



# Trade Matters

## Lowenstein Sandler's Global Trade & Policy Newsletter

November 2021

Share:



### 1. New Cybersecurity Export Controls From BIS Go Into Effect in January

The Bureau of Industry and Security (BIS) has released an **interim final rule**, establishing new export controls on certain cybersecurity items and creating a new license exception for those exports. The rule establishes greater restrictions on items that can be used for “malicious cyber activities” such as surveillance, espionage, and other actions that disrupt, deny, or degrade the network or devices on the network. The rule creates the new Export Administration Regulations License Exception “Authorized Cybersecurity Exports” (ACE). License Exception ACE will not apply if the exporter, reexporter, or transferor has reason to know at the time of the transaction that the cybersecurity item will be used to affect the confidentiality, integrity, or availability of information or information systems without authorization by the owner, operator, or administrator of the information system.

These changes will go into effect on January 19, 2022, and will align U.S. cybersecurity restrictions with controls previously agreed to at the multilateral Wassenaar Arrangement. Companies have until Dec. 6 to provide comments to BIS on the changes.

### 2. Recent Enforcement Actions for Russian Transactions Violating U.S. Laws

- Vorago Technologies will pay a **civil fine of \$497,000 and have its export privileges denied for three years** to settle the unauthorized export of radiation-hardened silicon wafers. Vorago allegedly engaged in a conspiracy with Russian company Cosmos Complect to avoid U.S. export controls by selling and shipping to a company in Bulgaria. However, these exports were ultimately destined for

### Contact Us

for more information about any matters in this newsletter:

#### Doreen M. Edelman

Partner  
Chair, Global Trade & Policy  
202.753.3808  
[dedelman@lowenstein.com](mailto:dedelman@lowenstein.com)

#### Laura Fraedrich

Senior Counsel  
202.753.3659  
[lfraedrich@lowenstein.com](mailto:lfraedrich@lowenstein.com)

#### Abbey E. Baker

Counsel  
202.753.3806  
[abaker@lowenstein.com](mailto:abaker@lowenstein.com)

#### Andrew Bisbas

Counsel  
202.753.3807  
[abisbas@lowenstein.com](mailto:abisbas@lowenstein.com)

#### Christian C. Contardo

Associate  
202.753.3804  
[ccontardo@lowenstein.com](mailto:ccontardo@lowenstein.com)

Russia, and issued a license from BIS. BIS stated that it will vigorously pursue companies like Vorago that attempt to subvert U.S. export licensing requirements.

- Cameron International, a Texas-based subsidiary of oil services company Schlumberger Ltd., agreed to pay **approximately \$1.4 million to settle allegations** of U.S. sanctions violations for providing services to Russian energy firm Gazprom-Neft Shelf. Managers of Cameron International approved contracts for its Romania-based subsidiary to supply goods to Gazprom-Neft Shelf's Prirazlomnaya platform, an oil-producing Russian Arctic offshore project, in violation of **Directive 4** issued by the Office of Foreign Assets Control (OFAC) pursuant to Executive Order 13662. This enforcement action highlights the importance of U.S. firms with international operations evaluating the totality of their business processes for risk exposure.

### 3. California Jury Hits New Jersey Company With \$8 Million FCA Verdict for Import Violations

False Claims Act (FCA) cases continue to expose import violations, as in the case of Sigma Corp., a New Jersey-based waterworks and fire protection company. An eight-person jury unanimously found that Sigma violated the FCA by knowingly making false statements to avoid paying 182.9 percent antidumping duties when importing Chinese-made pipe fittings. According to the whistleblower, Sigma has deprived the United States of approximately \$200 million since 2004 by evading the duties.

### 4. Brain Computer Interface Technologies May Soon Be Subject to Export Controls

BIS is seeking **public comments** on a proposed rule that would add brain-computer interface (BCI) technologies to the Commerce Control List as an emerging technology. BCI technologies function as a direct communication pathway between an enhanced or wired brain and an external device, sending information in both directions, and has potential application in the multimedia, entertainment, medicine, and military industries. The agency is seeking feedback addressing (1) what specific uniform standards for BCI technology should be adopted; (2) whether the U.S. is the leading developer of BCI technology; (3) whether the technology is commercially available in other countries; (4) what types of ethical or policy issues will likely arise from the use of BCI technology; and (5) what impact export controls would have on U.S. technology leadership. BIS also hopes to better understand which aspects of BCI technology should be monitored and whether additional government policies, regulations, and industry standards are needed before the technology becomes widely and commercially available. Comments on this proposed rule are due by December 10.

### 5. Biden Administration National Security Policy Review and Guidance

- The U.S. Treasury Department released the results from its comprehensive **2021 sanctions review** and issued recommendations to ensure the continued efficacy of U.S. sanctions programs in supporting U.S. national security

**Megan C. Bodie**

Administrative Coordinator

202.753.3809

[mbodie@lowenstein.com](mailto:mbodie@lowenstein.com)

## Subscribe—and stay in the know!

If you would like to update your mailing preferences for Lowenstein Sandler communications, please [click here](#).

[MANAGE MY PREFERENCES](#)

interests in future years. Potential challenges include increasing risks posed by cybercriminals, new payments systems, and digital assets, as well as the “impact of sanctions on the flow of legitimate humanitarian aid to those in need.” The recommendations to address these challenges and to ensure continued effectiveness of sanctions programs are: (i) adopt a structured policy framework linking sanctions to a clear policy objective; (ii) engage in multilateral coordination when possible; (iii) calibrate sanctions to prevent unintended economic, political, and humanitarian impact; (iv) expand existing outreach to ensure sanctions are easily understood, enforceable, and, where possible, reversible; and (v) invest in modernizing the Treasury Department’s sanctions technology, workforce, and infrastructure, especially with respect to digital assets and services.

- The Treasury Department released reports providing **virtual currency and ransomware guidance** by the [Office and Foreign Assets Control \(OFAC\)](#) and the [Financial Crimes Enforcement Network \(FinCEN\)](#). Publication of OFAC guidance often corresponds with increased enforcement in the area highlighted by the guidance. The guidance emphasizes that U.S. sanctions apply to all those operating in the virtual currency space, including tech companies, digital currencies exchanges, wallet providers, digital currency miners, and administrators. The government also has established a ransomware resource center at [stopransomware.gov](http://stopransomware.gov) to assist individuals and organizations.
- The National Counterintelligence and Security Center (NCSC) is [raising awareness of national security risks](#) for U.S. companies working in five emerging technology sectors: artificial intelligence, quantum computing, biotechnology, semiconductors, and autonomous systems. NCSC specifically identified **risks posed by Chinese and Russian actors**, including companies linked to government, military, and intelligence services. NCSC highlighted overt and hidden links between Chinese companies, Chinese intelligence services, and universities that the government of China uses to obtain U.S. technology. NCSC also disclosed Russian government methods to acquire U.S. technology, including technology transfers through joint ventures with U.S. companies and requirements that companies seeking to do business in Russia turn over their source code. According to NCSC, the U.S. government is not prohibiting companies from doing business with Chinese or Russian companies but rather is ensuring that U.S. companies are aware of risks and potential vulnerabilities as they consider business, research, or other opportunities with Chinese and Russian organizations. NCSC also provides resources and guidance that companies can use to mitigate counterintelligence vulnerabilities.

**Trade tip of the month:** Importers have until December 1, to submit comments on the Office of the United States Trade Representative’s (USTR) new, but narrow, exclusion renewal request process. USTR will use this process to decide whether it will extend up to 549 Section 301 exclusions that were previously granted but have since expired. The list of exclusions that are up for renewal can be found [here](#). Any exclusion that is ultimately reinstated as a result of this process will apply retroactively to October 12, 2021. USTR will conduct its review on a case-by-case basis with a focus on whether the particular

product remains available only from China. More information about requirements and how to submit comments can be found [here](#).

## Additional Resources

- **Article:** "Key Business Considerations for U.S. Global Trade Policy"  
November 1, 2021  
*Risk Management*  
Doreen M. Edelman, Abbey E. Baker, and Christian C. Contardo
- **Article:** "Startups Need a Grasp of U.S. Trade Controls"  
October 21, 2021  
*CFO*  
Doreen M. Edelman and Abbey E. Baker
- **Client Alert:** "USTR Announces New Narrow Exclusion Renewal Process for Section 301 Tariffs"  
October 6, 2021  
*Lowenstein Sandler LLP*  
Doreen M. Edelman and Andrew Bisbas
- **Article:** "CMMC: An ounce of prevention is worth a pound of cure"  
October 5, 2021  
*Security*  
Christian C. Contardo

Follow us on:



[lowenstein.com](https://www.lowenstein.com)

NEW YORK

PALO ALTO

NEW JERSEY

UTAH

WASHINGTON, D.C.

© 2021 Lowenstein Sandler LLP | One Lowenstein Drive, Roseland, New Jersey 07068 | +1 973.597.2500

If you would like to update your mailing preferences for Lowenstein Sandler communications, please [click here](#).

To unsubscribe from Lowenstein Sandler email communications, [click here](#).