Published on *The National Law Review* https://natlawreview.com

Technology Protection is a Core National Security Priority: BIS Strengthens Its Policy on Disclosures

Article By:

Fatema K. Merchant

Julien Blanquart

Recently, the Department of Commerce issued a memo, emphasizing that "technology protection is a core national security priority" and how companies that choose not to disclose significant violations of export regulations may have to bear concrete costs for non-disclosure. This memo highlights the continued focus to control U.S. technology security breaches, especially in the semiconductor and advanced computing industries.

On Voluntary Self-Disclosure

The Bureau of Industry and Security ("BIS")'s memo, issued on April 18, explains the incentive structure for voluntarily disclosing significant potential violations of the Export Administration Regulations ("EAR").

BIS reiterates that fully cooperating and disclosing potential violations in a timely manner will substantially reduce applicable civil penalties. That is because a disclosure will be considered a "mitigating factor" when assessing civil penalties. Many companies decide to disclose violations to receive that benefit. But there is a flip side to that calculus. BIS makes clear that if a company decides not to disclose after uncovering significant violations and BIS discovers the violations, the agency will consider non-disclosure as an "aggravating factor" when making penalty determinations. Based on the settlement guidelines, this could result in a sharply increased monetary penalty.

On Disclosures Concerning Others

BIS emphasized that protecting U.S. technologies from being used by adversaries for malign purposes is a "shared endeavor." In addition to the policy on self-disclosure, BIS announced incentives for individuals and entities to inform the agency of any potential violations of others through its confidential reporting form. BIS clarifies that disclosing violations by others could be considered a mitigating factor for the disclosing party in any future enforcement action against that party.

Additionally, BIS notes that the Financial Crimes Enforcement Network ("FinCEN") has a strong

whistleblowing policy and may financially reward individuals, in the United States and abroad, if they notify U.S. violations to the U.S. government that lead to enforcement action.

National Law Review, Volume XIII, Number 116