Biden Administration Focus on Cybercrime Continues with Israeli Companies Added to Entity List, New Export Controls, and Cryptocurrency Sanctions

Written by Luciano Racco, Anthony D. Mirenda, Anna Maria Annino

November 12, 2021

On November 3, 2021, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") added two Israeli entities to the Entity List due to malicious cyber activities. In its press release, BIS stated that the designation of Israeli companies NSO Group and Candiru was based on evidence that these entities developed and supplied spyware to foreign governments, which was then used for malicious surveillance, including targeting journalists and activists. This addition aligns with the Biden administration's increased use of the Entity List to target human rights abuses, especially related to cybercrime and unlawful surveillance. A Russian entity (Positive Technologies) and a Singaporean entity (Computer Security Initiative Consultancy PTE. LTD) were also added to the Entity List for selling cyber tools used to gain unauthorized access to information systems. While the addition of Israeli entities is not common – the vast majority of entities on the Entity List are Chinese and Russian – Israeli entities were previously added to the list in 1997, 2016, and 2020, for a total of 12 entities to date.

BIS uses the Entity List to restrict the export of certain items subject to the Export Administration Regulations ("EAR") to certain end-users. As a result of the November 3, 2021 action, BIS has imposed a license requirement for the export of all items subject to the EAR to these entities, including EAR99 items, with a presumption of denial, and no license exceptions will be available. The BIS Entity List is distinct from the Specially Designated Nationals and Blocked Persons List ("SDN List") administrated by the Office of Foreign Assets Controls ("OFAC") of the U.S. Department of the Treasury. The Entity List restricts the export of U.S.-origin items, while the SDN List more broadly prohibits U.S. persons from engaging in most transactions with SDNs. Entities on the Entity List may also be separately subject to OFAC sanctions.

Cybercrime has been a key area of focus for the Biden administration. On October 21, 2021, BIS released an interim final rule which adds new export controls on "intrusion software," which are "tools that could be used for surveillance, espionage, or other actions that disrupt, deny or degrade the network or devices on it." These items are now controlled for National Security ("NS") and Anti-terrorism ("AT") reasons. While items subject to NS and AT controls are ineligible for export to most countries without the exporter first receiving a license, BIS has also added a new License Exception Authorized Cybersecurity Exports ("ACE") to allow for exports of otherwise covered items for legitimate cybersecurity purposes to many end-users. However, Group E:1 and E:2 countries (Cuba, Iran, North Korea and Syria), certain Group D government end-users (such as China, Russia, Saudi Arabia and the UAE), and certain non-governmental end-users in Russia and China are excluded from the license exception. Exports under License Exception ACE to Group D government end-users that are also included in Country Group A:6 (which includes Israel) are permitted only in limited circumstances.

As reported earlier by Foley Hoag, OFAC also recently released updated guidance related to sanctions and ransomware and also added the first cryptocurrency exchange to the SDN List. Cryptocurrency is often the payment mechanism of choice for hackers seeking a ransom to release a victim's data. Continuing this focus, on November 8, 2021, OFAC added several individuals and entities to the SDN List. The designated entities include Chatex, a cryptocurrency exchange, and its affiliated entities, which were designated for facilitating ransomware transactions. The designation also includes multiple digital currency addresses associated with Chatex. Digital currency addresses are potential destinations for the transfer of digital currency and are stored in a virtual "wallet" which allows the user to send, hold, and receive money. More information on digital currency, wallets, and addresses in the context of OFAC sanctions programs is available here.

Companies with questions about these new cyber-related actions or how to ensure compliance with U.S. sanctions and export control regulations should contact a member of Foley Hoag's Trade Sanctions & Export Controls practice.

RELATED INDUSTRIES

- Technology

RELATED PRACTICES

- Trade Sanctions & Export Controls
- Cybersecurity Incident Response
- Privacy & Data Security
