Published by *Privacy Law360* on October 28, 2013. Also ran in *Aerospace & Defense Law360, Government Contracts Law360, Public Policy Law360* and *Technology Law360*.

Cybersecurity Program Will Help Defense Industrial Base

--By Ronald Lee, Lauren Schlanger and Nicholas Townsend, Arnold & Porter LLP

Law360, New York (October 28, 2013, 6:31 PM ET) -- The U.S. Department of Defense has published a final rule implementing its Voluntary Cyber Security and Information Assurance (CS/IA) Activities for Defense Industrial Base (DIB) companies.[1]

The DIB CS/IA program is designed to enhance DIB participants' ability to defend against cyber intrusions on their networks through voluntary information sharing between the government and DIB companies. Companies that voluntarily participate in the DIB CS/IA program receive threat intelligence and technical assistance from the DOD that allows them to better recognize and repel cyber attacks based on compiled patterns regarding attack vectors and hacking trends. As of September 2013, nearly 100 defense contractors with facility security clearances had signed up for the program. Cleared companies that qualify to participate in DIB CS/IA must sign a framework agreement with the DOD after they enroll for the program online at http://dibnet.dod.mil/.

The DOD expanded its voluntary DIB CS/IA program from the original pilot program through the issuance of an interim final rule in May 2012 and invited the public to submit comments.[2]

The final rule makes few changes to the interim final rule. In response to public comments, the DOD has clarified the definitions of "U.S.-based" and "U.S. citizen."[3] Under the terms of the program, generally participants may use information provided by the government to safeguard information only on covered DIB systems that are U.S.-based and must restrict distribution of information to U.S. citizens.[4]

As clarified, "U.S. based" means "provisioned, maintained, or operated within the physical boundaries of the United States" and a U.S. citizen includes a person born in the United States or naturalized. In appropriate circumstances on a case-by-case basis, the government may authorize use of government-furnished information to protect a non-U.S.-based covered DIB system, or may authorize distribution of information to a non-U.S. citizen.[5]

Notably, the final rule maintains the provision requiring a DIB participant to "perform a legal review of its policies and practices that support its activities under [the] program" and to "make a determination that such policies, practices, and activities comply with applicable legal requirements" before sharing any information with the government under the program.[6]

In the interim final rule, Section 236.6(c) contained a second sentence advising that the government "may request from any DIB participant additional information or assurances" regarding the DIB participant's policies or practices, or the DIB's determination that such policies or practices comply with applicable legal requirements.[7]

In response to public comments questioning whether those government requests would threaten communications protected by the attorney-client privilege, the final rule deletes this second sentence. The DOD's explanation for the deletion advises that such language was intended "merely to provide notice that the Government may request additional information" from a DIB participant and did not

intend to imply that the DOD required additional information as a condition of the program.[8] Thus, while the DOD has deleted the language to avoid confusion, the DOD may still request additional information from participants.

With the publication of this final rule, the DOD has solidified the framework for the voluntary DIB CS/IA program. This program is part of the U.S. government's increasing efforts to combat cyber threats posing risks to U.S. economic and national security interests. Congress has been working for several years on legislation to facilitate cyber information sharing and provide liability protection to companies that share information with the government.

For example, the House of Representatives has repeatedly passed the Cyber Intelligence Sharing and Protection Act. However, such legislation is unlikely to be enacted this year, which increases the importance of regulatory initiatives such as the DIB CS/IA program and the executive branch activities that President Obama directed in his executive order on implementation of critical infrastructure cybersecurity (EO 13636).[9]

[1] 78 Fed. Reg. 62430 (Oct. 22, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf
[2] 77 Fed. Reg. 27615 (May 11, 2012).
[3] 32 C.F.R. § 236.2(n) and (o).
[4] 32 C.F.R. § 236.4(g).
[5] Id.
[6] 78 Fed. Reg. at 62437.
[7] 77 Fed. Reg. at 27620.
[8] 78 Fed. Reg. at 62434.
[9] Arnold & Porter's advisory on the executive order is available here: http://www.arnoldporter.com/public_document.cfm?id=22077&key=19H1

Ronald Lee is a partner and Lauren Schlanger and Nicholas Townsend are associates in Arnold & Porter's Washington, D.C., office.