Advisory

MARCH 2014

If you have any questions about this Advisory, please contact:

JAMES GLASSER
203.498.4313
jglasser@wiggin.com

DAVID HALL
215.988.8325
dhall@wiggin.com

DAVID RING
860.297.3703
dring@wiggin.com

TAHLIA TOWNSEND
203.498.4339
ttownsend@wiggin.com

ERIC LAPRE
203.498.4373
elapre@wiggin.com

Commerce Department Hints At Broadening Export Enforcement

Does an "export" occur when a foreign person has the mere ability to access export-controlled data, regardless of whether he actually accesses that data? The Department of State and the Department of Commerce have long diverged on this issue. Since its landmark settlement with General Motors in 2004, the Department of State has generally considered the mere ability to access data sufficient to constitute an "export" under the International Traffic in Arms Regulations ("ITAR"), which regulate the export of defense articles and services. That interpretation makes quite a leap from the ITAR's definition of "export," which includes "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person." The Department of Commerce, on the other hand, appeared to be sticking with the plain language of the regulations in considering only actual access sufficient to constitute an "export" under the Export Administration Regulations ("EAR"), which regulate the export of certain munitions and so-called "dual-use" items having both civil and military applications. But a recent settlement suggests that the Commerce Department may be coming into step with the State Department's more aggressive stance - a shift that could pose significant compliance implications for businesses across a broad range of industries.

On February 24, 2014, the Commerce Department's Bureau of Industry and Security ("BIS") announced that it reached a $115,000 settlement with Intevac, Inc. ("Intevac"), a U.S. company that develops night-vision technology and equipment used to manufacture hard disks and solar cells. BIS charged Intevac with EAR violations for releasing, without an export license, EAR-controlled drawings, blueprints, and part identification numbers (the "Technology") to a Russian national employee at Intevac's California headquarters. Under the EAR's "deemed export" rule, that release was deemed to be an export to the employee's home country of Russia. According to the settlement agreement, "Intevac released the [Technology] . . . by providing the Russian national employee with a login identification code and password that enabled him to view, print, and create attachments." The agreement does not explicitly state that the Russian national actually accessed the Technology.

BIS further alleged that three additional releases occurred when Intevac, after learning of the unauthorized release discussed above, "stored technology" on its server on three occasions and "provided the employee with a login identification code and password that enabled him to view, print, and create attachments." Again, the agreement fails to specify whether the Russian national actually accessed the technology on those three occasions, or if the additional violations stemmed from Intevac merely storing technology on the server while the Russian national still had access.

CONTINUED ON NEXT PAGE

New Guidance on Providing Financial Services to Medical Marijuana Businesses CONTINUED

Taken alone, the agreement's silence as to whether actual access occurred is probably insufficient to signal the beginning of a BIS crusade against potential access. It is possible that the Russian national did access the subject technology, but BIS failed to say so explicitly. Indeed, the agreement's ambiguous language ("enabled him to") could be interpreted to mean that actual access did, in fact, occur.

But the agreement goes on.

In a separate charge, BIS alleged that Intevac released drawings, blueprints, and part identification numbers to its China-based subsidiary. This time, the agreement unequivocally discusses actual access, noting that "a Chinese national employee working at the Chinese subsidiary used a login identification code and password provided by Intevac to access a server storing the technology . . . and to open a file attachment containing the technology."

When language is included in one place and omitted in another, the omission is often intentional. BIS's explicit discussion of actual access by the Chinese national could indicate that no actual access occurred in the case of the Russian national, where BIS was silent on the issue.

Not every silence is pregnant. Sloppy drafting could be the culprit here, and so it may be premature to conclude that BIS is expanding its enforcement efforts to police potential access. Nevertheless, the Intevac case reminds us that compliance and IT professionals should work hand-in-hand to ensure that sensitive data is accessed – and accessible – only by authorized persons.

Wiggin and Dana LLP's Defense, OFAC, and Export Compliance practice is tracking further developments.