UNITED STATES DEPARTMENT OF COMMERCE
Assistant Secretary for Export Enforcement
Washington, D.C. 20230

April 18, 2023

MEMORANDUM FOR ALL EXPORT ENFORCEMENT EMPLOYEES

FROM: MATTHEW S. AXELROD
ASSISTANT SECRETARY FOR EXPORT ENFORCEMENT

SUBJECT: Clarifying Our Policy Regarding Voluntary Self-Disclosures and Disclosures Concerning Others

Export Enforcement's core mission is to protect sensitive U.S. technologies and goods from being used by our adversaries for malign purposes. That mission has never been more important or complex than right now – when transformative technologies, such as advanced semiconductor production and advanced computing capabilities, have the potential to alter the world's future balance of power. As the Intelligence Community's 2023 Annual Threat Assessment recently noted, rapidly emerging or evolving technologies have the potential to disrupt traditional business and society, while creating unprecedented vulnerabilities. Simply put, technology protection is a core national security priority.

It's also a shared endeavor. Effective compliance is the first line of effective enforcement and we need the support and cooperation of U.S. businesses and universities – those who are at the forefront of these extraordinary technological advances. Both industry and academia must have proper compliance systems in place to identify, prevent, and mitigate export control violations. And an important part of a robust export compliance system is a process for making two different types of disclosures to our Office of Export Enforcement: (1) voluntary self-disclosures (VSDs) about parties' own possible violations of the Export Administration Regulations (EAR); and (2) disclosures about possible EAR violations by someone else.

Voluntary Self-Disclosures

Last June, we implemented a dual-track system to handle VSDs. The vast majority of VSDs – those that involve minor or technical infractions – are now resolved on a fast-track basis with our issuance of a warning or no-action letter within 60 days of final submission. For VSDs that present a more serious issue, we assign both a field agent, an Office of Chief Counsel attorney, and, in the most serious cases, an attorney from the Department of Justice's Counterintelligence and Export Control Section. Since we've implemented this system, we've heard from industry that they appreciate getting quick resolutions for minor or technical infractions. Also, we haven't seen a material change up or

down in the number of VSDs we receive (which isn't surprising since last year's changes weren't designed to drive a change in the calculus of whether to file or not).

Today's policy announcement is different from last June's. We specifically want to further incentivize the submission of VSDs when industry or academia uncovers significant possible violations of the EAR. Note the modifier "significant" before "possible violations of the EAR." We're not focused on increasing the number of minor or technical VSDs we receive. In fact, we want to let VSD filers know that when they identify multiple minor technical violations close in time, they can submit one overarching submission (as opposed to in multiple separate VSDs) to help streamline the process on their end and conserve resources on ours. Instead, we're interested in increasing the number of VSDs we receive that disclose significant possible violations – the types of violations that reflect potential national security harm.

To do that, we want everyone to understand the risk calculus. Under the existing BIS settlement guidelines, a VSD that is timely, comprehensive, and involves full cooperation substantially reduces the applicable civil penalty under the base penalty matrix. It may also entitle the filer to additional mitigation, including the possibility of a fully suspended penalty in certain cases. If a company or university voluntarily discloses a violation (and the violation is considered non-egregious), the base penalty amount is one-half of the transaction value and capped at a maximum base penalty amount of $125,000 per violation. In some non-egregious cases, full suspension of the penalty may even be possible. And even in an egregious case, the base penalty amount is reduced up to one-half of the statutory maximum penalty applicable to the violation. Moreover, the filing of a VSD is also a factor for consideration in weighing the impact of a party's compliance program at the time of the violation, as well as its remedial response, on the final administrative penalty. So, whatever the situation, a voluntary self-disclosure entitles the reporting entity to a steep and concrete reduction in potential monetary liability.

What we're clarifying, effective immediately, is how we apply the existing guidelines in situations where there is a deliberate non-disclosure of significant possible violations. When someone chooses to file a VSD, they get concrete benefits; when someone affirmatively chooses not to file a VSD, however, we want them to know that they risk incurring concrete costs. Here's why. While it's true the guidelines provide that "[f]ailure to voluntarily disclose an apparent violation to OEE does not constitute concealment,"[1] another of the factors that OEE uses to help determine the appropriate penalty amount in administrative cases focuses on "[t]he existence, nature and adequacy of a Respondent's export compliance program at the time of the apparent violation."[2] More specifically, the settlement guidelines provide that "OEE will also consider whether a Respondent's export compliance program uncovered a problem, thereby preventing further violations, and whether the Respondent has taken steps to address compliance concerns raised by the violation, to include the submission of a VSD and steps to prevent reoccurrence of the violation that are reasonably calculated to be effective."[3] Because this factor is a "General Factor," it is designed to be "either mitigating or aggravating." In the past, we have consistently applied it as a mitigating factor when a VSD has been filed after a potential violation was uncovered. Going forward, we will also consistently apply this factor as an aggravating factor when a significant possible violation has been uncovered by a party's export compliance program but no VSD

[1] See Note to Section III to Supplement No. 1 to Part 766 of the EAR. Concealment is further discussed at Section III.A.3.
[2] Section III.E to Supplement No. 1 to Part 766 of the EAR.
[3] *Id.*

has been submitted. In other words, when someone submits a VSD, they receive concrete and identifiable benefits under our guidelines. By the same token, however, when someone uncovers a significant possible violation but then affirmatively chooses not to file a VSD, they are running a substantial risk – because if it does come to our attention, the decision not to disclose will be considered an aggravating factor under our existing guidelines.

In summary, companies and universities should carefully weigh any decision not to disclose significant possible violations to us. If a company or university commits a violation of the EAR and makes a disclosure, they benefit greatly by getting a sharply reduced penalty – but if they make a deliberate decision not to disclose a significant possible violation, they risk a sharply increased one.

Disclosures About the Conduct of Others

We want to do everything in our power to encourage parties to invest in strong compliance programs and comply with our rules. We also want to incentivize individuals, companies, and universities to come forward and tell us when they become aware of others who are violating our rules. Because protecting sensitive U.S. technology is a shared endeavor, we need everyone's assistance in bringing potential EAR violations to our attention. Moreover, we don't want parties to suffer in silence when they're forgoing sales because of our controls while their competitors continue to book revenue. We want them to reach out to us or to use our confidential reporting form. We will aggressively investigate and, as appropriate, take action in such situations. But we can't investigate what we don't know about – which is why we want parties to come forward and tell us when they are aware of potential EAR violations by others.

In addition to making such disclosures being the right thing to do, our existing settlement guidelines make clear that there are concrete benefits for the disclosing party. One of the three "Mitigating Factors" contained in our guidelines is "Exceptional Cooperation with OEE." And among the subfactors that OEE considers in evaluating "exceptional cooperation" is whether a party has "previously made substantial voluntary efforts to provide information (such as providing tips that led to enforcement actions against other parties) to federal law enforcement authorities in support of the enforcement of U.S. export control regulations."[4] In other words, when a company becomes aware that some other company's conduct may have violated the EAR, discloses such conduct to OEE, and that tip results in enforcement action – then we will consider that a mitigating factor if a future enforcement action, even for unrelated conduct, is ever brought against the disclosing party.

When the conduct disclosed includes not just a potential export control violation but also a potential sanctions violation, there may also be monetary rewards available. The Financial Crimes Enforcement Network, or FinCEN, now maintains a robust whistleblower program designed to incentivize individuals, both here in the United States and abroad, to notify the government about violations of U.S. sanctions programs, in addition to violations of the Bank Secrecy Act. Individuals who provide FinCEN or the Department of Justice with information about such violations may be eligible for substantial financial awards if the information they provide ultimately leads to a successful enforcement action. Importantly, FinCEN can pay awards to whistleblowers whose original information also led to successful enforcement of "related actions." This means that FinCEN could even pay awards

[4] *Id*, at Section III.G.

on Export Control Reform Act penalties – so long as either Treasury or Justice take a qualifying action based on the same original information provided by a whistleblower.

As Deputy Attorney General Lisa Monaco said in her September 2022 Memorandum, commitment to fostering a strong culture of compliance at all levels of a corporation – and not just within the compliance department – is a key aspect of an effective compliance program and ethical corporate culture. We agree. Today's policy clarifications underscore our commitment to incentivizing a strong culture of compliance – one that generates appropriate disclosures of potential EAR violations, both when those disclosures are VSDs and when they're disclosures about the conduct of others.