ALERT MEMORANDUM

NSD Flags Its Role as the Front Door for National Security-Related Voluntary Self-Disclosures Under the New Department-Wide Corporate Enforcement Policy

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Rahul Mukhi
+ 212 225 2912
rmukhi@cgsh.com

WASHINGTON D.C.

Christopher R. Kavanaugh
+1 202 974 1867
ckavanaugh@cgsh.com

David A. Last
+1 202 974 1650
dlast@cgsh.com

Samuel Chang
+ 1 202 974 1816
sachang@cgsh.com

Chase D. Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

April 1, 2026

On March 30, 2026, the Department of Justice's National Security Division (NSD) issued a press release reinforcing that companies seeking to voluntarily self-disclose criminal violations of national security laws—including export control and sanctions laws, and foreign investment and foreign telecommunication laws—should report those disclosures directly to NSD.[1] The announcement follows the Department of Justice's (DOJ) March 10, 2026 release of its first-ever Department-wide Corporate Enforcement Policy (CEP), which established a unified framework for how DOJ evaluates corporate voluntary self-disclosures, cooperation, and remediation across all DOJ components, except the Antitrust Division.[2]

[1] Press Release, "Reporting Voluntary Self-Disclosures of Violations of National Security Laws Under the Department-wide Corporate Enforcement Policy" (March 30, 2026), *available at* https://www.justice.gov/opa/pr/reporting-voluntary-self-disclosures-violations-national-security-laws-under-department-wide.

[2] Press Release, "Department of Justice Releases First-Ever Corporate Enforcement Policy for All Criminal Cases" (March 10, 2026), available at https://www.justice.gov/opa/pr/department-justice-releases-first-ever-corporate-enforcement-policy-all-criminal-cases. For further detail, *see also* Cleary Gottlieb Steen & Hamilton LLP, DOJ Releases First Department-Wide Corporate Enforcement Policy (Mar. 13, 2026), available at https://www.clearygottlieb.com/-/media/files/alert-memos-2026/doj-releases-first-department-wide-corporate-enforcement-policy.pdf (hereinafter, "Cleary Alert on CEP, dated March 13").

Summary of the Press Release

NSD's press release signals that NSD is staking out its position as the primary intake point for self-disclosures involving criminal violations of a broad swath of national security-related offenses—areas where companies often look to other agencies, such as the Department of the Treasury's Office of Foreign Assets Control (OFAC), the Department of Commerce's Bureau of Industry and Security (BIS), the Federal Communications Commission (FCC), or the Committee on Foreign Investment in the United States (CFIUS). The press release also suggests that other DOJ components may similarly declare their purview over certain voluntary self-disclosures, likely along the lines of the Justice Manual's approval, consultation, and notification requirements.

— **NSD as the Central Reporting Channel for National Security Violations.** NSD's press release makes clear that the Division views itself as the appropriate recipient of voluntary self-disclosures for criminal violations spanning export control laws, including the Export Control Reform Act (ECRA) and the Arms Export Control Act (AECA), sanctions laws, including the International Emergency Economic Powers Act (IEEPA), provision of material support to or financing of foreign terrorist organizations, and criminal violations in connection with CFIUS and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom). Within these categories, NSD repeatedly emphasizes preventing the unlawful export of sensitive goods and services and unlawful transactions with sanctioned countries and designated entities, suggesting the Division's prioritization of these types of violations. Notably, NSD omitted mention of the new DOJ's Data Security Program and Bulk Data Rule, which is also an IEEPA offense, and raises the question of whether—and to what extent—DOJ is investigating and enforcing potential criminal violations of the rule.

— **Alignment with the Department-Wide CEP**. The announcement underscores that NSD's former voluntary self-disclosure policy, the Enforcement Policy for Business Organizations, announced in 2016 and updated periodically, has now been replaced by the Department-wide CEP. The CEP, released in March, established for the first time a single, consistent framework governing how all DOJ components—including all 93 U.S. Attorney's Offices and divisions of "Main Justice," with the exception of the Antitrust Division—evaluate voluntary self-disclosures, the quality of a company's cooperation, and the adequacy of its remediation efforts. [3] NSD's press release also provides a potential reference point for companies to identify the appropriate DOJ component for voluntary self-disclosures under the new CEP.[4]

Practical Implications for Companies Facing Potential National Security Violations

The announcement raises important strategic considerations for companies navigating potential violations. Historically, a company that discovered an apparent sanctions violation might have self-disclosed to OFAC, and a company that uncovered an export control issue might have gone to BIS. NSD's press release makes clear that, where criminal liability is at stake, companies should be engaging directly with NSD—potentially in addition to, rather than instead of, the relevant regulatory agency. Companies should carefully and thoroughly weigh the available benefits of the CEP and self-disclosure to NSD against the risks and burdens of engaging with an additional enforcement body, and

[3] The CEP is organized into three parts: (i) guidance on obtaining a declination under the CEP, (ii) guidance on DOJ's approach to a "near miss" voluntary self-disclosure or presence of aggravating factors; and (iii) guidance on how DOJ will approach resolutions in other cases. While NSD's former policy similarly encouraged companies to voluntarily self-disclose to NSD violations of ECRA, AECA, and IEEPA, the CEP further incentivizes corporate self-disclosure by guaranteeing more significant benefits. *See* Cleary Alert on CEP, dated March 13.
[4] *See* Cleary Alert on CEP, dated March 13.

should seek counsel with experience across these agencies.

Key Takeaways

Companies with operations touching export-controlled goods or technology, sanctions-restricted jurisdictions or parties, CFIUS mitigation agreements, or Team Telecom obligations should take note of NSD's announcement and consider the following steps:

— Review internal compliance programs and escalation protocols to ensure that potential national security-related violations are investigated and flagged for assessment of whether a voluntary self-disclosure to NSD is appropriate—in addition to any disclosure that may be made to the relevant regulatory agency.

— Review the specific requirements and expectations of NSD under the CEP, including the timelines and substantive elements that DOJ considers in evaluating whether a disclosure qualifies for the declination of prosecution, a Non-Prosecution Agreement, or other favorable treatment under the CEP, and engage experienced advocacy and guidance where appropriate.

Conclusion

NSD's press release is an indication that NSD intends to be a central player in the corporate enforcement landscape and views itself as the appropriate front door for companies seeking to self-disclose potential violations of national security laws. Companies operating in regulated sectors should consider this when devising their compliance, internal investigation, and disclosure strategies.

This article was prepared with contributions from Cleary associates, Joie Goodman and Emily Janikowski.

…

CLEARY GOTTLIEB