. *See* Department of Defense (DOD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (SC/IA) Activities, 77 Fed. Reg. 27615 (May 11, 2012). The interim rule implements procedures to facilitate information sharing between eligible DIB companies and DoD's Cyber Crime Center, which is the Department's lead agency for cyber-investigations and analysis. In particular, the interim rule will allow DoD to share cyber-threat information about network intrusions that could compromise critical DoD programs and missions, including information "to address sophisticated cyber threats that represent an imminent threat to U.S. national security and economic security interests."

The interim rule acknowledges previous limitations on DoD's ability to share threat information with eligible DIB companies, which are attributed to the highly sensitive, proprietary and sometimes classified nature of DoD's threat information. The "one-way" flow of information under the existing framework of the voluntary disclosure program, however, largely prevented DIB companies from receiving real-time, actionable information about cyber threats and mitigation strategies. DoD expressed concern that without this information, "DIB companies' ability to protect [DoD] information cannot be fully effective" and the government "faces an elevated risk that critical program information could be compromised, resulting in potential economic losses or damage to U.S. national security."

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Ethics Advice & Compliance Audits and Plans

Government Contracts

Patent and Data Rights Counseling and Disputes

Under the interim rule, which will be implemented in 32 C.F.R. Part 236, eligible DIB companies will be able to enter into "Framework Agreements" with the government that will enable them to receive both classified and unclassified cyber-threat information and information assurance practices. In turn, recipients would be limited to sharing that information with U.S. citizens on a need-to-know basis within the company, and restricted to using such information only to safeguard "covered defense information" on domestic "covered DIB systems." Any broader use or dissemination of shared government information would require government authorization.

It remains unclear how the government will implement the information-sharing procedures, while at the same time adequately protect the confidential and proprietary nature of threat information that is voluntarily disclosed to DoD by other DIB companies. The interim rule acknowledges "that information shared by the DIB participants under this program 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." While the government pledges to "take reasonable steps to protect against the unauthorized use or release of such information," and intends to share only "non-attribution information" that will not directly or indirectly identify the DIB participant first reporting the information, the interim rule provides little insight into the process that the government will use to determine what information is suitable for release. Once information is shared with a DIB company, the Framework Agreement between the company and the government likely will include non-disclosure covenants that reflect the procedures outlined in the interim rule.

The website devoted to the program, http://dibnet.dod.mil/ is already up and running. Comments on the interim rule must be submitted by July 10, 2012.