December 19, 2019

DOJ Issues Updated Export Control and Sanctions Enforcement Policy for Business Organizations

DOJ Policy Includes Concrete Benefits for Voluntary Self-Disclosure but Requires that Disclosure Be Made Directly to DOJ

SUMMARY

On December 13, 2019, the National Security Division of the Department of Justice ("DOJ") issued a new policy that applies to business organizations that voluntarily report possible violations of export controls or sanctions to DOJ (the "Policy").[1] The Policy applies to export control and sanctions violations, including those under the Arms Export Control Act ("AECA"), the Export Control Reform Act ("ECRA"), and the International Emergency Economic Powers Act ("IEEPA").[2] Most significantly, the Policy establishes a presumption that a matter will be resolved by a non-prosecution agreement and without a fine when a company voluntarily self-discloses the misconduct to DOJ, fully cooperates, and timely and appropriately remediates, assuming no aggravating factors are present.[3] In other respects, the Policy is aligned with DOJ's recently revised policy regarding enforcement of the Foreign Corrupt Practices Act (the "FCPA Enforcement Policy").[4] Other key points are that the Policy requires self-disclosure directly to DOJ, not to other agencies; it applies to companies that discover misconduct through due diligence in the mergers and acquisition context; and it now applies to financial institutions, eliminating the carve-out that existed under the previous (now obsolete) guidance issued on October 2, 2016 (the "2016 Guidance").[5]

DISCUSSION

A. PRESUMPTION OF NON-PROSECUTION AGREEMENT

The most significant revision in the Policy is that it creates a "presumption that the company will receive a non-prosecution agreement and will not pay a fine" when the company: (1) voluntarily self-discloses export

control or sanctions violations to the Counterintelligence and Export Control Section of DOJ's National Security Division ("CES"); (2) fully cooperates; and (3) timely and appropriately remediates.[6] Previously, there had been no presumption of a particular outcome. The 2016 Guidance encouraged companies to self-disclose, but said only that self-disclosure would put the company "in a better position than if it had not submitted a VSD [voluntary self-disclosure], cooperated, and remediated," including because self-disclosing companies "may be eligible for a significantly reduced penalty" and "the possibility of a non-prosecution agreement."[7]

A company meeting the same criteria under the FCPA Enforcement Policy is entitled to a presumption of a declination—a more lenient outcome—rather than a non-prosecution agreement with no fine under the Policy, which is aimed at threats posed to national security.[8] The criteria for determining that a company has met the three predicate requirements—voluntary self-disclosure, full cooperation, and timely and appropriate remediation—are largely consistent with the criteria used in the FCPA Enforcement Policy.[9]

1. Voluntary Self-Disclosure

In order for a company's disclosure to DOJ to be within the Policy, the following must be true: (a) disclosure must be made "prior to an imminent threat of disclosure or government investigation"; (b) the company must disclose the conduct "within a reasonably prompt time after becoming aware of the offense"; and (c) "the company must disclose all facts known to it at the time of the disclosure, including as to any individuals substantially involved in or responsible for the misconduct at issue." The Policy acknowledges that a company may not know all of the relevant facts at the time it is making a prompt self-disclosure, in which case the company should simply make clear that its disclosure is based on a preliminary investigation or assessment and make its disclosure as complete as possible.[10]

2. Full Cooperation

The Policy enumerates actions that a company must take in order to have fully cooperated, with reference to the Justice Manual provisions on the same topic.[11] Some of the key requirements are: disclosure of all facts along with attribution of the sources of evidence establishing those facts; timely and proactive updates to DOJ; facts related to the involvement in the criminal activity by the company's individual officers, employees, or agents; preservation of and access to data, including data residing overseas when feasible; and both de-confliction with DOJ when the company conducts its own interviews of witnesses, and making witnesses available for DOJ to interview directly.[12] The Policy notes that DOJ may ask a company to refrain from taking particular actions for purposes of de-confliction, but it will not otherwise affirmatively direct a company's internal investigation.[13] This language is consistent with other DOJ policy designed to avoid issues that resulted in a recent ruling that DOJ had "outsourced" its own investigation to the company's outside law firm.[14]

3. Timely and Appropriate Remediation

The Policy sets forth specific requirements that must be met in order for the company's remediation to satisfy the Policy. The company must: conduct a thorough root cause analysis; impose appropriate disciplinary measures for both personnel directly involved, and those that failed to oversee or supervise those who were directly responsible; retain records, including controls and guidance regarding personal communications and ephemeral messaging platforms; and implement an effective compliance program. The Policy sets forth a list of factors that may be considered when evaluating a compliance program, including: its culture; how resourced its compliance program is; the quality and experience of compliance personnel; the authority and independence of the compliance function; compensation and promotion of compliance personnel; auditing of the compliance function; and the reporting structure of compliance personnel. These factors are consistent with the key elements of effective compliance programs identified both in the DOJ Guidance on Evaluation of Corporate Compliance Programs issued in April 2019, and in the sanctions compliance framework issued by the Department of the Treasury's Office of Foreign Assets Control ("OFAC") in May 2019.

4. Aggravating Factors

The new presumption of a non-prosecution agreement accompanied by no fine is caveated by the effect of aggravating factors, which can result in a different outcome, such as a deferred prosecution agreement or a guilty plea.[15] Aggravating factors include (but are not limited to): export of items controlled for nuclear nonproliferation or missile technology reasons to a proliferator country; exports of items 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 power; repeated violations; and knowing involvement of upper management in the misconduct.[16]

Even when aggravating factors are present, however, the company will be entitled to a fine reduction of 50% below the applicable fine, as measured by the gross gain or loss, and will not be required to implement a monitor, assuming an effective compliance program is in place at the time of resolution.[17] Civil enforcement agencies separately may impose administrative fines, although DOJ will "endeavor to coordinate" and consider those other fines when resolving a case involving the same conduct. It should be noted that the applicable criminal fine in many export control and sanctions matters is *twice* the gross gain or gross loss, and therefore a reduction of 50% will yield a penalty equal to the gross gain or gross loss.[18] The company will not, however, be permitted to retain any gains from unlawful conduct, although significant or disproportionate profits are no longer an aggravating factor alone as they were under the 2016 Guidance.[19]

B. REPORTING DIRECTLY TO DOJ

In order for a company to gain the benefit of the Policy, it must disclose the possible misconduct directly to DOJ, specifically to CES. The Policy continues to encourage companies to report possible misconduct

directly to the responsible enforcement agency, *e.g.*, the State Department's Directorate of Defense Trade Controls for AECA violations, the Commerce Department's Bureau of Industry and Security for ECRA violations, and OFAC for IEEPA violations.[20] But reporting to those agencies without promptly reporting the same conduct to CES will not allow the company to benefit from this Policy governing criminal resolutions.

C. APPLICATION TO FINANCAL INSTITUTIONS

The new Policy applies to all business organizations, including financial institutions. The 2016 Guidance did "not apply to financial institutions," and financial institutions were directed to report possible misconduct to the Asset Forfeiture and Money Laundering Section (now the Money Laundering and Asset Recovery Section) of DOJ or to a U.S. Attorney's Office, who in turn would consult with CES or other parts of the National Security Division.[21] With no specific policy covering their disclosure of export control or sanctions violations under the 2016 Guidance, financial institutions would be credited for their voluntary disclosure as one of the many factors evaluated when prosecuting any business organization for any type of crime.[22] Under the new Policy, financial institutions can self-disclose to CES and receive the benefits of this Policy.[23]

D. APPLICATION TO MERGERS AND ACQUISITIONS

The Policy explicitly covers disclosures in the context of mergers and acquisitions when a company discovers misconduct through its due diligence, if the company voluntarily discloses the information, implements an effective compliance program, and otherwise conforms to the Policy's requirements.[24] The Policy will apply "in appropriate instances" when a company learns of misconduct after the transaction through "post-acquisition audits or compliance integration efforts," when the same requirements are met.[25] The Policy does not elaborate on what facts may cause post-acquisition discovery of misconduct to be "appropriate" such that the Policy would apply.

IMPLICATIONS

As a result of the new Policy, companies—including for the first time financial institutions—now have clearer expectations regarding the consequences of self-reporting possible export control or sanctions violations to DOJ and the possible outcome of that reporting.

The Policy states that it applies to "willful" violations, which are generally those violations where the person or company committing the offense acts with knowledge that it is illegal.[26] Willfulness is a necessary element for a criminal export control or sanctions penalty, and it generally separates civil enforcement actions from criminal enforcement actions.[27] Evidence establishing or refuting willfulness is often nuanced and the result of an in-depth investigation, and decision-makers within a company will often only be aware of limited facts at the time they must decide whether to report possible misconduct and to whom. Analyzing willfulness is also more complicated when evaluating the criminal liability of a corporation. As a practical matter, companies may consider reporting possible violations directly to DOJ before they have the ability

to discern whether the conduct by its particular employees or collectively was willful in order to ensure their voluntary self-disclosure is prompt and that it occurs before there is an imminent threat of disclosure or a government investigation.

* * *

ENDNOTES

1 U.S. Dep't of Justice, National Security Division, "Export Control and Sanctions Enforcement Policy for Business Organizations" (Dec. 13, 2019) https://www.justice.gov/nsd/ces_vsd_policy_2019/download. (the "2019 Sanctions Enforcement Policy").

2 22 U.S.C. § 2778; 50 U.S.C. § 4801 *et seq.*; 50 U.S.C. § 1705.

3 2019 Sanctions Enforcement Policy at 2.

4 U.S. Dep't of Justice, Justice Manual § 9-47.120, "FCPA Corporate Enforcement Policy," https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120 ("FCPA Enforcement Policy").

5 U.S. Dep't of Justice, National Security Division, "Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations" (Oct. 2, 2016) (the "2016 Guidance").

6 2019 Sanctions Enforcement Policy at 2.

7 2016 Guidance at 8-9.

8 FCPA Enforcement Policy at § 9-47.120(1); Remarks by Principal Deputy Assistant Attorney General David Burns Announcing New Export Controls and Sanctions Enforcement Policy for Business Organizations (Dec. 13, 2019), http://justice.gov/opa/speech/principal-deputy-assistant-attorney-general-david-burns-delivers-remarks-announcing-new ("Burns Remarks").

9 2019 Sanctions Enforcement Policy at 3; FCPA Enforcement Policy at § 9-47.120(1); Burns Remarks.

10 2019 Sanctions Enforcement Policy at 3 n.8.

11 2019 Sanctions Enforcement Policy at 3-5.

12 2019 Sanctions Enforcement Policy at 4.

13 2019 Sanctions Enforcement Policy at 4 n.9.

14 FCPA Enforcement Policy at 9-47.120(3)(b) n.2; *United States* v. *Connolly*, No. 16 Cr. 0370 (CM), 2019 WL 2120523 (S.D.N.Y. May 2, 2019).

15 2019 Sanctions Enforcement Policy at 2.

16 2019 Sanctions Enforcement Policy at 6 & n.11.

17 2019 Sanctions Enforcement Policy at 2.

18 18 U.S.C. § 3571(d); 2019 Sanctions Enforcement Policy at 2 n.5.

19 2019 Sanctions Enforcement Policy at 2-3, 6; 2016 Guidance at 8.

20 2019 Sanctions Enforcement Policy at 1 n.3; Burns Remarks.

21 2016 Guidance at 2 n.3.

22 U.S. Dep't of Justice, Justice Manual § 9-28.900, "Principles of Federal Prosecution of Business Organizations: Voluntary Disclosures," https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.900.

23 2019 Sanctions Enforcement Policy; Burns Remarks.

24 2019 Sanctions Enforcement Policy at 3 n.7.

25 2019 Sanctions Enforcement Policy at 3 n.7.

26 2019 Sanctions Enforcement Policy at 1 & n.2, 3; *Bryan* v. *United States*, 524 U.S. 184 (1998).

27 22 U.S.C. § 2778(c); 50 U.S.C. § 4819(b); 50 U.S.C. § 1705(c).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
Nicolas Bourtin	+1-212-558-3920	bourtinn@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Sharon Cohen Levin	+1-212-558-4334	levinsc@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
James A. Earl	+1-202-956-7566	earlja@sullcrom.com
Adam J. Szubin	+1-202-956-7528	szubina@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com