Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Mistakes Vs. Falsehoods In Trade Controls Submissions

By **Steven Fagell, Peter Lichtenbaum and Eric Sandberg-Zakian**
(August 12, 2019, 2:54 PM EDT)

Steven Fagell

Peter Lichtenbaum

Eric Sandberg-Zakian

The U.S. government has stepped up enforcement of trade controls laws, and multinational companies are increasingly in the crosshairs. This year alone, the U.S. Treasury Department has dramatically increased the number of economic sanctions enforcement actions, bringing more than twice as many cases in the first six months of 2019 as it brought in all of 2018.

On the export controls front, during President Donald Trump's first two and a half years in office, the U.S. Commerce Department imposed the two largest civil monetary penalties for export controls violations in department history, and opened 21% more enforcement cases than the department opened during President Barack Obama's final two and a half years. These developments are part of a longer-term trend of increasing government focus on penalizing corporate trade controls violations, with nearly all of the most costly civil and criminal trade controls settlements in history announced in the last 10 years.

Often, U.S. government trade controls investigations focus not only on whether a company violated substantive export controls or sanctions laws, but also on whether the company made false statements to U.S. trade controls regulators. The most recent, notable example is Huawei Technologies, which the U.S. Department of Justice accused in January 2019 of violating U.S. sanctions against Iran and providing false information to the government.

In this prevailing climate of heightened U.S. trade controls enforcement, companies operating in markets outside the United States must remain vigilant regarding their interactions with the U.S. government, especially if they find themselves making written submissions to U.S. regulatory agencies that administer U.S. trade controls. These submissions can take different forms.

For example, a company may ask the U.S. State Department — through a commodity jurisdiction request — whether a product is subject to the International Traffic in Arms Regulations, or ITAR, necessarily including significant product description. A company may submit a license application to the U.S. State, Commerce or Treasury Departments that includes extensive discussion of the facts of a planned business transaction. Or a company may voluntarily

disclose a violation of U.S. trade controls to one of those three departments, and thereafter provide written answers to detailed follow-up questions.

These submissions frequently are prepared by trade controls professionals who may not be attorneys (let alone attorneys with backgrounds in criminal law), and who may be forced to rely on information gathered from far corners of often sprawling and complex global organizations. Notwithstanding these process challenges, companies should appreciate that such a written submission can give rise to criminal liability if it includes knowing and willful false statements — even when the company's signatory on the submission lacked any knowledge of its falsity.

Criminal investigations of trade controls submissions often do not begin at the U.S. Department of Justice. Rather, in the first instance, civil regulators (e.g., the State, Commerce or Treasury Department) will receive and scrutinize these submissions, considering not only the substance of the submissions, but also their accuracy and completeness.

If a regulator concludes that a submission contained false or misleading statements, the regulator may be more likely to impose civil monetary penalties for any underlying substantive violations, or to use its authority to impose such penalties for the statements themselves. Even more seriously, if the regulator becomes concerned that a criminal violation of the trade controls laws may have been committed, or that the submission may have been deliberately misleading, a referral to the Justice Department for criminal investigation could ensue.

When a matter is referred for criminal investigation, the risks to the company increase exponentially — and the accuracy and completeness of the company's submission are likely to face even greater scrutiny. The Justice Department has long viewed criminal false statements charges as a key arrow in its quiver, even if only as ancillary to charges relating to substantive violations of the trade controls laws. In this regard, consider that many well-publicized trade controls enforcement actions include false statements charges.

In 2007, ITT Corporation reached a combined civil and criminal settlement in which it pleaded guilty to violating the ITAR and making false statements to the State Department, and agreed to pay a penalty of $100 million that was reduced to $50 million due to certain offsets. In 2010, BAE Systems plc pleaded guilty to making false statements to the State Department and agreed to pay a $400 million criminal fine. In 2012, various affiliates of United Technologies Corporation agreed to pay approximately $55 million, after offsets for spending on compliance enhancements, in a global criminal and civil settlement involving ITAR violations and false statements included within voluntary disclosures to the State Department.

In 2014, BNP Paribas pleaded guilty to criminal sanctions violations and agreed to a settlement worth approximately $8.9 billion. The government alleged, among other things, that the bank engaged in inaccurate communications designed to hide from the Treasury Department its long-running dealings with Cuba. In 2018, FLIR Systems Inc. entered into a civil settlement with the State Department worth up to $30 million in fines and expenditures on remedial measures for a wide range of alleged ITAR violations, dozens of which involved false or misleading statements in license applications and voluntary disclosures.

Even more prominently, in 2017 and 2018, ZTE agreed to two successive trade controls settlements involving alleged false statements together worth up to approximately $2.4 billion. The company's initial criminal settlement included a guilty plea to making false statements by lying to and misleading criminal

and civil investigators. Another instance of alleged dishonesty — inaccurately claiming to have disciplined employees responsible for impermissible dealings with Iran — prompted the Commerce Department to re-impose ZTE's previously suspended export denial order and effectively put the company out of business.

The company is reported to have survived only because Trump intervened, agreeing to remove the denial order in exchange for a $1 billion cash payment, an additional $400 million in escrow, a wholesale replacing of ZTE's board of directors and senior executives, and the adoption by ZTE of an intensive external compliance monitoring arrangement.

Against this backdrop, companies cannot rely merely on the good faith of the official empowered to sign the submission on the company's behalf. Sufficient care, attention and resources should be devoted to ensuring that critical information residing deep within the company is not missed, lost, mischaracterized or concealed. While every company is different and the most effective techniques will vary depending on the context, we have identified seven steps that companies can take to mitigate these risks.

Give a Single Person Primary Responsibility for the Accuracy of the Submission

The preparation of complicated trade controls submissions is often a team effort. The legal or compliance department, key business leaders, engineers, salespeople, product managers, the logistics department, IT professionals and outside counsel all may be involved.

When so many different people provide information — some of whom may not understand the context or seriousness of the submission to which they are contributing — fact-checking can be a formidable challenge. A good approach is to assign primary responsibility for ensuring the accuracy of the submission — and corresponding accountability — to a single individual.

That individual presumably will not have sufficient personal knowledge to fact-check the full submission on his or her own. However, the point person for the submission can pressure-test information coming from different contributors, ask for back-up documentation or other corroboration, and follow up on any unclear or incomplete contributions.

Decide How Thorough the Fact-Finding Will Be

The amount of time and resources a company can and should spend on a given submission will vary, depending on the importance of the submission and the company's circumstances. At one end of the spectrum, a submission may rely primarily on information gathered on telephone calls with relevant employees. At the other end of the spectrum, a submission may be tested through forensic document collection and review conducted by outside counsel.

Other, more intermediate levels of review also can be devised. Companies should decide on a considered and deliberate approach for each submission — one that balances hard costs, time and allocation of resources against the risk of a misrepresentation in light of the circumstances surrounding the submission in question.

Provide a Limited and Appropriately Caveated Account of the Facts

When possible, offer facts instead of opinions susceptible to dispute. "Although design work for the helmet was funded by the Department of Defense, the helmet provides essentially the same protection

as privately developed helmets sold for use in industrial applications" invites the government to define the vague term "essentially the same protection" for itself, or look through marketing materials in search of statements touting the helmet's superior quality. A more specific, factual statement — "in durability testing conducted by the company, privately developed helmets sold for commercial applications passed the tests at the same rate as the Defense Department-funded helmet" — can serve the same purpose.

Similarly, do not overstate the facts. Instead, describe the available information and avoid sweeping factual conclusions. "No employees at the company knew the shipment was destined for Syria" is difficult to prove and susceptible to attack if the government undertakes a detailed email review. "The company is aware of no evidence that the sales and logistics personnel who approved the shipment knew it was destined for Syria" communicates the same information with less risk.

In the voluntary disclosure context, in particular, avoid the temptation to minimize, justify or defend controls shortcomings or employee misconduct. Detailing the relevant facts and documents is more likely to establish credibility than presenting a narrative that an agency may interpret as excusing or downplaying serious mistakes.

Finally, embrace language conveying that the company's review is ongoing. "Based on our review to date" allows for supplementing the disclosure and for the possibility that facts may change. But do not over-commit. "We will update [the agency] as circumstances warrant" provides more flexibility than, "We will update [the agency] after we have completed our investigation."

Design Corrective Actions Carefully and Implement Them Faithfully

In a voluntary disclosure, it is sometimes necessary to describe corrective actions that have not yet been completed. In our experience, implementing corrective actions often proves more difficult than anticipated.

Terminating a business partner that engaged in misconduct may seem less appealing after learning that materials, services or market access provided by the partner cannot be replaced. Technical enhancements to automated controls can seem promising, but unexpected IT challenges may make them unworkable. Procedures calling for extensive due diligence or complicated paperwork may prove too time-consuming to implement.

The ZTE case provides an admittedly extreme example of the risk a company may run by failing to complete promised corrective actions, but it nonetheless underscores the extent to which failure to follow through on corrective actions can result in false statements allegations. Ideally, all corrective actions should be completed before a final disclosure is submitted. When it is necessary to commit to future actions, the company should be certain those actions can be implemented and, after committing to them, should focus on implementing them fully and promptly.

Report Violations Stemming From Any Delay in Submitting a Disclosure

A company should ensure its voluntary disclosure covers all relevant violations to avoid any suggestion that the company deliberately omitted material facts. This issue is especially important if there is a delay between when an employee of the company learns of an export controls violation and when the company submits its disclosure, because the delay itself can result in additional, independent violations.

Under Section 126.1(e) of the ITAR, anyone with knowledge of a violation involving China or another arms-embargoed country must "immediately inform" the State Department. If an employee learned of an unlawful export, but the company did not promptly make a disclosure, then the company may need to disclose a 126.1(e) violation in addition to the underlying export violation. Inadvertently failing to identify the 126.1(e) violation separately and clearly in a disclosure may raise questions at the State Department about a company's honesty and transparency.

Similarly, General Prohibition 10 of the Export Administration Regulations, or EAR, prohibits a company from doing almost anything with an item if it knows the item has been unlawfully exported in violation of the EAR, including selling, transferring, financing, servicing, storing, using or disposing of the item. Thus, in preparing a disclosure, a company should consider whether it undertook any action involving an item that had been unlawfully exported after a company employee learned of the unlawful export. If so, the company's disclosure may need to identify violations of General Prohibition 10, in addition to the underlying unlawful export.

Protect the Privilege

The attorney-client privilege and work-product doctrine play an important role in false statements investigations. They allow for such investigations to be conducted with a measure of confidentiality and discretion, which, in turn, can help to ensure that the company is best positioned to develop a reliable and accurate record of the facts.

Companies can take several steps to ensure the application of the privilege and work product protection. These steps include seeking legal advice from attorneys regarding the disclosure process, making explicit in communications with attorneys that the communications are for the purposes of seeking legal advice or reflect the advice of counsel, and clearly memorializing that any non-attorney work has been requested by, and will be performed at the direction of, counsel for the purpose of providing legal advice to the company.

To preserve attorney-client and work-product protections once established, companies should phrase submissions so as to avoid any risk of waiver. Whenever possible, submissions should provide facts that are supported by non-privileged documents (whether or not those documents are cited in the submission or provided to the regulator). When it is necessary to provide facts gathered by the company through privileged interviews or other privileged communications, the submission's language should stick to the facts themselves and avoid referencing the privileged communications.

Correct Any Errors With Your Eyes Wide Open

No matter how carefully a submission is researched and pressure-tested, it can still include a statement that turns out to be inaccurate. When a company discovers an inaccuracy and there is no mandatory duty to correct it (as there is with respect to license applications to the Commerce Department), the most prudent course of action often can be unclear.

Certain factors can weigh in favor of a corrective disclosure. For example, to some government officials, correcting an inaccurate statement may serve as persuasive evidence that the error was inadvertent. Moreover, a correction can mitigate the risk of the company engaging in further correspondence with the government premised on the inaccurate information or allowing the government to make a decision based on that information.

Other factors can weigh against a corrective disclosure. As a legal matter, there is no way to cure a false statement through subsequent correction. If inaccurate material information is knowingly and willfully provided to the government, the false statements offense is complete, regardless of the company's later conduct. And of course, bringing the error to the government's attention can make the error an easy target for further investigation.

As with many risk-based decisions, the most advisable path will depend on the facts of the case, the course of dealing with the government and a host of other factors.

Naturally, the extent to which these steps are necessary or worthwhile will vary from company to company and submission to submission. But companies should try to put them into practice when possible, to reduce the ever-present false statements risk in high-stakes submissions to U.S. trade controls regulators.

Steven E. Fagell is co-chair of Covington & Burling LLP's white collar defense and investigations practice group. He is a former senior official in the Criminal Division at the U.S. Department of Justice.

Peter Lichtenbaum is a partner at Covington. He formerly served as assistant U.S. secretary of commerce for export administration.

Eric Sandberg-Zakian is an associate at Covington.