GIBSON DUNN

December 13, 2019

DOJ NATIONAL SECURITY DIVISION RELEASES UPDATED GUIDANCE ON VOLUNTARY SELF-DISCLOSURES

To Our Clients and Friends:

Today, the U.S. Department of Justice ("DOJ" or the "Department") announced changes to its policy governing the treatment of voluntary self-disclosures (or "VSDs") in criminal sanctions and export control investigations. Critically, DOJ will now offer VSD benefits to financial institutions in such matters, generally aligning the Department's guidance to financial institutions in this area with other enforcement policies meant to encourage corporate disclosures.

As we discussed at length last year, deciding whether to voluntarily self-disclose corporate wrongdoing to DOJ is a complex exercise, marked by potential benefits that are difficult to anticipate and quantify. DOJ's efforts to incentivize corporate disclosures of U.S. Foreign Corrupt Practices Act ("FCPA") violations—and thus provide more certainty for companies facing criminal prosecution—have served as a model for corporate criminal investigations in other areas. In early 2018, Acting Assistant Attorney General John Cronan announced that DOJ's 2017 FCPA Corporate Enforcement Policy ("CEP") would serve as non-binding guidance for corporate investigations beyond the FCPA context. Many aspects of the CEP (and its predecessor, the 2016 FCPA Pilot Program) were incorporated into the Justice Manual ("JM") (previously known as the United States Attorneys' Manual), which outlines the Department's high-level approach to voluntary self-disclosures.

In a similar vein, the changes announced today by DOJ's National Security Division ("NSD") with respect to criminal sanctions and export control violations include the following key features:

- **Applies to Financial Institutions:** Financial institutions are now subject to NSD's newly issued policy (the "2019 NSD Guidance"). Accordingly, rather than relying on general DOJ guidance applicable to all business organizations—like the high-level guidance provided in the JM—financial institutions may instead rely on the requirements and assurances set forth in the 2019 NSD Guidance when evaluating the potential costs and benefits of self-disclosing export control and sanctions violations to DOJ.

- **Presumption of Non-Prosecution Agreement:** Companies that discover a criminal export control or sanctions violation, voluntarily self-disclose the violation to DOJ, and satisfy the requirements set forth in the 2019 NSD Guidance will now benefit from a presumption that they will receive a non-prosecution agreement ("NPA") and will not be assessed a fine, provided no aggravating factors are present.

- **Reduced Penalties:** Where aggravating circumstances warrant an enforcement action other than an NPA, companies that otherwise satisfy all the requirements of a VSD will be eligible for at

least a 50 percent reduction off the statutory base penalty—effectively capping the penalty for such companies at the dollar value of the violative transactions—and the Department will not require a monitor, provided the company has implemented an effective compliance program.

- **Successor Liability:** In mergers and acquisitions, successor companies that uncover a criminal export control or sanctions violation by the merged or acquired entity through timely due diligence and voluntarily self-disclose the violation to DOJ also will benefit from a presumption in favor of an NPA.

To help make sense of this latest development, we provide below an overview of NSD's prior policy regarding VSDs in the export control and sanctions area, a comparison with the Department's guidelines in FCPA investigations, and conclude with an analysis of the changes announced today and what they mean for businesses considering whether to self-disclose.

Background

U.S. sanctions and export controls are primarily administered and enforced by U.S. regulatory agencies, including the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), and the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"). NSD—the DOJ office with primary responsibility for overseeing and coordinating criminal investigations related to violations of U.S. export controls and sanctions—has historically played a secondary role to civil enforcement agencies, becoming involved in enforcement matters referred to them by OFAC, BIS, or DDTC.

NSD became more forward leaning during the waning days of the Obama administration, and in 2016 published the first iteration of its "Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations" (the "2016 NSD Guidance"). The 2016 NSD Guidance articulated the Department's policy of encouraging business organizations to voluntarily self-disclose criminal violations of sanctions and export controls and for the first time set forth the criteria that NSD would use in determining the potential benefits that may be offered to an organization for its self-disclosure, cooperation, and remediation efforts.

Notably, the 2016 NSD Guidance specifically exempted financial institutions from receiving the VSD benefits offered to other corporate actors in the export control and sanctions context, citing the "unique reporting obligations" imposed on financial institutions under their applicable statutory and regulatory regimes. Indeed, most U.S. financial institutions are required to file Suspicious Activity Reports ("SARs") to the U.S. Department of the Treasury when the institution knows, suspects or has reason to suspect that a transaction by, through or to it involves illegal activity. Moreover, financial institutions must report blocked property to OFAC within ten business days from the date that the property becomes blocked or else risk violating their own sanctions compliance obligations. In recent years, DOJ has accused numerous banks of engaging in practices that involved omitting, removing, or masking references to sanctioned parties and jurisdictions so as to allow transactions to be processed through the U.S. financial system. Given the potentially enormous fines for sanctions violations—which, for large banks, can easily rise to hundreds of millions of dollars—financial institutions have strong incentives to

over-comply with U.S. sanctions. As a result of their visibility into a huge volume of daily transactions and their deep aversion to sanctions-related risk, financial institutions have in effect been pressed into service as the leading edge of DOJ's and OFAC's sanctions enforcement efforts.

NSD has also become more heavily involved in the criminal enforcement of U.S. export controls—measures that are increasingly relied upon to combat the unauthorized transfer of sensitive, U.S.-origin technologies to adversaries such as China. From a policy perspective, these efforts appear to be driven by an interest in both denying China the technological means to engage in activities that threaten U.S. national security (such as spying on U.S. telecommunications networks), as well as blunting China's ability to dominate the technologies of the future (such as artificial intelligence). In the face of such risks, NSD officials have also sought to incentivize disclosures from U.S. companies targeted by Chinese economic espionage.

Key Considerations

Timing

The 2019 NSD Guidance makes explicit the stringent timing requirement applicable to VSDs for a company to qualify for full mitigation credit. DOJ requires companies to submit a VSD to the relevant office of the Counterintelligence and Export Control Section ("CES") of the NSD at substantially the same time that it submits a VSD related to the matter to the appropriate regulatory agency, whether that is DDTC, BIS, OFAC, or a combination thereof. While this timing requirement was included in the 2016 NSD Guidance, the revised policy emphasizes the point with more blunt language.

The 2016 NSD Guidance indicated that a VSD must be submitted to DOJ "within a reasonably prompt time after becoming aware of the offense," with the burden on the company to demonstrate timeliness. In export control and sanctions cases, it is now clear that the VSD must be submitted to DOJ at substantially the same time that it is submitted to DDTC, BIS, or OFAC, as the case may be.

Timely and Appropriate Remediation

The 2019 NSD Guidance generally harmonizes the requirements for companies disclosing export control and sanctions-related violations with those applicable to FCPA-related matters. The 2016 NSD Guidance was already substantially similar to the CEP, but with several subtle divergences. For example, the 2016 NSD Guidance lacked the CEP's root cause analysis requirement; the 2016 NSD Guidance did not require companies to conduct a "root cause" analysis to determine the causes of the underlying misconduct in the export control and sanctions context. The 2019 NSD Guidance adds the root cause analysis requirement for companies disclosing to NSD.

Another point of harmonization relates to the treatment of personal communications and ephemeral messaging systems. Under the CEP, companies are required to implement appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine a company's ability to retain relevant business records. The 2019 NSD Guidance incorporates this requirement into the export control and sanctions context.

With respect to possible sanctions violations, the 2019 NSD Guidance is also broadly consistent with OFAC's recent guidance, titled "A Framework for OFAC Compliance Commitments." That policy, which we described here, sets forth OFAC's views regarding what constitutes an effective sanctions compliance program and, when violations do occur, provides transparency into how OFAC will assess the adequacy of a company's compliance program in determining what penalty to impose. The 2019 NSD Guidance similarly includes the implementation of an effective compliance program—which NSD will now evaluate using criteria substantially similar to those described by OFAC—as one of the requirements for a company to remediate a criminal export control or sanctions violation.

Aggravating Factors

The 2019 NSD Guidance retains and lightly updates the list of aggravating factors specific to violations of export control and sanctions rules. These factors are in addition to others generally applicable to business organizations, which are mirrored in the CEP.

The 2016 NSD Guidance also listed examples of aggravating factors specific to the export control and sanctions area, the presence of which in substantial degree would result in a more stringent resolution for the company.

The updated list of aggravating factors includes:

- Exports of items controlled for nuclear nonproliferation or missile technology reasons to a proliferator country;
- Exports of items known to be used in the construction of weapons of mass destruction;
- Exports to a Foreign Terrorist Organization or Specially Designated Global Terrorist;
- Exports of military items to a hostile foreign power;
- Repeated violations, including similar administrative or criminal violations in the past; and
- Knowing involvement of upper management in the criminal conduct.

Benefits

The 2019 NSD Guidance provides that when a company voluntarily self-discloses export control or sanctions violations to CES, fully cooperates, and timely and appropriately remediates, there is now a presumption that the company will receive an NPA and will not pay a fine, absent aggravating factors like those described above. In cases where a different resolution—such as a DPA or a guilty plea—is warranted due to the presence of aggravating factors, but the company has otherwise satisfied all the requirements set forth in the 2019 NSD Guidance, the company can expect a reduced fine and, provided the company has implemented an effective compliance program, DOJ will not require a monitor.

Under the 2016 NSD Guidance, when a company voluntarily self-disclosed criminal violations of export controls and sanctions, fully cooperated, and provided timely and appropriate remediation, the company may have been eligible for a significantly reduced penalty, to include the possibility of (under the best case scenario) an NPA, a reduced period of supervised compliance, a reduced fine and forfeiture, and no requirement for a monitor.

Under the CEP, when a company has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and provided timely and appropriate remediation, there is a presumption that the company will receive a declination absent aggravating circumstances involving the seriousness of the offense or the nature of the offender. However, unlike in the FCPA context, DOJ stated today that a declination would generally not be appropriate with respect to export control and sanctions violations because of the likely harm to U.S. national security interests.

Voluntary Disclosure Considerations

DOJ's publication of the 2019 NSD Guidance provides additional clarity for businesses confronting the challenging decision of whether to self-report. NSD should be applauded for its efforts to sync its guidance with the CEP.

Companies—including now financial institutions—can potentially enjoy the benefit of a presumption in favor of an NPA and no fine in the export control and sanctions space if they meet the requirements set out by NSD with respect to voluntary self-disclosure, cooperation, and remediation. Moreover, by bringing NSD's guidance more closely into line with the CEP, companies and their counsel can perhaps develop a more consistent, predictable set of expectations about how DOJ's various components will treat their VSD.

The 2019 NSD Guidance creates a more elaborate set of options for corporations, particularly financial institutions. If the disclosure path is pursued, disclosure would possibly be made to NSD, OFAC, and, for financial institutions, prudential regulators as well as potentially to the Money Laundering and Asset Recovery Section of DOJ's Criminal Division ("MLARS").

As before, when considering whether to self-disclose to DOJ, companies should be mindful of a number of other considerations. Today's announcement notwithstanding, a company that discovers a potential willful export control or sanctions violation must carefully consider, among other things, the likelihood that DOJ will discover the misconduct (such as through a tip from a whistleblower or another regulator); at what stage in an investigation the misconduct should be disclosed to the government; and to what agencies the disclosure should be made and in what sequence. By taking these and other factors into account, companies that uncover export control and sanctions violations can enhance their prospects of both avoiding a full-blown criminal investigation and minimizing institutional liability to the extent possible.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any of the

leaders and members of the firm's International Trade, Financial Institutions or White Collar Defense and Investigations practice groups, or the following authors in the firm's Washington, D.C. office:

M. Kendall Day (+1 202-955-8220, kday@gibsondunn.com)
Adam M. Smith (+1 202-887-3547, asmith@gibsondunn.com)
F. Joseph Warin (+1 202-887-3609, fwarin@gibsondunn.com)
Stephanie L. Connor (+1 202-955-8586, sconnor@gibsondunn.com)
Samantha Sewall (+1 202-887-3509, ssewall@gibsondunn.com)
Scott R. Toussaint (+1 202-887-3588, stoussaint@gibsondunn.com)

Please also feel free to contact any of the following practice group leaders:

International Trade Group:
Ronald Kirk - Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
Judith Alison Lee - Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)

Financial Institutions Group:
Matthew L. Biben - New York (+1 212-351-6300, mbiben@gibsondunn.com)
Stephanie Brooker - Washington, D.C. (+1 202-887-3502, sbrooker@gibsondunn.com)
Arthur S. Long - New York (+1 212-351-2426, along@gibsondunn.com)

White Collar Defense and Investigations Group:
Joel M. Cohen - New York (+1 212-351-2664, jcohen@gibsondunn.com)
Charles J. Stevens - San Francisco (+1 415-393-8391, cstevens@gibsondunn.com)
F. Joseph Warin - Washington, D.C. (+1 202-887-3609, fwarin@gibsondunn.com)