DOJ wants your U.S. export controls and sanctions disclosures: what's the impact?

The U.S. Department of Justice, National Security Division recently published guidance which encourages companies to voluntarily self-disclose directly to it possible wilful violations of U.S. export controls and sanctions. David A. Ring examines the pros and cons of self-disclosure of what are, essentially, criminal violations.

On 2 October 2016, the U.S. Department of Justice ('DOJ'), National Security Division ('NSD') published guidance[1] encouraging organisations to voluntarily self-disclose possible wilful – and therefore criminal – violations of U.S. export controls and sanctions directly to NSD. This guidance is applicable not only to U.S. companies, but to non-U.S. companies that are subject to the extraterritorial reach of U.S. export and sanctions laws. Because this policy marks an extension of the U.S. government's efforts to hold individuals criminally liable for corporate wrongdoing, companies everywhere should take notice.

NSD's newly announced guidance, at its core, encourages companies to disclose possible criminal violations of export control and sanctions laws, and offers leniency and benefits to companies that do so and, then, cooperate with law enforcement. This guidance aligns NSD with other DOJ components that have promulgated disclosure guidelines in an attempt to bolster DOJ's efforts to hold companies and – especially – individuals criminally responsible for regulatory wrongdoing. Consistent with the Yates Memo[2] issued late last year, NSD's guidance makes clear that its primary purposes include encouraging companies to implement stronger efforts to 'prevent and detect' violations, and increasing NSD's ability '*to prosecute individual wrongdoers whose conduct might otherwise have gone undiscovered or been impossible to prove*' [emphasis added].

Of interest to non-U.S. businesses headquartered in the U.S., the new guidance explicitly offers leniency to U.S.-parent companies that make available evidence and witnesses from their overseas subsidiaries, especially when such evidence and witnesses otherwise would not be available under international treaties. Similarly, leniency would be extended to non-U.S. companies that voluntarily disclose to NSD criminal violations of U.S. laws by their non-U.S. employees. While DOJ recognises that, in some instances, non-U.S. law may prohibit disclosure, it places the burden on companies to prove that a disclosure was prohibited, and nonetheless encourages companies to 'identify all available legal bases' for cooperating with the DOJ.

Leniency would be extended to non-U.S. companies that voluntarily disclose to NSD criminal violations of U.S. laws by their non-U.S. employees.

NSD's new guidance marks a significant departure from the long-established practice of encouraging companies to voluntarily disclose export and sanctions violations to the pertinent regulatory agencies (i.e., the Department of State's Directorate of Defense Trade Controls, the Department of Commerce's Bureau of Industry and Security, the Treasury Department's Office of Foreign Assets Control), and then relying on law enforcement liaisons within those agencies to determine which disclosures warrant additional scrutiny. Now, companies are expected to determine whether a violation is wilful (and therefore criminal), and, if so, whether to disclose the violation to both the regulatory agency and NSD.

Not only does this mark a change in DOJ's expectations regarding where a disclosure should go, it marks a change in what is said in disclosures and how they are investigated, as well. Under current regulations, companies are instructed to disclose (among other things) whether any individual acted 'intentionally'. That analysis is largely factual and straightforward: Did the employee act purposefully to accomplish what was done, or not? But NSD's newly released guidance requires another level of legal analysis: whether any employee acted 'wilfully,' which NSD defines as 'done with the knowledge that it is illegal'.

NSD's 'wilfulness' analysis raises a number of questions and challenges. First, it's by no means settled that a criminal violation of export laws requires only general knowledge of illegality, rather than specific knowledge of the underlying regulatory requirements. Compare *U.S. v. Pulungan*, 569 F3d 326 (7th Cir. 2009) (defendant cannot be convicted of wilfully attempting to export a defence article unless he knew the item was a 'defence article') with *U.S. v. Bishop*, 740 F3d 927 (4th Cir. 2014) (upholding conviction of wilfully attempting to export a defence article where the defendant believed the export was illegal, but did not know the items were 'defence articles'). The new guidance, therefore, may put companies in the uncomfortable position of disclosing 'wilful' conduct to NSD in order to obtain leniency, while still maintaining that the conduct was not wilful under applicable law. Moreover, and perhaps more problematic, compliance personnel who typically draft and submit disclosures may be ill-suited to make the delicate determination of

Links and notes

[1] https://www.justice.gov/nsd/file/902491/download
[2] https://www.justice.gov/dag/file/769036/download

whether a fellow employee may have known his or her actions were illegal. Typically, criminality turns on circumstantial evidence and inference, which require a type of analysis not normally made by in-house personnel. The consequences for disclosing a wilful violation to NSD can be extreme, and the decision to do so should not be made lightly by those who are not well versed with the intricacies of U.S. criminal law.

Disclosure dilemmas

So what of the beleaguered business manager who authorises IT access to a new non-U.S. employee knowing that company policy – and presumably the underlying regulations – doesn't allow access to a portion of the data contained in the system? Surely the violation (if there was one) would be 'knowing' under the ITAR, but is it 'wilful'? What if the new employee was Chinese? What if, unknown to the manager, technical data were actually accessed by the new employee for no known business reason? In the highly technical realm of export and sanctions compliance – where violations can occur in a myriad of ways – a decision to disclose to NSD will involve a calculation of numerous factors beyond whether an employee acted with knowledge that a regulatory violation would occur. For instance, consideration should be given to the seriousness of the conduct, the potential for harm, the employee's underlying motivations, and the subjective determination of whether a law enforcement agency might care. As a practical matter, companies will now be asked to make a law enforcement assessment for the government, and must face the risks inherent to this determination: under-disclosure may deprive the company of significant benefits, whereas over-disclosure might lead to absurd results, including criminal referrals for pedestrian conduct.

Companies need to proceed with caution before deciding whether to disclose potential wilful conduct to NSD.

At bottom, it remains to be seen what tangible benefits will be bestowed on companies that make disclosures under NSD's new policy. If recent FCPA cases are any indicator, the benefits may be substantial. But companies need to proceed with caution before deciding whether to disclose potential wilful conduct to NSD. And at the very least, NSD's new guidelines should make clear that DOJ expects companies to do more to detect possible criminal violations, and that DOJ itself intends to do more to hold individuals criminally responsible for trade compliance violations.

David Ring, a partner at Wiggin and Dana LLP, serves as a U.S. State Department appointed monitor for a global aerospace company. He also conducts corporate investigations on a variety of legal and regulatory issues, provides compliance and ethics counseling, and defends individuals and companies accused of crime.

dring@wiggin.com

This article is reprinted from the November 2016 issue of *WorldECR*, the journal of export controls and sanctions.

www.worldecr.com