
Hughes Hubbard & Reed

\$140M US Export Controls Enforcement Action for ‘Reason to Know, Including Awareness of a High Probability’ Violations

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Attorney advertising. This advisory is for informational purposes only and is not intended as legal advice. Prior results do not guarantee a similar outcome. For more information: <https://www.hugheshubbard.com/legal-notice>.

July 29, 2025 – On July 28, the U.S. Department of Justice’s National Security Division and the Department of Commerce’s Bureau of Industry and Security (BIS) jointly announced resolutions of parallel criminal and administrative investigations of Cadence Design Solutions Inc. for more than \$140 million in fines, penalties and forfeiture. Of this amount, \$95 million is attributable to the BIS resolution — making it the largest stand-alone BIS corporate penalty in more than two years. The three key takeaways for export controls compliance professionals are:

- This settlement underscores our prior guidance that export controls risk assessments should be both dynamic and holistic, in that this settlement revolved around local employees’ efforts to re-route sales to a listed customer through front companies;
- BIS will expect companies subject to U.S. export control laws to review the facts of this settlement (summarized below), which to BIS considered to establish the company’s “reason to know, including awareness of a high probability”; and
- Self-certifications (here, a Letter of Assurance and end-use certifications) are insufficient to overcome “red flags” absent risk-based due diligence.

We summarize below the underlying facts and lessons learned.

First-Ever Significant Corporate Resolution Leveraging the Full Definition of “Knowledge”

The BIS resolution is also the first significant corporate resolution, following a \$5.8 million resolution on Aug. 15, 2024, expressly based on the full definition of “knowledge” under the U.S. Export Administration Regulations (EAR), which creates liability — even without proof that an exporter had actual knowledge — when a company has “reason to know” and “an awareness of a high probability” that an export was destined for a prohibited recipient. This guilty plea agreement and administrative settlement agreement, along with the prior resolution, directly answer criticism levied at BIS from members of Congress at the end of 2024 for failing to have leveraged the full definition of knowledge in its enforcement activity.

In the context of these investigations, Cadence admitted to having a “reason to know, including awareness of a high probability,”¹ that exports were being sent — indirectly through front companies Central South CAD Center (CSCC) and Phytium Technology Co. Ltd. — to a prohibited end user, the National University of Defense Technology (NUDT), a Chinese university connected to China’s military, under the catchall provision applicable to entities on the BIS Entity List.² The NUDT had been on the Entity List since Feb. 18, 2015, due to its use of U.S. technology to produce supercomputers “believed to be used in nuclear explosive activities.”³

Cadence also admitted to violating General Prohibition 10 in causing the transfer of hardware, software and technology from one front company to another with “knowledge” of a prior violation of the EAR⁴ and the inchoate offense of attempting further violations.⁵

Key Takeaways: What Facts Evidence a “Reason to Know, Including an Awareness of a High Probability”?

In BIS’ settlement agreement with Cadence, the following facts established a “reason to know, including an awareness of a high probability” of EAR violations:

- Employees knew that the NUDT shared personnel with CSCC.
- Equipment sold or loaned to CSCC was installed on the NUDT campus.
- The address for CSCC was a close match for that of the NUDT campus.
- Internal employee correspondence included instructions to use “CSCC” when writing in English and “NUDT” when writing in Chinese.
- CSCC was a “key account,” and through many business and social interactions with CSCC personnel, local sales and technical support employees of Cadence’s China subsidiary knew CSCC employees had ties to the NUDT.
- Overseas training for CSCC employees was organized by Cadence and paid for by the NUDT.
- Cadence’s China employees corresponded with an NUDT person regarding CSCC sales.
- Cadence’s China employees provided on-site technical support at NUDT locations for hardware sold to CSCC — and described the NUDT campus as a military installation.
- Certain Cadence employees were aware of payment and credit issues with CSCC and CSCC’s lack of public presence or credit record.
- According to the settlement, “a now-former Vice President and Deputy General Counsel” facilitated the sales team’s assignment of intellectual property rights from CSCC to Phytium and directed that “of course the email addresses should all be @phytium.com.cn corporate addresses.”
- Another Cadence employee referred internally to CSCC and Phytium as “the same customer.”

Neither a letter of assurance that Cadence received from CSCC nor end-use certifications obtained later from Phytium were sufficient to protect Cadence from the above red flags.

What’s Next?

Following the enforcement “playbook” used in other high-probability-based enforcement regimes, companies subject to U.S. export controls should appreciate that BIS expects others in industry to take lessons from this settlement.

The settlement underscores the importance of dynamic and holistic assessments of export controls diversion risks — especially looking at changes to customer relationships around key events — and ensuring that legacy assessments of enforcement risks are recalibrated in light of this significant July 28 corporate resolution for more than \$140 million. An object of such risk assessments is to identify where, and based on what information, there might be red flags indicating a risk of knowledge of a potential violation of the EAR that require more than self-certifications from counterparties to mitigate.

Some suggested resources for doing this are:

- Our Red Flags Rising podcast episode "[FRESH LOOKS - Export Controls Risk Assessments](#)"
- Our prior "Fresh Looks" post with the NYU Program on Corporate Compliance and Enforcement, "[Know Your Customer, But Also Yourself: A Fresh Look at Sanctions & Export Controls Risk Assessments in the Era of the 'New FCPA'](#)"
- Our prior article featured on the cover of the April 2025 issue of WorldECR magazine [explaining the full definition of "knowledge" under the EAR](#), including "reason to know" and "an awareness of a high probability."

* * * *

Hughes Hubbard's Sanctions, Export Controls & and Anti-Money Laundering practice focuses on designing and implementing risk-based programs to identify, assess and mitigate corporate compliance and enforcement risks. We are happy to discuss how we can help.

[The BIS press release, with a link to the settlement documents, is here.](#)

[The DOJ NSD press release, with a link to the plea agreement and criminal information, is here.](#)

-
1. 15 C.F.R. § 764.2(e) (acting with "knowledge" of a violation); see § 772.1 (defining "knowledge"). ↩
 2. 15 C.F.R. § 744.11 (a strict-liability offense on its own, but which can also be violated "knowingly" when combined with § 764.2(e)). ↩
 3. 15 C.F.R. § 744.2(a). ↩
 4. 15 C.F.R. § 736.2(b)(10). ↩
 5. 15 C.F.R. § 764.2(c). ↩

Related People



Michael H. Huneke

Related Areas of Focus

[Sanctions, Export Controls & Anti-Money Laundering](#)