



EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

February 1, 2024 - Volume 19, Issue 3

CELEBRATING OVER
30
YEARS

Businessman Arrested for Scheme to Illegally Export Semiconductors and Other Controlled Technology to Russia

Thursday, January 18, 2024

**For Immediate Release
Office of Public Affairs**

Defendant Allegedly Used Network of Businesses in China and Other Countries to Illegally Transfer Hundreds of Thousands of Semiconductors to Sanctioned Business with Ties to Russian Military and Russian Intelligence Agencies Ilya Kahn, 66, a citizen of the United States, Israel and Russia, and resident of Brooklyn, New York, and Los Angeles, California, was arrested yesterday in Los Angeles for his alleged involvement in a years-long scheme to secure and unlawfully export sensitive technology from the United States for the benefit of a Russian business. The business was sanctioned by the U.S. government following Russia's unprovoked invasion of Ukraine in February 2022 and whose clients include elements of the Russian military and the Federal Security Service (FSB), the main successor agency to the Soviet Union's KGB.

According to court documents, Kahn is charged by criminal complaint with conspiracy to violate the Export Control Reform Act (ECRA). Kahn will make his initial appearance in the Central District of California.

"Mr. Kahn stands accused of repeatedly exporting sensitive technology to Russia before, during, and after Russia launched its unprovoked invasion of Ukraine," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Violations of U.S. sanctions and export control laws that aid Russia and other hostile powers endanger our nation's security and will be met with the full force of the Justice Department."

"This arrest reflects our continued aggressive enforcement of export control violations involving the Russian military and the Federal Security Service," said Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department's Bureau of Industry and Security (BIS). "Stopping the flow of semiconductors and sensitive technologies to those aiding Russia's unjust war in Ukraine is a critical priority for BIS and our Disruptive Technology Strike Force partners."

"As alleged, Kahn illegally sent specialized technology from the United States to a Russian semiconductor manufacturer with ties to multiple other sanctioned Russian entities and did so by circumventing U.S. export laws and regulations," said U.S. Attorney Breon Peace for the Eastern District of New York. "Evading U.S. export regulations to send goods to benefit the Russian military complex presents a danger to our national security and our allies and partners abroad. We will continue to use all of our law enforcement and national security tools to hold these enablers, both individuals and corporations, accountable for flouting the rule of law."

*(*Continued On The Following Page)*

NEWSLETTER NOTES

- [Businessman...](#)
- [Condemnations of Iran's...](#)
- [Frequently Asked Questions...](#)
- [United States Department of Commerce...](#)
- [NuDay Charity...](#)
- [Department of the Treasury](#)
- [Secretary Blinken's Remarks...](#)
- [JetBlue's Merger...](#)
- [Terrorist Desig...](#)
- [Imposing Sanction...](#)
- [For Immediate Rel...](#)
- [Businessman Arr...](#)
- [Virginia man co...](#)
- [Hossein Hatefi...](#)
- [Commerce Strengthens...](#)
- [For Immediate Release...](#)
- [01.24.2024...](#)
- [January 23, 2024...](#)
- [Fact Sheet...](#)
- [Firearms Export...](#)
- [BIS May...](#)
- [For Immediate...](#)
- [Ocean State...](#)
- [Washington Post...](#)
- [Chinese Nationals...](#)
- [New EIB Podcast...](#)

“As alleged, Kahn illegally sent specialized technology from the United States to a Russian semiconductor manufacturer with ties to multiple other sanctioned Russian entities and did so by circumventing U.S. export laws and regulations,” said U.S. Attorney Breon Peace for the Eastern District of New York. “Evading U.S. export regulations to send goods to benefit the Russian military complex presents a danger to our national security and our allies and partners abroad. We will continue to use all of our law enforcement and national security tools to hold these enablers, both individuals and corporations, accountable for flouting the rule of law.”

“This arrest marks the end of Ilya Khan’s alleged involvement in a years-long scheme to secure and export millions of dollars’ worth of sensitive technologies from the U.S. to Russia to be used by its military and intelligence services,” said Executive Assistant Director Larissa L. Knapp of the FBI’s National Security Branch. “Any attempt to circumvent U.S. laws, sanctions, and regulations will not be tolerated, and thanks to a coordinated interagency effort, our national security and our partners’ are stronger than ever.”

According to court documents, Kahn is the owner of Senesys Incorporated, which is based in California, and Sensor Design Association, which maintains a contact address in Brooklyn. As alleged in the complaint and other public filings, Kahn operated these two businesses – ostensibly involved in “security software development” and the testing of silicon wafers for military avionics and space users – through which he engaged in a years-long conspiracy to acquire and export sensitive and sophisticated electronics from the United States to a sanctioned Russian business without acquiring the appropriate licenses. The Russian business, Joint Stock Company Research and Development Center ELVEES (Elvees) was added to the Commerce’s Department’s Entity List in March 2022 and was sanctioned by the Treasury Department in September 2022 because of its critical role in facilitating Russia’s military and its invasion of Ukraine.

For example, according to the complaint, in 2019, Kahn exported multiple U.S.-origin microcontrollers to Elvees in Russia, and in 2022, he exported U.S.-origin network interface controllers and a radio-frequency transmitter to Elvees in Russia by way of a Hong Kong-based shipping company. Each of these items required an export license from the Commerce Department, which Kahn did not obtain, and were controlled for national security and anti-terrorism reasons.

As alleged, Kahn also arranged for Elvees to continue to receive semiconductors manufactured in Taiwan following Russia’s invasion of Ukraine in February 2022. Specifically, after the Taiwanese company that manufactured Elvees-designed semiconductors refused to ship those semiconductors to Russia, Kahn arranged for the semiconductors to be sent to the United States and then re-exported them to Russia, often through a shipping company based at John F. Kennedy International Airport in Queens, New York. Kahn also used Hong Kong and other locations around the world as transshipment points to evade U.S. export laws and regulations and to conceal the Russian end users.

*(*Continued On The Following Column)*

Even after Elvees was added the Entity List, Kahn continued to work with the company. In May 2022, Kahn emailed design guidance for an Elvees-branded microchip to a Taiwan manufacturer. Subsequently, Kahn shipped thousands of units of this microchip – through a New York-based shipper – to a Hong Kong shipping company, and then to a company located in mainland China. Kahn noted in communications with the Hong Kong shipping company that he received a “call from Russia” about the Chinese business to which he was directing the goods.

If convicted, Kahn faces a maximum penalty of 20 years in prison for conspiracy to violate the ECRA.

The FBI and Department of Commerce’s BIS New York Field Office are investigating the case. The U.S. Attorney’s Office for the Central District of California provided significant assistance.

Assistant U.S. Attorneys Craig R. Heeren, Artie McConnell, and Matthew Skurnik for the Eastern District of New York and Trial Attorney Scott Claffee of the National Security Division’s Counterintelligence and Export Control Section are prosecuting the case, with assistance from Litigation Analysts Joseph Levin and Mary Clare McMahon.

Today’s actions were coordinated through the Justice and Commerce Departments’ Disruptive Technology Strike Force and the Justice Department’s Task Force KleptoCapture. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation states. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia’s unprovoked military invasion of Ukraine.

A complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

<https://www.justice.gov/opa/media/1334321/dl?inline>

Condemnation of Iran’s Attacks in Erbil

01/15/2024 08:55 PM EST

Matthew Miller, Department Spokesperson

The United States strongly condemns Iran’s attacks in Erbil today and offers condolences to the families of those who were killed. We oppose Iran’s reckless missile strikes, which undermine Iraq’s stability. We support the Government of Iraq and the Kurdistan Regional Government’s efforts to meet the aspirations of the Iraqi people.

Frequently Asked Questions (FAQs) for:

“Export Controls on Semiconductor Manufacturing Items” (SME IFR) And “Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use;

Updates and Corrections” (AC/S IFR) Public Inspection at the Federal Register: October 18, 2023

Publication in the Federal Register: October 25, 2023

Effective: November 17, 2023

Comments Due: January 17, 2024

FAQ Date: December 29, 2023

These Interim Final Rules (IFRs) address comments received in response to the “Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use” (October 7 IFR)(87 Fed. Reg. 62186, October 13, 2022) and amend the Export Administration Regulations (EAR) to implement export controls on semiconductor manufacturing equipment (SME), advanced computing items, and supercomputers more effectively and to address ongoing national security concerns that items in these rules can be used for military modernization and other applications such as the development and production of weapons of mass destruction (WMD).

I. General

I.Q1. A commenter requested that BIS should consider the impact on potential public benefits derived from advanced technologies developed through cross-border cooperation, especially in the realm of global health and environmental issues.

I.A1. BIS has considered this impact and notes that existing licensing policies are designed to be flexible, enabling authorization of certain types of collaboration when warranted, such as to maintain supply chains, assuming the risks of diversion to prohibited end uses are sufficiently mitigated. In addition, BIS has adjusted the scope of certain controls, e.g., SME end use control in § 744.23(a)(4), expanded license exception eligibility, and added exclusions to the controls in both §§ 744.6 and 744.23.

I.Q2. The BIS press release states “Expanding license requirements for semiconductor manufacturing equipment to apply to additional countries beyond the PRC and Macau, to 21 other countries for which the U.S. maintains an arms embargo.” However, supplement no. 1 to part 740, Country Group D:5 has 23 countries listed and minus China that makes 22 countries. Why did the press release state 21 other countries instead of 22?

*(*Continued On The Following Column)*

I.A2. While BIS has not yet removed Cyprus from Country Group D:5, it is effectively removed because it has been removed from 22 C.F.R. 126.1 of the State Department’s International Traffic in Arms Regulations (ITAR). Currently Country Group D:5 has 23 countries but subtracting China and Cyprus results in 21 countries.1

I.Q3. Do worldwide controls include exports to the United States?

I.A3. No, because the definitions for “export” and “reexport” in § 734.13 and § 734.14 do not include shipments or transmissions into the United States. See excerpts from definitions below.

§ 734.13(a)(1): An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner § 734.14(a)(1): An actual shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner II. AC/S IFR Revised Parameters

Performance density: 3A090.a.2 and b. Technical Note 4 of Export Control Classification Number (ECCN) 3A090: ‘Performance density’ is ‘TPP’ divided by ‘applicable die area’. For purposes of 3A090, ‘applicable die area’ is measured in millimeters squared and includes all die area of logic dies manufactured with a process node that uses a non-planar transistor architecture.

II.Q1. How should we measure the die size? Physical die area that we can find on the product specification announced by the chip makers could be different from the die area defined in the rule. The current rule uses the area of ‘logic die’ that uses non-planar architecture.

II.Q1.a. Does the ‘logic die’ mean that we exclude area for Static random-access memory (SRAM), or the whole (nonseparable) die that has logic functions?

II.A1.a. Count the area of the whole nonseparable logic die – SRAM on the logic die should not be excluded from the area calculation.

II.Q1.b. If only certain parts of chips use non-planar architecture, should we still consider the whole die area?

II.A1.b. BIS is not aware of instances where a single logic die uses multiple transistor architectures. BIS can respond to concrete examples. For ‘chiplets’ you should count only the 1 Footnote 1 to Country Group D:5 in supplement no. 1 to part 740 states that “The list of arms embargoed destinations in this table is drawn from 22 CFR 126.1 and State Department Federal Register notices related to arms embargoes (compiled at www.pmddtc.state.gov/embargoed_countries/index.html) and will be amended when the State Department publishes subsequent notices. If there are any discrepancies between the list of countries in this table and the countries identified by the State Department as subject to a U.S. arms embargo (in the Federal Register), the State Department’s list of countries subject to U.S. arms embargoes shall be controlling.” Currently, 22 C.F.R. 126.1(r)(2) states “From October 1, 2023, through September 30, 2024, the policy of denial and the status of Cyprus as a proscribed destination is suspended.” area of each logic chiplet within the package using a non-planar architecture – the area of chiplets with a planar transistor architecture should be excluded from the calculation. Note: A chiplet is a tiny integrated circuit that contains a well-defined subset of functionality.

*(*Continued on the Following Page)*

It is designed to be combined with other chiplets on an interposer in a single package.

II.Q1.c. For chips with vertical structure, should we count areas for all levels (floors) of die or just the maximum of all levels of such die?

II.A1.c. For 'High Bandwidth Memory' (HBM), all this area should be excluded as HBM is memory, not logic. For 3D packaging of logic on logic, the area of all levels should be counted. BIS welcomes specific examples.

Note: High Bandwidth Memory (HBM) is a computer memory interface for 3D-stacked synchronous dynamic random-access memory (SDRAM)

III. License Exception NAC (Notified Advanced Computing)

III.Q1. Sometimes License Exception Notified Advanced Computing (NAC) requires a notification to BIS. What circumstances require notification under NAC?

III.A1. Exports and reexports authorized under License Exception NAC to Macau or a destination specified in Country Group D:5 (in supplement no. 1 to part 740 of the EAR), or to an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located, must meet the notification requirements under § 740.8(a)(2) of the EAR and identified by License Type C67 – (NAC) Notified Advanced Computing in the Automated Export System (AES). The NAC notification requirement does not apply to exports or reexports to any destination specified in Country Groups D:1 or D:4 (other than Macau or destinations also specified in Country Group D:5) nor does it apply to transfers (in-country) to any destination.

III.Q2. Do the requirements in License Exception NAC for the export, reexport, or transfer (in-country) of computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in Export Control Classification Number (ECCN) 3A090.b, apply to any ECCN 4A090 items not enumerated in ECCN 4A090.a? Paragraph .b in ECCN 4A090 (computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in 3A090.b) is reserved but the NAC eligibility paragraph for ECCN 4A090 makes computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in 3A090.b, eligible for NAC. Will BIS revise ECCN 4A090.b or the NAC eligibility paragraph for 4A090 to clarify this issue?

III.A2. Yes. Exporters should assess all computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in 3A090.b, against the requirements of License Exception NAC notwithstanding ECCN 4A090.b currently being reserved. BIS will revise ECCN 4A090.b to clarify this issue.

III.Q3. What do I need to include with my NAC notification submission via SNAP-R?

III.A3. The NAC notification application in SNAP-R must include certain information to allow for BIS to determine if the item in question otherwise meets the criteria for an item eligible for License Exception NAC. Required information to include in the NAC submission is as follows: **(*Continued on the Following Column)**

- a. Name of the exporter
- b. Point of Contact and contact information
- c. Item description, including model name/number
- d. Total Processing Performance of the item, as defined in 3A090
- e. Performance density of the item, as defined in 3A090; and
- f. Data sheet or other documentation showing how the item is designed and marketed (in particular, whether it is designed or marketed for datacenter or consumer use)
- g. Parties to the transaction (Ultimate and intermediate consignees, end user and purchaser)
- h. Volume and value
- i. Expected end use of the items

III.Q4. What if I am not the designer/manufacturer of the chip and do not have access to the performance density?

III.A4. When submitting your NAC notification via SNAP-R, provide authorization to allow BIS to contact the designer/manufacturer on your behalf to obtain this parameter. In most cases this will not be necessary as BIS will probably have this information.

III.Q5. How many items can I submit for a NAC notification?

III.A5. The NAC notification is limited to six items – same as commodity classification requests. BIS recommends limiting the notification to one model number per notification.

III.Q6. How many ultimate consignees and end users may I submit on one NAC notification?

III.A6. Only one ultimate consignee and one end user is allowed. NAC notifications which include more will be returned without action. A distributor may not be a party to the NAC notification.

III.Q7. How will I know if my NAC is approved?

III.A7. After the notification has been registered in SNAP-R and within twenty-five calendar days, BIS will inform you if a license is required. If BIS has not contacted you, then System for Tracking Export License Applications (STELA) (<https://snapr.bis.doc.gov/stela>) will, on the twenty-fifth calendar day following the date of registration, provide either confirmation that you can use License Exception NAC and a NAC confirmation number (Axxxxxx) to be submitted in AES or confirmation that you cannot use License Exception NAC and you must apply for a license to continue with the transaction.

III.Q8. BIS currently has the license exception NAC (Notified Advanced Computing) to authorize exports of certain advanced computing chips. Can we safely assume that all products eligible for NAC will be authorized for exports and reexports to Macau and Country Group D:5, and the 25-day review period only exists to check if the products actually satisfy parameters to be eligible for the NAC?

III.A8. No. BIS will review the NAC notifications for national security concerns and require a license application for any notifications that raise concerns. National security concerns could be based on many factors including the type of item, quantity, and the end user/end use.

(*Continued On The Following Page)

III.Q9. To make it less burdensome, does BIS plan to publish a list of advanced computing chips that are eligible for NAC?

III.A9. No, BIS does not intend to publish a list of chips at this time because the review process also considers additional factors, such as end users, end uses, and volume.

III.Q10. Would there be duplicative NAC notification requests for the same product from different exporters?

III.A10. Yes. Approval of the NAC notification request is only valid for the exporter who submitted the application. Therefore, it seems likely that more than one exporter will file a NAC notification for the same product.

III.Q11. How do I fill out the Electronic Export Information (EEI) Filing in the Automated Export System (AES) for License Exception NAC?

III.A11. Use the code C67 for NAC. For the ECCN, input the ECCN number – not the .z. For example, for a 3A001.z item, input 3A001. If a notification is required, then input the NAC confirmation number (Axxxxxx) issued by BIS in the license number block.

In addition, in § 758.1 of the EAR, the AC/S IFR added a new paragraph (g)(5) (Exports of .z items that meet or exceed the performance parameters of ECCN 3A090 or 4A090) for any item classified in ECCNs 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z. Section 758.1(g)(5) imposes a requirement to input “.z” as the first text to appear in the Commodity description block in the EEI filing in AES.

III.Q12. If I have a 5A002.z or 5A992.z item that is authorized under License Exception NAC, do I also need to comply with the requirements for license exception ENC?

III.A.12 Yes. Items classified under the .z paragraphs may sometimes have to meet the requirements of more than one provision of the EAR to be authorized for export. For items in Category 5 Part 2, they must meet both the requirements of license exception NAC and of license exception ENC. Thus, some items could require a license exception ENC classification request in addition to a NAC notification to be authorized for export without a license.

IV. 744.23 “Supercomputer,” “Advanced-node Integrated Circuits,” and Semiconductor Manufacturing Equipment End Use Controls
IV.Q1. A commenter stated that § 744.23(a)(4) (former § 744.23(a)(2)(v)) does not include “incorporation” of EAR99 items into Category 3B items. This commenter notes that the wording in § 744.23(a)(4) prohibits the “development” or “production” of Category 3B items. This commenter believes that if BIS wanted to prohibit the incorporation of EAR99 items (e.g., screws and tubing) into Category 3B items, it should have prohibited the incorporation of any item that is subject to the EAR into a Category 3B item under § 744.23(a)(4), just as it did in § 744.23(a)(2).

*(*Continued On The Following Column)*

IV.A1. BIS has narrowed the product scope in paragraph (a)(4) to items subject to the EAR and specified on the Commerce Control List (CCL), i.e., paragraph (a)(4) no longer controls EAR99 items. Such incorporation of EAR99 items would be addressed under end-use controls in § 744.23(a)(2), which controls all items subject to the EAR “when you know the items will be used in the “development” or “production” of ICs destined to a “facility” located in Macau or a destination specified in Country Group D:5 where “production” of “advanced-node ICs” occurs” or “where “production” of integrated circuits occurs, but you do not know whether “production” of “advanced-node ICs” occurs at such “facility.”” However, if the EAR99 part will be incorporated into a finished item, e.g., for repair, then it does not meet the “production” or “development” criteria.

IV.Q2. Is a license required under § 744.23(a)(2)(i) of the EAR to transfer or release EAR99 “technology” subject to the EAR, including technology for the operation, installation, maintenance, repair, overhaul, or refurbishing of any item, when the EAR99 “technology” is destined for use in the “development” or “production” of an integrated circuit at a “facility” where the “production” of “advanced-node integrated circuits” occurs (or any other end -use for which EAR99 items are controlled)?

IV.A2. Yes, a license is required to transfer or release EAR99 “technology” subject to the EAR under § 744.23(a)(2)(i) of the EAR because the scope of the license requirement for §744.23(a)(2)(i) is “any item subject to the EAR,” which includes EAR99.

IV.Q3. Scenario: Company A is a company headquartered in the U.S. or a Country Group A:5 or A:6 country. Company A produces “front-end integrated circuit “production” equipment” specified in a Category 3B ECCN. Company B is an integrated circuit “production” company headquartered in a Country Group D:5 destination. Company B asks Company A to supply commodities, software, or technology subject to the EAR to upgrade Company A’s equipment installed in a “facility” in a D:5 country where the “production” of integrated circuits occurs, but not where “advanced-node integrated circuits” occurs. Does Company A require a license under § 744.23(a)(4) (assume no other license requirement applies)? If yes, is Company A’s upgrade transaction eligible for the Temporary General License in supplement no. 1 to part 736 paragraph (d)(1) of the EAR?

IV.A3. The upgrade transaction would qualify as a “development” activity, and a license would be required under § 744.23(a)(4) of the EAR. However, in this situation, BIS would conclude that Company A is eligible for the TGL because the transaction does not reflect “indigenous “development” or “production” of a Category 3B” tool. Instead, the scenario is identical, in substance, to one in which Company A “develops” or “produces” an upgraded version of the tool in a D:5 country and then sells the upgraded tool to Company B, which – under the hypothetical facts provided – would be eligible for the TGL 1 in supplement no. 1 to part 736 paragraph (d)(1) of the EAR.

Even though Company B made the request for the equipment to Company A, that does not change the fact that Company A is still “directing” the shipment of the equipment under the authority of the TGL. In fact, Company A could direct another manufacturer, Company C, who is not a company headquartered in the U.S. or a Country Group A:5 or A:6 country and who produces the equipment that is subject to the EAR, to export the equipment to Company B under the TGL authority.

*(*Continued on the Following Page)*

IV.Q4. Scenario: Company A, located in China but headquartered in the U.S. or a Country Group A:5 or A:6 country, needs to upgrade or repair their SME, so they direct Company B, who is a Chinese headquartered company also located in China, to produce 3B001 parts or equipment. Could Company B transfer (in-country) the equipment or parts, at the written direction of Company A under the Temporary General License in supplement no. 1 to part 736 paragraph (d)(1) of the EAR?

IV.A4. Yes.

IV.Q5. The SME IFR sections “10. Revisions to § 744.6 Activities of U.S. Persons,” and “11. Revisions of § 744.23 “Supercomputer,” “advanced-node integrated circuits,” and semiconductor manufacturing equipment end use controls” discuss examples of facilities covered under the end-use controls in §§ 744.6 and 744.23. Can BIS verify that “facility” includes the following?

1) Facilities where “production” may occur beyond a fabrication facility (e.g., beyond the clean room or production floor); 2) Facilities where important late-stage product engineering or early-stage manufacturing steps (among others) may occur; and 3) “Development” and product engineering activities at R&D fabrication “facilities” that may not engage in volume manufacturing.

VI.A5. “Facility” does include 1 through 3 above. V. “U.S. Persons” Activities Controls V.Q1. The exclusion in § 744.6(d)(4) applies to a natural U.S. person. Does that mean that a U.S. entity, which is included in the definition of U.S. Person, is not covered under this exclusion, but only the natural U.S. persons who are employed by or acting on behalf of the U.S. entity?

V.A1. Correct, § 744.6(d)(4) only applies to a natural U.S. person and not to a U.S. entity.

V.Q2. How can an entity that is a U.S. person engage in such covered activities other than through its employees or personnel working on its behalf? Is the purpose of excluding a U.S. entity to eliminate personal liability for the individual U.S. Person, but not for the U.S. entity that is a U.S. Person?

V.A2. Yes, to eliminate discrimination against U.S. person employees of non-U.S. person entities headquartered in allied countries.

V.Q3. Assuming § 744.6(c)(2)(iii) in addition to servicing also covers authorizing or conducting activities, are authorizing or conducting activities limited to facilities where production of advanced-node ICs occurs, similar to how servicing is limited to such facilities pursuant to § 744.6(d)(5)?

V.A3. Yes, § 744.6(c)(2)(iii) applies to all three activities in § 744.6(c)(3)(i), not just servicing. The exclusion in § 744.6(d)(5) only applies to servicing (including installation) activities.

V.Q4. Based on the exclusion in § 744.6(d)(5), does § 744.6(c)(2)(iii) only cover facilities where production of advanced-node ICs occurs, or does it also cover facilities where production of ICs occurs, but you do not know whether production of advanced-node ICs occurs?

*(*Continued On The Following Column)*

V.A4. Section 744.6(c)(2)(iii) states “regardless of end use or end user,” therefore the type of facility is not relevant to the application of paragraph (c)(2)(iii).

V.Q5. Regarding the scope of the end use control in § 744.23(a)(2), BIS stated in its comments that the term “where ‘production’ . . . occurs” captured “R&D fabrication ‘facilities’ that may not engage in volume manufacturing of integrated circuits.” Our question involves clarity of this statement in relation to the EAR’s definitions of “production” and “development.” The EAR defines “development” as “all stages prior to serial production, such as . . . assembly and testing of prototypes [and] pilot production schemes.” Accordingly, if an R&D facility is engaged only in the manufacture of prototypes that are not intended for sale, and the R&D facility is not capable of serial production, is the R&D facility still considered a “facility” where “production” occurs and, therefore, captured by the end use control in Section 744.23(a)(2)? Or is it excluded from this end use control as it is solely a “development” facility?

V.A5. BIS encourages this commenter to submit additional details, such as through an Advisory Opinion request, to facilitate BIS’s assessment of whether the activity would qualify as “development” versus “production.”

VI. Regional Stability (RS) Controls and .z Export Control Classification Numbers (ECCNs)

VI.Q1. We understand that the AES EEI filing is mandatory for the .z category items for all Countries. Does that also apply to transactions below the USD 2500 threshold?

VI.A1. Yes.

VI.Q2. Do we need to include the .z in front of the article/commodity descriptions for all .z category items in the AES EEI filing as stated in the below screenshot?

For example, ECCN 3A001.z is described as:

“Any commodity described in 3A001 that meets or exceeds the performance parameters in 3A090.” Do we need to modify this description to: “.z Any commodity described in 3A001 that meets or exceeds the performance parameters in 3A090.”?

VI.A2. Yes.

VI.Q3. Do the .z items require licenses to countries other than Country Groups D:1, D:4, and D:5?

VI.A3. Yes. The .z entries are intended to control items that fall under 3A090/4A090 and another ECCN on the CCL. The .z paragraphs were created to retain both the original license requirements for that item plus the new RS-related license requirements from the October 17 th AC/S IFR, as well as related license exceptions. For example, 4A003.z controls items that meet both 4A003.b and 4A090. It requires a license to the same destinations as 4A003.b items plus the additional restrictions on 4A090 items. Outside of Country Group D:1, D:4, and D:5 countries, it is eligible for the same license exceptions as a 4A003.b item.

UNITED STATES DEPARTMENT OF COMMERCE
Assistant Secretary for Export Enforcement
Washington, D.C. 20230
Export Enforcement: 2023 Year in Review

At no point in history have export controls been more central to our collective security than right now. Advances in science and technology are poised to define the geopolitical landscape of the 21st century, with disruptive technologies like artificial intelligence and quantum computing at the forefront. Export Enforcement’s work to protect these advanced technologies from falling into the wrong hands is critical. To protect our national security, over the past calendar year, we:

Launched the Disruptive Technology Strike Force with the Department of Justice (DOJ) to protect U.S. advanced technologies from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran. The Strike Force brings together experienced agents and prosecutors in fourteen locations across the country, supported by an interagency intelligence effort in Washington, D.C., to pursue investigations and take criminal and/or administrative enforcement action as appropriate. Since its inception, the work of the Strike Force has resulted in numerous indictments, temporary denial orders (TDOs), and Entity Listings. Took enforcement action against significant national security threats, including the highest number ever of convictions, TDOs, and post-conviction denial orders. Together with FBI, HSI, ATF, and other law enforcement partners, we:

- Imposed the largest standalone administrative penalty in BIS history – a \$300 million penalty against Seagate and Seagate Singapore International Headquarters Pte. Ltd. of Singapore related to their continued shipment of millions of hard disk drives to Huawei even after their two main competitors stopped shipping due to the foreign direct product rule.

- Announced the initial round of Disruptive Technology Strike Force cases with the filing of criminal charges by five different U.S. Attorney’s offices in cases involving China, Russia, and Iran. Also issued a related TDO suspending the export privileges of five entities and two of the charged defendants for diverting civilian aircraft parts to Russia.

- Imposed the largest standalone administrative penalty in BIS history – a \$300 million penalty against Seagate and Seagate Singapore International Headquarters Pte. Ltd. of Singapore related to their continued shipment of millions of hard disk drives to Huawei even after their two main competitors stopped shipping due to the foreign direct product rule.

- Announced the initial round of Disruptive Technology Strike Force cases with the filing of criminal charges by five different U.S. Attorney’s offices in cases involving China, Russia, and Iran. Also issued a related TDO suspending the export privileges of five entities and two of the charged defendants for diverting civilian aircraft parts to Russia.

- In coordination with DOJ, charged a Belgian national for a scheme to export military-grade technology, including accelerometers and missile components, to China and Russia. At the same time, the defendant was arrested by Belgian authorities and he and his companies were added to the Entity List by BIS and to the Specially Designated Nationals and Blocked Persons List by the Department of the Treasury’s Office of Foreign Assets Control (OFAC).

- Worked with DOJ to bring eight separate indictments charging 14 people for their role in procuring items for the Russian military and Russian security service, including: o Two Kansas men for an alleged scheme to illegally export sophisticated avionics, one of whom subsequently pleaded guilty;

*(*Continued On The Following Column)*

- o A Russian national for allegedly supplying electronic devices used for counterintelligence operations to the Federal Security Service of the Russian Federation (FSB) and North Korea; and o Three Russian nationals for allegedly using companies in Brooklyn to unlawfully purchase millions of dollars’ worth of dual-use electronics on behalf of end users in Russia, including companies affiliated with the Russian military.

- Worked with DOJ to obtain a guilty plea from a program administrator for a NASA contractor who secretly funneled sensitive aeronautics software to Beihang University, which is on the Entity List for its involvement in developing Chinese military rocket systems and unmanned air vehicle systems.

- Imposed a \$2.77 million penalty on a 3D printing company related to its sending export-controlled blueprints for aerospace and military electronics to China.

- With DOJ, announced two different seizures of 16 website domains associated with Lebanese Hizballah.

- In coordination with OFAC, imposed a \$3.3 million combined penalty against Microsoft Corporation for alleged and apparent violations of U.S. export controls and sanctions laws, including violations involving Russia, Cuba, Iran, and Syria.

- Helped convict a Pennsylvania man of torture – the second time an American has been convicted of the crime since the federal torture statute went into effect in 1994.

- With DOJ, obtained a guilty plea from a Rhode Island man for purchasing “ghost gun” kits and machining them into working firearms, which were unlawfully exported to the Dominican Republic.

- Worked with DOJ to obtain a guilty plea from Broad Tech System for its involvement in a scheme to illegally export chemicals to a Chinese company that has ties to the Chinese military. Strengthened our enforcement policies to help keep the most critical U.S. technology out of the most dangerous hands:

- Clarified our voluntary self-disclosure (VSD) policy to specify that if a company knows of a significant potential violation and affirmatively decides not to divulge it, that lack of disclosure will be an aggravating factor in any subsequent penalty calculation should the violation later be discovered.

- Announced that when a party informs us about another party’s conduct and that information allows us to take enforcement action, we will consider it “extraordinary cooperation” and treat it as a mitigating factor if the notifying party engages in prohibited conduct in the future.

- Revised the categories of what we measure internally – our metrics – to better reflect and further our prioritized enforcement efforts against the most pressing national security threats.

*(*Continued On The Following Page)*

- Amended our regulations to permit the renewal of certain TDOs for a period of one year, rather than just 180 days, where a party has engaged in a pattern of repeated, ongoing and/or continuous apparent violations of the EAR.
- Joined DOJ in proposing an amendment to the federal Sentencing Guidelines to clarify that §2M5.1 unambiguously encompasses the full spectrum of national security related controls. Developed key partnerships with the interagency, academia, industry, and foreign governments:
 - With the assistance of foreign governments, completed over 1,500 end-use checks – our most ever in a single year.
 - Issued a joint alert with FinCEN containing the first-ever key term for financial institutions to use when filing Suspicious Activity Reports (SARs) for global export evasion.
 - Issued a FinCEN/BIS joint alert regarding Russian evasion of U.S. export controls, detailing evasion typologies, introducing nine new high priority Harmonized System (HS) codes to inform U.S. financial institutions’ customer due diligence, and identifying additional transactional and behavioral red flags.
 - Published “best practice” guidance for industry related to the nine highest-priority HS codes sought by Russia for its missile and unmanned aerial vehicle (UAV) programs and provided a model customer certification form.
 - For the first time ever, issued tri-seal compliance notes with DOJ and Treasury on Russian evasion tactics and voluntary self-disclosures.
 - Established export enforcement coordination mechanisms with export enforcement partners in Australia, Canada, New Zealand, and the United Kingdom (i.e., the “Export Five” or “E5”) and G7 counterparts.
 - Published joint guidance from the E5 for industry and academia addressing high priority items needed by Russia’s military and explaining how exporters can identify Russian diversion pathways.
 - Implemented a new data sharing arrangement with the European Anti-Fraud Office (OLAF) to allow closer coordination on export enforcement.
 - Issued guidance to industry with the Departments of Justice, Treasury, and State on Iran’s procurement, development, and proliferation of UAVs and on Iran’s ballistic missile procurement activities.
 - Issued a “Know Your Cargo” joint compliance note with the Departments of Justice, Homeland Security, State, and Treasury focused on maritime and other transportation industries.
 - Expanded our Academic Outreach Initiative to 29 institutions to help academic institutions maintain an open, collaborative research environment in a way that also protects them from national security risk.
 - Signed a memorandum of understanding with OFAC formalizing our close coordination and partnership.
 - Created an Export Enforcement listserv, so that industry and academia can sign up to receive a notification whenever something enforcement-related gets posted to the BIS website.
- Expanded and enhanced our antiboycott enforcement efforts to ensure that U.S. companies are not used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel:
 - Amended the Boycott Reporting Form to include the name of the specific party making a boycott- related request, which will help the Office of Antiboycott Compliance investigate such requests.

*(*Continued On The Following Column)*

- Imposed over \$425,000 in penalties on companies for alleged violations of the antiboycott regulations, including \$283,500 against Regal Beloit FZE, a foreign subsidiary of Regal Beloit America, Inc., to resolve 84 violations related to antiboycott requests from a Saudi Arabian customer. Successfully placed numerous parties on the Entity List for actions contrary to our national security and foreign policy. Through the established interagency process, nominations from Export Enforcement resulted in the addition to the Entity List of more than 465 parties from China, Russia, Iran, and elsewhere.

NuDay Charity Sentenced for Illegal Exports to Syria - Thursday, December 28, 2023 For Immediate Release U.S. Attorney's Office, District of New Hampshire

CONCORD – The New Hampshire charity NuDay, a/k/a NuDay Syria, was sentenced today in federal court for export offenses, U.S. Attorney Jane E. Young announces.

NuDay was sentenced by U.S. District Court Judge Joseph N. Laplante to five years of probation, the maximum penalty for an organizational defendant. NuDay was also ordered to pay a \$25,000 fine. On September 8, 2023, NuDay pleaded guilty to three counts of Failure to File Export Information.

“Our national security depends on exporters truthfully disclosing where goods are being shipped to ensure that hostile foreign actors do not get their hands on potentially dangerous items,” said U.S. Attorney Jane E Young. “This prosecution shows that willful violations of export law, even by a non-profit charity, will result in criminal consequences.”

“This charity blatantly violated U.S. export control laws when it sent over 100 shipments of humanitarian goods to Syria, a country that is a designated state sponsor of terrorism, and in many instances, lied about where those shipments were going,” said Jodi Cohen, Special Agent in Charge of the FBI Boston Division. “This case highlights the FBI’s ongoing commitment to working with our law enforcement partners to prevent the erosion of public trust in charitable organizations by ensuring that anyone who engages in criminal activity in order to evade our laws and regulations is held accountable.”

“Customs and export laws exist to protect the integrity of our systems of commerce and to protect our national security. The individuals involved with NuDay knew they were breaking the law but did so anyway, sending shipments whose contents were falsely undervalued to Syria, a country subject to export restrictions and sanctions. As today’s sentence shows, these actions have consequences,” said Michael J. Krol, Special Agent in Charge of Homeland Security Investigations in New England.

*(*Continued On The Following Page)*

“Despite the availability of a limited waiver of the restrictions allowing for the export and re-export of a wide range of items necessary to provide humanitarian support to the Syrian people, NuDay devalued \$8.3 million of goods to avoid reporting requirements and transshipped the items through a third country without disclosing their ultimate destination. The end did not justify the means in this case,” said Acting Special Agent in Charge Aaron Tambrini of the Office of Export Enforcement’s Boston Field Office. NuDay was founded by Nadia Alawa as a non-profit charity in 2013 and is headquartered in Windham, New Hampshire. Alawa served as NuDay’s President, and several family members served as board members and employees. Between 2013 and 2019, NuDay claimed significant growth of in-kind donations, starting from approximately \$231,000 in 2013 and reaching almost \$71 million in 2019. By way of comparison, in 2019 OXFAM America reported approximately \$73.5 million in donations, and the Syrian American Medical Society Foundation reported approximately \$41.4 million in donations.

Between 2018 and 2021, NuDay made over 100 shipments to Syria, a country that was subject to sanctions and export restrictions. NuDay claimed that these shipments were worth over \$100 million. NuDay had the items shipped to Mersin, Turkey, where another company would transship them into Syria. U.S. Department of Commerce regulations require exporters, such as NuDay, to report true and accurate information about the items being exported, including the shipment’s description, end user, and monetary value. However, NuDay falsely reported that the end destination of the shipments was Turkey and not Syria, and artificially deflated the value of the goods to be below the \$2,500 reporting threshold. Alawa’s Facebook messages indicated that she and NuDay were aware of export restrictions, including the need to obtain export licenses, but ignored them.

As a condition of the plea, Nadia Alawa and her family members have ceased involvement with NuDay.

The Federal Bureau of Investigation, U.S. Department of Commerce’s Office of Export Enforcement, Internal Revenue Service’s Criminal Investigations, and Homeland Security Investigations led the investigation. Assistant U.S. Attorney Alexander S. Chen prosecuted the case.

**DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.
OFFICE OF FOREIGN ASSETS CONTROL**

Venezuela Sanctions Regulations 31 CFR Part 591 GENERAL LICENSE NO. 5N Authorizing Certain Transactions Related to the Petr6leos de Venezuela, S.A. 2020 8.5 Percent Bond on or After April 16, 2024

(a) Except as provided in paragraph (b) of this general license, on or after April 16, 2024, all transactions related to, the provision of financing for, and other dealings in the Petr6leos de Venezuela, S.A. 2020 8.5 Percent Bond that would be prohibited by subsection I(a)(iii) of Executive Order (E.O.) 13835 of May 21, 2018, as amended by E.O. 13857 of January 25, 2019, and incorporated into the Venezuela Sanctions Regulations, 31 CFR part 591 (the VSR), are authorized.

*(*Continued On The Following Column)*

(b) This general license does not authorize any transactions or activities otherwise prohibited by the VSR, or any other part of 31 CFR chapter V.

(c) Effective January 16, 2024, General License No. 5M, dated October 18, 2023, is replaced and superseded in its entirety by this General License No. 5N.

Bradley T. Smith
Director
Office of Foreign Assets Control
Dated: January 16, 2024

Secretary Blinken’s Remarks at a World Economic Forum Event: Treating Soil as a Precious Resource
01/16/2024 01:31 PM EST

Antony J. Blinken, Secretary of State
Davos, Switzerland
World Economic Forum

SECRETARY BLINKEN: John, thank you very much.
(Applause.)

Thank you. Thank you. Good afternoon. John, my old friend, thank you very, very much. And as always, here, it’s particularly good to be with leaders from across government, business, civil society. So when you think about soil, the U.S. Secretary of State is probably not the first person who comes to mind. (Laughter.) But the truth is soil is literally at the root of many pressing national security challenges that we face.

You all know this, and we know this increasingly with every passing day: without good soil, crops fail, prices rise, people go hungry. Eroding soil also worsens the impact of droughts, of floods, of other climate-driven extreme weather, making crop yields even lower – and as a result, food even scarcer. As we meet here today, 700 million people do not know if they will have enough food to eat tomorrow.

This hunger fuels instability, and instability fuels hunger. A parent who can’t put food on the table for their children picks up the family and moves because it’s the most basic thing, the most important thing that they can do, and they will do it however they have to do it. And if that means moving halfway around the world, they will. But that contributes to unprecedented migration flows that we’re facing around the world. Shifting climate patterns force neighbors to compete for dwindling resources, further straining ethnic tensions, destabilizing entire communities.

Meanwhile, Russia’s attacks on fields, on granaries, on ports in Ukraine, the world’s breadbasket, have disrupted global markets, making food harder to afford and harming the poor and most vulnerable most of all. In the Red Sea, through which 15 percent of the world’s commerce passes, Houthi attacks have forced ships to take longer, more expensive routes, further raising the price of food and energy.

*(*Continued On The Following Page)*

The United States has been and is working intensely to tackle this food crisis and support those who are most affected by it. Going back to January of 2021, the U.S. Government has devoted \$17.5 billion to provide vital sustenance to people in need. We are honored to fund over one third of the World Food Programme’s budget. Now I had a chance to see some of these efforts just last week at a World Food Programme warehouse in Jordan, where I met with UN staff that is working relentlessly, often at great personal risk, to get aid to Palestinians in Gaza, over 90 percent of whom are facing acute food insecurity.

Too many people already go to sleep hungry, and it’s set to get worse. If you project out to 2050, global demand for food is projected to rise by 50 percent. But over that same period, climate change could reduce yields by as much as 30 percent. So do the math and it doesn’t balance out. In short, we need to feed more people as growing food becomes harder.

That’s why the United States is partnering to adapt and transform agriculture and food systems, because as vital as emergency assistance is, if we don’t get at the underlying infrastructure, if we don’t get at a way to produce better, stronger, more resilient crops, then we won’t solve the problem. But we joined a pledge with over 130 countries signing the Emirates Declaration at COP 28 to address a big part of this. Our Agriculture Innovation Mission for Climate initiative with the UAE has mobilized \$17 billion to invest in efforts like regenerating degraded crop land and capturing carbon in soil. Through the global partnership for infrastructure and investment, we are working with dozens of countries – from India to Zambia – to scale climate-smart agriculture and bolster supply chains. And together with the African Union and the Food and Agriculture Organization, we’ve launched a new initiative. It’s called Vision for Adapted Crops and Soils, or VACS, and VACS is part of the USAID’s flagship Feed the Future initiative. This is our comprehensive response in the U.S. Government to food insecurity around the world, and the approach that we have is two-pronged. And it really boils down to this, two very basic things: First, we’re investing above ground, identifying the indigenous African crops that are most nutritious and most resilient to climate change, improving these varieties, delivering them to the world; at the same time, we’re investing below ground, mapping, conserving, building healthy soils. If you get this right, if you get the seeds right, if you get the soil right, then you have your agricultural foundation for the future.

We’ve been incredibly fortunate at the State Department to have one of the world’s leading experts, Dr. Cary Fowler, lead our efforts in helping develop this initiative. We’ve committed \$150 million thus far toward VACS. We’re also rallying a broad coalition of governments around the world to advance this work: Japan, Norway, the United Kingdom, the Netherlands, as well as leading nonprofits and corporations. Just to cite one example, IBM is expanding access to its OpenHarvest platform, which is using AI and climate modeling to deliver tailored farm and field management recommendations right to farmers’ cell phones. We have the capacity as we’re doing this with all of this technology to literally map the soil any place in the world, any given field, to tell whether the soil is good, bad, deficient, and then to figure out how we can make it as productive as possible.

*(*Continued On The Following Column)*

So, this is something that I believe is genuinely revolutionary – seeds and soil, we put them together, and we can begin to answer a lot of the challenges that our world is going to face over the next 25 or 30 years. And so my simple pitch to you today is this: Join us. This is a powerful investment. It has extraordinary, even transformational returns.

Some of you may know that the word human comes from the Latin term for earth, for soil. There are a few things that are more human, more and more important to humanity, than figuring out how to cultivate this planet so that it can feed and support all of us. We have an opportunity in this moment to actually deliver better for people today while actually building a sustainable tomorrow.

So part of the reason – and John said at the outset – this event in and of itself is unusual for Davos. Having foreign policy types participate in it may also seem a little bit unusual, but it only underscores the importance that all of us attach to both this challenge but also this incredible, incredible opportunity to get maybe the most fundamental thing in life that we need to sustain us right going forward into the future, and that’s the food to feed everyone on this planet and to feed them well.

So those of you who have the interest and the opportunity, please join us in this initiative, join us in this effort. We can make a huge difference together. Thanks very much. (Applause.)

JetBlue’s merger with Spirit is blocked by a federal judge — a big win for the Biden administration’s antitrust efforts

U.S. District Court Judge William G. Young wrote: “A post-merger, combined firm of JetBlue and Spirit would likely place stronger competitive pressure on the larger airlines in the country. At the same time, however, the consumers that rely on Spirit’s unique, low-price model would likely be harmed.”

Terrorist Designation of the Houthis

01/17/2024 10:44 AM EST

Antony J. Blinken, Secretary of State

The Department of State today is announcing the designation of Ansarallah, commonly referred to as the Houthis, as a Specially Designated Global Terrorist group, effective 30 days from today.

Since November, the Houthis have launched unprecedented attacks against international maritime vessels in the Red Sea and Gulf of Aden, as well as military forces positioned in the area to defend the safety and security of commercial shipping. These attacks against international shipping have endangered mariners, disrupted the free flow of commerce, and interfered with navigational rights and freedoms. This designation seeks to promote accountability for the group’s terrorist activities. If the Houthis cease their attacks in the Red Sea and Gulf of Aden, the United States will reevaluate this designation.

*(*Continued On The Following Page)*

The Houthis must be held accountable for their actions, but it should not be at the expense of Yemeni civilians. As the Department of State moves forward with this designation, we are taking significant steps to mitigate any adverse impacts this designation may have on the people of Yemen. During the 30-day implementation delay, the U.S. government will conduct robust outreach to stakeholders, aid providers, and partners who are crucial to facilitating humanitarian assistance and the commercial import of critical commodities in Yemen. The Department of the Treasury is also publishing licenses authorizing certain transactions related to the provision of food, medicine, and fuel, as well as personal remittances, telecommunications and mail, and port and airport operations on which the Yemeni people rely.

Today's announced action is being taken pursuant to Executive Order 13224, as amended, which targets terrorists, terrorist organizations, leaders of terrorist groups, and those providing support to terrorists or acts of terrorism. Ansarallah is being designated for having committed or attempted to commit, posing a significant risk of committing, or having participated in training to commit acts of terrorism that threaten the security of United States nationals or the national security, foreign policy, or economy of the United States. This designation and the associated general licenses will be effective on February 16, 2024.

Imposing Sanctions on Former Guatemalan Official for Corruption

Matthew Miller, Department Spokesperson

The United States is imposing financial sanctions on Alberto Pimentel Mata, Guatemala's former Minister of Energy and Mining, for his role in corruption. Pimentel used his official position to exploit the Guatemalan mining sector through bribery schemes, including schemes related to government contracts and mining licenses. Corrupt and anti-democratic acts undermine Guatemala's public institutions, threaten regional stability, and fuel migration from the northern Central America region. The United States remains committed to taking action against illicit activities carried out by officials who abuse their positions of power to seek personal benefit at the expense of the Guatemalan people.

On October 31, 2023, the Secretary of State announced the public designations under Section 7031(c) of Alberto Pimentel Mata, and his immediate family members, for his involvement in significant corruption. The Department of the Treasury action was taken pursuant to Executive Order 13818, which builds upon and implements the Global Magnitsky Human Rights Accountability Act and targets perpetrators of serious human rights abuse and corruption around the world. For more information on this designation, see Treasury's [press release](#).

FOR IMMEDIATE RELEASE

January 18, 2024

www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

OCPA@bis.doc.gov

BIS Deploys Assessment On The Use Of Mature-node Chip

WASHINGTON, DC.--The U.S. Department of Commerce's Bureau of Industry and Security (BIS) is conducting a comprehensive assessment of the use of mature-node semiconductor devices in the supply chains that support—directly or indirectly—U.S. national security and critical infrastructure.

The intent of the survey is to identify how U.S. companies are sourcing mature-node semiconductors, also known as legacy chips. This analysis will inform U.S. policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People's Republic of China (PRC).

The assessment was requested by the Secretary of Commerce in response to findings in a Congressionally mandated report released in December 2023 that assessed the capabilities of the U.S. microelectronics industrial base to support U.S. national defense. The findings of that report, titled "Assessments of the Status of the Microelectronics Industrial Base in the United States," are available online at: <https://www.bis.doc.gov/index.php/other-areas/office-of-technology-eval...>

The survey will be performed under Section 705 of the Defense Production Act of 1950 to evaluate the extent of, and visibility into, the use of mature-node chips manufactured by PRC-based companies in supply chains of critical U.S. industries like telecommunications, automotive, medical device, and the defense industrial base.

FAQs

Q. Under what authority does the Bureau of Industry and Security conduct this survey?

A. BIS has authority under Section 705 of the Defense Production Act of 1950 (DPA) (50 U.S.C. App. Sec. 4555), as amended, to conduct research and analysis of critical technologies and industrial sectors to advance U.S. national security and economic competitiveness. BIS uses industry-specific surveys to obtain production, R&D, export control, employment, and other relevant data to inform U.S. Government policies and proposals.

Q. Is this an annual/repeated collection?

A. This assessment is a one-time information collection, though BIS has performed similar assessments in the past and may be tasked to carry out similar assessments in the future.

Q. What will the information from the assessment be used for?

A. This analysis will inform U.S. policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People's Republic of China (PRC). The data will also support preparation for the implementation of Section 5949 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Public Law 117-263).

(*Continued On The Following Page)

Q. Has BIS conducted similar studies in the past?

A. Yes. Since 1986, BIS has conducted over 60 assessments and 150 surveys on a wide range of topics, including shipbuilding, strategic materials, space and aeronautics, rocket propulsion, munitions, and semiconductors, among others. To view public versions of previous BIS reports and surveys, please visit our website at: <https://www.bis.doc.gov/dib>.

Q. Will the findings from this assessment be publicly available?

A. BIS expects to provide a public summary of key findings, though the Department’s priority is the development of policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People’s Republic of China (PRC). Data provided in response to the survey is deemed business confidential under the DPA and is protected from disclosure under the Freedom of Information Act (FOIA), should it be the subject of a FOIA request.

Q. Is this assessment part of the CHIPS Act?

A. No. This survey is not part of the application for funding under Section 9902 of the 2021 NDAA (15 USC § 4652). Individual survey responses will not affect eligibility and/or consideration for CHIPS Act or other government funding.

Q. How does this effort relate to BIS’s advanced computing chips rules?

A. This assessment is not part of BIS’s advanced computing chips rules. The focus of this assessment is on older generations of technology referred to as mature-node or legacy chips. The information collected will guide U.S. policies to ensure safe and reliable semiconductor supply chains, particularly for the legacy chips essential to U.S. national security and critical infrastructure.

Businessman Arrested for Scheme to Illegally Export Semiconductors and Other Controlled Technology to Russia

**Thursday, January 18, 2024
For Immediate Release
Office of Public Affairs**

Defendant Allegedly Used Network of Businesses in China and Other Countries to Illegally Transfer Hundreds of Thousands of Semiconductors to Sanctioned Business with Ties to Russian Military and Russian Intelligence Agencies Ilya Kahn, 66, a citizen of the United States, Israel and Russia, and resident of Brooklyn, New York, and Los Angeles, California, was arrested yesterday in Los Angeles for his alleged involvement in a years-long scheme to secure and unlawfully export sensitive technology from the United States for the benefit of a Russian business. The business was sanctioned by the U.S. government following Russia’s unprovoked invasion of Ukraine in February 2022 and whose clients include elements of the Russian military and the Federal Security Service (FSB), the main successor agency to the Soviet Union’s KGB.

According to court documents, Kahn is charged by criminal complaint with conspiracy to violate the Export Control Reform Act (ECRA). Kahn will make his initial appearance in the Central District of California. *(*Continued On The Following Column)*

“Mr. Kahn stands accused of repeatedly exporting sensitive technology to Russia before, during, and after Russia launched its unprovoked invasion of Ukraine,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Violations of U.S. sanctions and export control laws that aid Russia and other hostile powers endanger our nation’s security and will be met with the full force of the Justice Department.”

“This arrest reflects our continued aggressive enforcement of export control violations involving the Russian military and the Federal Security Service,” said Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department’s Bureau of Industry and Security (BIS). “Stopping the flow of semiconductors and sensitive technologies to those aiding Russia’s unjust war in Ukraine is a critical priority for BIS and our Disruptive Technology Strike Force partners.”

“As alleged, Kahn illegally sent specialized technology from the United States to a Russian semiconductor manufacturer with ties to multiple other sanctioned Russian entities and did so by circumventing U.S. export laws and regulations,” said U.S. Attorney Breon Peace for the Eastern District of New York. “Evading U.S export regulations to send goods to benefit the Russian military complex presents a danger to our national security and our allies and partners abroad. We will continue to use all of our law enforcement and national security tools to hold these enablers, both individuals and corporations, accountable for flouting the rule of law.”

“This arrest marks the end of Ilya Khan’s alleged involvement in a years-long scheme to secure and export millions of dollars’ worth of sensitive technologies from the U.S. to Russia to be used by its military and intelligence services,” said Executive Assistant Director Larissa L. Knapp of the FBI’s National Security Branch. “Any attempt to circumvent U.S. laws, sanctions, and regulations will not be tolerated, and thanks to a coordinated interagency effort, our national security and our partners’ are stronger than ever.”

According to court documents, Kahn is the owner of Senesys Incorporated, which is based in California, and Sensor Design Association, which maintains a contact address in Brooklyn. As alleged in the complaint and other public filings, Kahn operated these two businesses – ostensibly involved in “security software development” and the testing of silicon wafers for military avionics and space users – through which he engaged in a years-long conspiracy to acquire and export sensitive and sophisticated electronics from the United States to a sanctioned Russian business without acquiring the appropriate licenses. The Russian business, Joint Stock Company Research and Development Center ELVEES (Elvees) was added to the Commerce’s Department’s Entity List in March 2022 and was sanctioned by the Treasury Department in September 2022 because of its critical role in facilitating Russia’s military and its invasion of Ukraine.

For example, according to the complaint, in 2019, Kahn exported multiple U.S.-origin microcontrollers to Elvees in Russia, and in 2022, he exported U.S.-origin network interface controllers and a radio-frequency transmitter to Elvees in Russia by way of a Hong Kong-based shipping company. Each of these items required an export license from the Commerce Department, which Kahn did not obtain, and were controlled for national security and anti-terrorism reasons.

*(*Continued On The Following Page)*

As alleged, Kahn also arranged for Elvees to continue to receive semiconductors manufactured in Taiwan following Russia's invasion of Ukraine in February 2022. Specifically, after the Taiwanese company that manufactured Elvees-designed semiconductors refused to ship those semiconductors to Russia, Kahn arranged for the semiconductors to be sent to the United States and then re-exported them to Russia, often through a shipping company based at John F. Kennedy International Airport in Queens, New York. Kahn also used Hong Kong and other locations around the world as transshipment points to evade U.S. export laws and regulations and to conceal the Russian end users.

Even after Elvees was added to the Entity List, Kahn continued to work with the company. In May 2022, Kahn emailed design guidance for an Elvees-branded microchip to a Taiwan manufacturer. Subsequently, Kahn shipped thousands of units of this microchip – through a New York-based shipper – to a Hong Kong shipping company, and then to a company located in mainland China. Kahn noted in communications with the Hong Kong shipping company that he received a “call from Russia” about the Chinese business to which he was directing the goods.

If convicted, Kahn faces a maximum penalty of 20 years in prison for conspiracy to violate the ECRA.

The FBI and Department of Commerce's BIS New York Field Office are investigating the case. The U.S. Attorney's Office for the Central District of California provided significant assistance.

Assistant U.S. Attorneys Craig R. Heeren, Artie McConnell, and Matthew Skurnik for the Eastern District of New York and Trial Attorney Scott Claffee of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case, with assistance from Litigation Analysts Joseph Levin and Mary Clare McMahon.

Today's actions were coordinated through the Justice and Commerce Departments' Disruptive Technology Strike Force and the Justice Department's Task Force KleptoCapture. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation states. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia's unprovoked military invasion of Ukraine.

Today's actions were coordinated through the Justice and Commerce Departments' Disruptive Technology Strike Force and the Justice Department's Task Force KleptoCapture. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation states. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia's unprovoked military invasion of Ukraine.

A complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
[Kahn complaint Updated January 18, 2024](#)

Virginia man convicted of exporting heavy equipment to Iran in violation of U.S. sanctions laws - Thursday, September 14, 2023 For Immediate Release

U.S. Attorney's Office, Northern District of Georgia

ATLANTA – A federal jury has convicted Jalal Hajavi of conspiring to violate the International Emergency Economic Powers Act (“IEEPA”) and the Iranian Transactions and Sanctions Regulations (“ITSR”), smuggling goods from the United States, unlawfully exporting and reexporting goods from the U.S. to Iran without a license, and unlawfully engaging in transactions and dealings based on his participation in a scheme to unlawfully export heavy equipment from the U.S. to Iran by routing the shipments through the United Arab Emirates.

“Hajavi chose to leverage his Florida business to illegally export materials to Iran rather than to lawfully contribute to the U.S. economy,” said U.S. Attorney Ryan K. Buchanan. “The U.S. trade sanctions against Iran exist to help keep our country and citizens safe. Those who seek to profit by evading these prohibitions will be held accountable.”

“Falsifying export documents in an attempt to obfuscate the transshipment of U.S. commodities through the United Arab Emirates to Iran is a serious violation of U.S. export laws, and will be vigorously investigated,” said John Johnson, Special Agent in Charge, Office of Export Enforcement's Miami Field Office. “By disrupting illicit procurement networks, we continue to deny U.S. dual-use commodities to countries such as Iran that threaten U.S. national security interests.”

According to U.S. Attorney Buchanan, the charges, and other information presented in court: Hajavi, through his company JSH Heavy Equipment, LLC, conspired with an individual in Iran to export U.S. heavy machinery indirectly to Iran without first obtaining the required licenses from the Office of Foreign Assets Control (“OFAC”). Hajavi orchestrated the scheme by locating heavy equipment for sale, such as bobcats and wheel loaders, and sending information about the equipment to his co-conspirator in Iran. Hajavi purchased the items from U.S. sellers and used freight forwarding companies to ship the heavy equipment from the U.S. to the U.A.E. Hajavi falsely claimed that the items were destined for his U.A.E. customers, which typically were general trading companies located in free trade zones in the U.A.E. But in truth, Hajavi intended for his Iranian co-conspirator to transship those items from the U.A.E. to Iran in circumvention of the U.S. export licensing requirement.

Utilizing this scheme, Hajavi purchased an Ingersoll Rand blasthole drill from a U.S. company. The drill is a type of heavy machinery used to create holes in the ground that are usually then filled with controlled charges. In a sham transaction, Hajavi sold the drill to a U.A.E. company that, in turn, provided the drill to Hajavi's Iranian co-conspirator, who shipped the tool to Iran.

*(*Continued On The Following Page)*

In addition to evading OFAC licensing requirements, Hajavi concealed his activities with his Iranian co-conspirator by causing false information to be entered into the Automated Export System ("AES"), a U.S. government database containing information about exports from the United States. Hajavi hired a U.S. freight forwarder to arrange the drill's export from the U.S. to the U.A.E. As part of the shipping process, the freight forwarder submitted information to AES about the shipment, including the ultimate consignee's name and the ultimate delivery destination. Hajavi lied to the freight forwarder by claiming that the U.A.E. company was the ultimate consignee and that the ultimate delivery destination was the U.A.E. In fact, Hajavi's co-conspirator in Iran was the true recipient and Iran was the ultimate delivery destination.

Sentencing for Jalal Hajavi, 59, of Sterling, Virginia, is scheduled for December 14, 2023, at 10:00 a.m. before U.S. District Judge Thomas W. Thrash.

This case is being investigated by the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement. Assistant U.S. Attorney Tracia M. King and Trial Attorney Emma Dinan Ellenrieder of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

For further information please contact the U.S. Attorney's Public Affairs Office at USAGAN.PressEmails@usdoj.gov or (404) 581-6016. The Internet address for the U.S. Attorney's Office for the Northern District of Georgia is <http://www.justice.gov/usao-ndga>.

Hossein Hatefi Ardakani
East Asia and Pacific | Near East (North Africa and the Middle East) Reward Up to \$15 million
About

Rewards for Justice is offering a reward of up to \$15 million for information leading to the disruption of financial mechanisms of the U.S.-designated terrorist organization Islamic Revolutionary Guard Corps (IRGC).

Hossein Hatefi Ardakani is Iranian businessman who has helped acquire and supply sophisticated technology that has supported IRGC weapons production and sales. Since 2014, Ardakani has used his network of intermediary companies, including Malaysia- and Hong Kong-based front companies and UAE logistics businesses, to procure and to facilitate the transfer of sensitive U.S.- and foreign-origin materials, components, and technology to the Islamic Republic of Iran (Iran) for Iran's weapons programs. These weapons, including the Shahed-136 and Shahed-131 attack Unmanned Aerial Vehicles (UAVs, or drones), are developed on behalf of the IRGC and then sold on the international market. Some of those UAVs have been sold to the Russian armed forces for its use in its illegal military operation in Ukraine. Proceeds from these arms sales directly benefit the IRGC.

*(*Continued On The Following Column)*

U.S.-origin flight guidance components procured by the Ardakani network have been identified in recovered wreckage of Shahed drones in Ukraine and other conflict zones. Additionally, the Ardakani network has illegally procured U.S. export-controlled high electron mobility transistors (a.k.a. HEMTs) and other components with ballistic missile applications, as well as other electronics with weapons application.

Malaysia-based front companies supporting the Ardakani network include Arta Wave Sdn Bhd, Integrated Scientific Microwave Technologies, and Tecknologi Merak Sdn Bhd. These companies and others have a corporate registration in Kuala Lumpur, Malaysia, with unregistered representation and common addresses in Hong Kong. The companies act as proxies for Ardakani to acquire U.S.- and foreign-origin materials, which are otherwise unobtainable through legitimate procurement channels due to U.S. sanctions and export controls targeting Iran and the IRGC.

UAE-based businesses, including Dubai-based Smart Mail Services, Ring Field FZE, and others, have been identified as witting shipping facilitators used to submit false or misleading shipping information, circumvent U.S. and non-U.S. sanctions and export control regulations, and transship illegally procured components to the IRGC on behalf of Ardakani.

Ardakani also operates Tehran-based businesses Kavan Electronics Co, Ltd, Basamad Electronic Pouya Engineering Co, and Teyf Tadbir Arya Engineering Co.

On December 19, 2023, the U.S. Department of Justice unsealed an indictment against Ardakani charging him with crimes related to his procurement of U.S.-manufactured dual-use microelectronics for the IRGC. Concurrently, the U.S. Department of the Treasury placed Ardakani and 10 related entities on its Specially Designated Nationals list pursuant to Executive Order (E.O.) 13382, which targets proliferators of weapons of mass destruction and their means of delivery. The sanctions prohibit all transactions by U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of blocked or designated persons.

COMMERCE STRENGTHENS CONTROLS AGAINST RUSSIA AND BELARUS IN RESPONSE TO RUSSIA'S CONTINUED WAR AGAINST UKRAINE

FOR IMMEDIATE RELEASE BUREAU OF INDUSTRY AND SECURITY
January 23, 2024 Office of Congressional and Public Affairs
<https://bis.doc.gov> Media Contact: OCPA@bis.doc.gov

WASHINGTON, D.C. -- Today, the Commerce Department's Bureau of Industry and Security (BIS) strengthened its existing controls under the Export Administration Regulations (EAR) against Russia and Belarus in response to the Russian Federation's (Russia's) ongoing aggression against Ukraine and Belarus's complicity in the invasion.

*(*Continued On The Following Page)*

Today's action expands the scope of the EAR's Russian and Belarusian Industry Sector Sanctions by adding 94 6-digit Harmonized Tariff Schedule (HTS) codes to the list of items requiring a license for export, reexport, or transfer (in-country) to Russia or Belarus. The expanded list of items includes certain chemicals, lubricants, and metals, and it covers the entirety of Chapter 88 of the HTS (aircraft, spacecraft, and parts thereof), thereby further restricting Russia's access to inputs for its defense industrial base and better aligning U.S. controls with those implemented by U.S. partners and allies.

The rule also expands controls on certain EAR99 antennas, antenna reflectors, and parts thereof to further restrict these items from going to Iran and Russia, including when produced abroad with U.S. technology or software.

Today's action also removes the lowest-level military and spacecraft-related items (i.e., y items) from being eligible for de minimis treatment when incorporated into foreign-made items for export from abroad or reexport to Russia or Belarus.

Finally, the new rule makes several clarifying changes, including by adding an exclusion from BIS license requirements in situations involving transactions that are related to deployments by the Armed Forces of Ukraine to or within the temporarily occupied Crimea region of Ukraine and covered regions of Ukraine.

"Today's action reflects the U.S. government's continuing commitment to respond to Russia's invasion of Ukraine and Belarus's complicity in the invasion, in concert with our allies and partners in the Global Export Control Coalition," said Under Secretary of Commerce for Industry and Security Alan F. Estevez. "Russia's continued aggression against Ukraine undermines global order, peace, and security."

"Export controls are more durable and effective when imposed on a multilateral basis, and today's rule better aligns U.S. controls with the stringent measures implemented by our allies and partners," said Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler. "In doing so, it will enhance the effectiveness of existing controls to further limit Russia's access to items that enable its military capabilities."

Additional Information:

In response to Russia's war against Ukraine, BIS has imposed extensive sanctions on Russia and Belarus under the EAR. During the last two years, BIS has published a number of additional final rules strengthening the export controls on Russia and Belarus, including measures undertaken in coordination with the 38 U.S. allies and partners of the Global Export Control Coalition.

Taken together, these actions under the EAR reflect the U.S. government's position that Russia's war against Ukraine and Belarus's complicity in the war flagrantly violate international law, are contrary to U.S. national security and foreign policy interests, and undermine global order, peace, and security.

Additional information on BIS's efforts to respond to Russia's war against Ukraine is available on BIS's website at: <https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/russia-belarus>. For additional information, please visit: <https://bis.doc.gov>.

Selling China

Insights, analysis and must reads from CNN's Fareed Zakaria and the Global Public Square team, compiled by Global Briefing editor Chris Good

A poor start to 2024 for China's stock market prompted **Foreign Policy's James Palmer to reflect this week** on China's recent, broader-based economic struggles, which have included slow growth and a shaky property sector: "The gulf between China's official (economic) optimism and the rest of the world's pessimism is at the root of the stock market slide, which is mostly fueled by an unprecedented sell-off by foreign investors that started in the second half of 2023 and has picked up speed this year. ... (T)he psychological shock of the (broader economic) downturn (in China) is hitting harder than it might in another country because the Chinese government and public have become used to high GDP growth in the last three decades. Although some parts of China, especially the country's northeast, have suffered through hard times for years, for many people this shock is a new experience."

That global pessimism can be heard in a slew of recent negative prospectuses. **In a Nikkei Asia feature this month, JC de Swaan wrote** that China has been slow to reform its economy, which now looks less impressive, and less impressively managed, than India's and Japan's. **In her econVue+ newsletter, Lyric Hughes Hale writes:** "Badly needed reforms have been delayed for the past decade and the process is unlikely to resume." **At the World Politics Review, Mary Gallagher writes** that in the coming years and decades, China's aging population will collide with an administrative and welfare system ill-suited to the challenge.

FOR IMMEDIATE RELEASE

January 29, 2024

www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY

Office of Congressional and Public Affairs

OCPA@bis.doc.gov

Commerce Proposes Rule to Advance U.S. National Security Interests and Implement Biden-Harris Administration's AI Executive Order and National Cybersecurity Strategy

Proposed Rule Seeks to Improve Detection and Prevention of Foreign Malicious Cyber Activity and Prevent U.S. Services from being Used Against U.S. Interests

WASHINGTON, D.C.— Today, the Department of Commerce (Department) published a notice of proposed rulemaking (NPRM) for establishing new requirements for Infrastructure as a Service providers (IaaS or "cloud infrastructure providers"). The NPRM outlines proposed requirements to address the risk of foreign malicious actors using U.S. cloud services that could be used in malicious cyber-enabled activity to harm U.S. critical infrastructure or national security, including to train large artificial intelligence (AI) models.

(*Continued On The Following Page)

This NPRM demonstrates the Biden-Harris Administration’s proactive efforts to address the potential national security risks associated with frontier AI models and the abuse of U.S. cloud infrastructure by malicious actors and is a significant step in implementing the President’s Executive Order (EO) on “Safe, Secure, and Trustworthy Use and Development of Artificial Intelligence” (EO 14110) and the National Cybersecurity Strategy.

“Today’s rule puts foreign malicious cyber actors on notice that we are taking action to prevent them from using our own cloud infrastructure to undermine our national security interests,” said **Under Secretary for Industry and Security Alan Estevez**. “Today’s proposed rule gives the Secretary of Commerce the tools she needs to address risks while maintaining the Department’s overall approach to national security: to innovate and do business wherever we can, and to protect what we must.”

The proposed rule introduces potential regulations that require U.S. cloud infrastructure providers and their foreign resellers to implement and maintain Customer Identification Programs (CIPs), which would include the collection of “Know Your Customer” (KYC) information. Similar KYC requirements already exist in other industries and seek to assist service providers in identifying and addressing potential risks posed by providing services to certain customers. Such risks include fraud, theft, facilitation of terrorism, and other activities contrary to U.S. national security interests.

The NPRM also authorizes the imposition of certain special measures that can restrict malicious cyber-enabled actors’ access to U.S. IaaS. In this NPRM, the Department seeks feedback on a number of issues, including: minimum verification standards, access, and record-keeping requirements that providers must adopt; the procedures by which the Secretary of Commerce decides when and how to impose a special measure; and the definitions of several key IaaS and AI-related terms as they apply to the regulations.

This NPRM incorporates many of the public comments received in response to a September 24, 2021, Advanced Notice of Proposed Rulemaking (ANPRM). That ANPRM sought feedback on how the Department should implement various provisions of EO 13984, “Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber Enabled Activities.” Based on these comments, the Department has drafted the proposed rule to clarify requirements for the public in ways that are consistent with industry and public understanding of IaaS-related products and services.

The text of the proposed rule released today is available on the Federal Register’s website [here](#). The deadline for public comments is April 29, 2024.

About the Office of Information and Communications Technology and Services:

The ICTS program became a mission of BIS in 2022. OICTS is charged with implementing a series of Executive Orders (EOs) under the International Emergency Economic Powers Act (IEEPA) focused on protecting domestic information and communications systems from threats posed by foreign adversaries.

*(*Continued On The Following Column)*

The ICTS program’s authorities include:

1. [EO 13873, “Securing the Information and Communications Technology and Services Supply Chain”](#) (May 15, 2019), delegated to the Secretary of Commerce broad authority to prohibit or impose mitigation measures on any ICTS Transaction subject to United States jurisdiction that poses undue or unacceptable risks to the United States.
2. [15 C.F.R. Part 7, “Securing the Information and Communications Technology and Services Supply Chain,”](#) is the implementing regulation for EO 13873 and establishes the scope of an ICTS Transaction and creates a process for reviewing ICTS Transactions the Department or other agencies (through referrals) believe may pose an undue or unacceptable risk. The Department can, on its own accord or upon referral, investigate ICTS Transactions. Ultimately, the Secretary can prohibit or mitigate ICTS Transactions if those transactions pose one of the three risks outlined in EO 13873.
3. [EO 13984, “Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities”](#) (January 19, 2021), directs the Secretary of Commerce propose rules to address malicious cyber actors’ use of Infrastructure as a Service (IaaS), by proposing “know your customer” (KYC) requirements.
4. [EO 14034, “Protecting Americans’ Sensitive Data from Foreign Adversaries”](#) (June 11, 2021), builds upon EO 13873 to address threats posed by connected software applications linked to foreign adversaries.
5. [EO 14110, “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”](#) (October 30, 2023), builds on E.O. 13984, directing the Secretary of Commerce to impose record keeping requirements on IaaS providers when transacting with a foreign person to train certain large AI models.

For more information, visit <http://www.bis.doc.gov>.

01.24.2024

Warren, Durbin, Castro, Torres to Commerce Department: Prevent Gun Violence Abroad by Strengthening Firearm Export Controls

Lawmakers Recommend Commerce Act to Reform Firearm License Approval and Monitoring Policies

Washington, D.C. – U.S. Senators Elizabeth Warren (D-Mass.) and Dick Durbin (D-Ill.), Chair of the Senate Judiciary Committee, and U.S. Representatives Joaquin Castro (D-Texas), Ranking Member of the House Foreign Affairs Committee’s Subcommittee on the Western Hemisphere, and Norma Torres (D-Calif.) sent a letter to Secretary of Commerce Gina Raimondo, calling on the Department of Commerce (Commerce) to incorporate a set of recommendations from the lawmakers to strengthen export controls and end-use checks for firearm exports to crack down on the unnecessary export of lethal weapons used in brutal killings abroad. The letter comes as Commerce prepares for the expiration of its 90-day pause on export approvals of certain firearms and related components.

*(*Continued On The Following Page)*

“The number of firearms export license approvals skyrocketed when the Trump Administration transferred firearms export control authority from the State Department to Commerce.... While we continue to support returning all firearms export controls to the State Department, we urge the Department to incorporate the recommendations in this letter as part of its policy review in order to strengthen export controls and end-use checks,” **wrote the lawmakers.**

On October 27, 2023, Commerce announced a 90-day pause of export license approvals for certain assault weapons and other firearms transferred by the Trump administration from the State Department’s jurisdiction to Commerce. That pause is scheduled to expire on January 25, 2024.

“Commerce’s decision to initiate the pause and review process was welcome, but sorely needed... new data show that from March 9, 2020 (the date of the Trump administration’s transfer) to June 30, 2023, Commerce approved nearly 25,000 firearms export licenses with a total value of \$34.7 billion, or roughly \$10.5 billion per year. This represents a more than \$1 billion increase in the annual value of license approvals as compared to the time period when the State Department controlled these approvals,” **continued the lawmakers.**

The lawmakers referenced recent reporting detailing the extent to which Commerce has worked with the National Sports Shooting Foundation and other industry trade groups to court foreign buyers for American-made firearms, despite the Biden administration’s efforts to stem the tide of gun violence at home.

The lawmakers detailed evidence of American-made firearms contributing to violence in countries such as Thailand, El Salvador, and Mexico. They also noted “evidence to suggest that soldiers and civilian militias in Israel are using American-made semi-automatic weapons to perpetrate shocking violence against Palestinian civilians.” The risks to civilians have likely increased after the Israeli government loosened gun ownership laws, authorizing “temporary licensing official(s)’ with only a single day of training to approve ‘anywhere from hundreds to thousands of firearm licenses’ over a few weeks.”

The lawmakers called for reversing the Trump administration’s decision and returning all firearms export controls to the State Department. However, given the seriousness and scale of the problem, the lawmakers are calling on Commerce to make significant changes in the interim to its export license approval and monitoring policies, as well as export promotion policies, including:

1. Recognizing in a formal policy statement that firearms are the only lethal weapons on the Commerce Control List and asserting that it is a foreign policy interest of the U.S. to restrain the global proliferation of these weapons.
2. Publicly posting requirements for end-use certification of exported semi-automatic firearms and committing to pre- and post-shipment transparency and end-use monitoring.

*(*Continued On The Following Column)*

1. Adding “crime control” to the list of criteria systematically considered by Commerce prior to approving a firearms export license.
2. Taking advantage of existing, comprehensive sources (such as the State Department’s International Vetting and Security Tracking-cloud system) when reviewing license applications to identify problematic proposed end users.
3. Encouraging countries of particular concern to fully participate in the Bureau of Alcohol, Tobacco, Firearms and Explosives’ (ATF’s) eTrace system to better track the use of U.S.-sourced firearms in criminal activity and facilitating programs to develop such capacities in countries of concern.
4. Reducing export license validity from four years to one year, particularly for destinations of concern.
5. Systematically reviewing licenses approved for export to countries importing very high numbers of firearms and confirming the identities of end users of these weapons.
6. Capping exports of firearms to civilian buyers, and aggressively enforcing policies prohibiting transfers to security forces with an elevated risk of human rights abuse.
7. Capping the number of exported firearms that can be covered by any single export license, particularly for destinations of concern, and distinguishing between firearms destined for security forces of trusted allies versus civilians or commercial retailers.
8. Ending Commerce’s involvement in the SHOT Show and other firearms export promotion activities that can lead to, and even enable, gun violence and death abroad.
9. Using its authority under the Export Control Reform Act of 2018 to issue all policy changes stemming from the review process as final rules to ensure prompt implementation.

“The Commerce Department’s decision to pause new firearm export approvals and promotion is welcome news. We urge the Commerce Department to implement our recommendations in its review of its export policies, and if necessary, to extend the temporary pause as needed to reconsider its export policies as rigorously as possible,” concluded the lawmakers.

The lawmakers are also asking Commerce to answer a set of questions about its plans concerning export licenses by February 7, 2024.

Senator Warren has led efforts to hold the Department of Commerce accountable for its lackluster oversight of firearms exports, which contradicts the Biden administration’s gun safety agenda:

- In September 2023, Senator Warren and Representatives Castro, Norma Torres (D-Calif.), and Dan Goldman (D-N.Y.) sent a letter to Secretary Raimondo, calling on Commerce to publicly release data on its approvals of assault weapons exports and provide a response to questions laid out in their September 2022 letter about Commerce’s troubling increase of assault weapons export approvals.

*(*Continued On The Following Page)*

January 23, 2024

**The Honorable Gina Raimondo Secretary of
Commerce - U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230**

Dear Secretary Raimondo:

We are writing in response to the Commerce Department's ("Commerce", "the Department") decision to temporarily pause approvals of new firearms export licenses and export promotion activity while it reviews the Department's relevant policies and procedures.¹ This is a positive development, coming after the number of firearms export license approvals skyrocketed when the Trump Administration transferred firearms export control authority from the State Department ("State") to Commerce.² The transfer—and the resulting increase in lethal weapons exports—has driven up gun violence in foreign countries, which in turn has driven more and more migration.³ While we continue to support returning all firearms export controls to the State Department, we urge the Commerce Department to incorporate the recommendations in this letter as part of its policy review in the interim, in order to strengthen export controls and end-use checks and to crack down on unnecessary export promotion of weapons used in brutal killings abroad. On October 27, 2023, the Commerce Department announced a 90-day pause of export approvals of certain firearms, related components, and ammunition while the Department reviews its export control policies and "determine[s] whether any changes are warranted."⁴ The pause on exports applies to certain assault weapons and other firearms that the Trump Administration had transferred from the export jurisdiction of State to Commerce. Commerce also paused the International Trade Administration's (ITA) activities to promote exports of those weapons. However, the pause does not apply to applications to export firearms to 44 countries, including Ukraine, Israel, and Mexico.⁵ The 90-day pause period will end on January 25, 2024.

1 Bureau of Industry and Security, "Bureau of Industry and Security Firearms Pause & Review: Frequently Asked Questions," October 27, 2023, <https://www.bis.doc.gov/index.php/documents/policy-guidance/3374-2023-10-27-bis-faqs-firearms-pause-and-review/file>.

2 Forum on the Arms Trade, "Transfer of Arms and Ammunition (USML Cat I-III) to Commerce," <https://www.forumarmstrade.org/catitooiii.html>.

3 Washington Post, "Why Gun Violence Has Become a Major US Export," Francis Wilkinson, August 12, 2023, https://www.washingtonpost.com/business/2023/08/12/biden-should-return-gun-export-regulation-back-to-statedepartment/60d40c30-390b-11ee-ac4e-e707870e43db_story.html.

4 Bureau of Industry and Security, "Bureau of Industry and Security Firearms Pause & Review: Frequently Asked Questions," October 27, 2023, <https://www.bis.doc.gov/index.php/documents/policy-guidance/3374-2023-10-27-bis-faqs-firearms-pause-and-review/file>.

5 Bureau of Industry and Security, "Bureau of Industry and Security Firearms Pause & Review: Frequently Asked Questions," October 27, 2023, <https://www.bis.doc.gov/index.php/documents/policy-guidance/3374-2023-10-27-bis-faqs-firearms-pause-and-review/file>; Bureau of Industry and Security, "License Exceptions," September 15, 2022, <https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-countrygroups-1/file>. (***Continued On The Following Column**)

Commerce's decision to initiate the pause and review process was welcome, but sorely needed. When some of us last wrote to you to raise our concerns about Commerce's lackluster oversight of firearms exports in September 2023,⁶ the Department's most recently published data on firearms exports and license approvals dated from June 2021. Later in the fall of 2023, the Department at long last published new data for July 2021 to June 2023 that once again showed a marked increase in license approvals.⁷ These new data show that from March 9, 2020 (the date of the Trump Administration's transfer) to June 30, 2023, Commerce approved nearly 25,000 firearms export licenses with a total value of \$34.7 billion, or roughly \$10.5 billion per year.⁸ This represents a more than \$1 billion increase in the annual value of license approvals as compared to the time period when the State Department controlled these approvals.⁹ As more and more firearms have left American shores, their impact in other countries has worsened. Reports abound of U.S.-manufactured weapons being used in horrific killings across the globe. In Thailand in October 2022, a gunman entered a nursery school and used an American-made Sig Sauer pistol to murder 36 people, including 23 children.¹⁰ In March 2022—the month with the most semiautomatic firearms exports from the U.S. to El Salvador in the previous four years—gang violence in that country killed a record 62 people.¹¹ U.S.-manufactured weapons have also had devastating impacts in countries that are not subject to the current pause. In June 2021, gunmen using U.S.-made firearms went on an eight hour-plus killing and kidnapping spree in Mexico.¹² There is also evidence to suggest that soldiers and civilian militias in Israel are using American-made semiautomatic weapons to perpetrate shocking violence against Palestinian civilians.¹³ The risks to civilians likely only increased after the Israeli government loosened gun 6 Letter from Senator Warren and Reps. Castro, Torres, and Goldman to Secretary Raimondo, September 6, 2023, <https://www.warren.senate.gov/imo/media/doc/2023.09.06%20Letter%20from%20Sen.%20Warren,%20Rep.%20Castro.pdf>.

7 Bureau of Industry and Security, "USML to CCL Regulatory Changes," <https://www.bis.doc.gov/index.php/statistical-reports/ecr-analysis>.

8 Forum on the Arms Trade, "Transfer of Arms and Ammunition (USML Cat I-III) to Commerce," <https://www.forumarmstrade.org/catitooiii.html>.

9 Government Accountability Office, "Export Controls: State and Commerce Should Share Watch List Information If Proposed Rules to Transfer Firearms Are Finalized," March 1, 2019, <https://www.gao.gov/products/gao-19-307>.

While GAO's review of the State Department's export license approvals includes some items not transferred to the CCL by the Trump administration's rule, a significant proportion of the items reviewed were semiautomatic and nonautomatic firearms that were subject to the transfer. See Forum on the Arms Trade, "Transfer of Arms and Ammunition (USML Cat I-III) to Commerce," <https://www.forumarmstrade.org/catitooiii.html>; Cato Institute, "2022 Arms Sales Risk Index," Jordan Cohen and A. Trevor Thrall, July 18, 2023, <https://www.cato.org/policy-analysis/2022-arms-sales-risk-index>.

10 Bloomberg, "How the US Drives Gun Exports and Fuels Violence Around the World," Michael Riley, David Kocieniewski and Eric Fan, July 24, 2023, <https://www.bloomberg.com/graphics/2023-us-made-gun-exportsshootings-violence-sig-sauer/>.

11 Just Security, "U.S. Guns Are Fueling Violence in Central America, Here's How to Help Stop the Arms Flow," Nate Smith, February 1, 2023, <https://www.justsecurity.org/84954/u-s-guns-are-fueling-violence-in-central-america/heres-how-to-help-stop-the-arms-flow/>.

(*Continued On The Following Page)

12 Foreign Policy, “Are U.S. Gun-Makers Responsible for Violence in Mexico?,” Chantal Flores, October 24, 2023, <https://foreignpolicy.com/2023/10/24/mexico-united-states-guns-arms-trafficking-lawsuit/>.

13 American Friends Service Committee, “U.S. Gun Exports to Israel: Report to Commerce Department,” January 5, 2024, <https://afsc.org/newsroom/us-gun-exports-israel-report-commerce-department>.

2

ownership requirements¹⁴ and authorized “temporary licensing official[s] with only a single day of training to approve “anywhere from hundreds to thousands of firearm licenses”¹⁵ over a few weeks. The 90-day pause also applies to the International Trade Administration’s (ITA) export promotion activity — welcome news in light of recent reporting detailing the unnecessarily close relationship between Commerce personnel and firearms exporters and importers. Since 2014, Commerce has worked directly with the National Shooting Sports Foundation (NSSF) and other gun industry mainstays to court foreign buyers of U.S. weapons.¹⁶ Reports indicate that Commerce officials and staff coordinate closely with the domestic gun industry to attract potential foreign customers to the annual Shooting, Hunting and Outdoor Trade Show (SHOT Show), which generates 75 percent of the NSSF’s revenue.¹⁷ One foreign gun importer noted, “The assistance we get from the Commerce Department, especially at SHOT Show, is invaluable ... You really can’t be in this business without that help.”¹⁸ Commerce classifies information about their work related to SHOT Show as “confidential commercial information,” meaning the public has little to no idea how much staff time and taxpayer dollars the Department spends on SHOT Show related activities each year.¹⁹ Despite the Biden Administration’s efforts to stem the tide of gun violence at home, Commerce continues to actively participate in firearms export promotion activities like the SHOT Show.

Clearly, a brief 90-day pause in export license approvals and promotion is insufficient to address the breadth of the problem. Before it ends this pause, Commerce must make significant changes to its export license approval and monitoring policies. These changes include:

1. Recognizing in a formal policy statement that firearms are the only lethal weapons on the Commerce Control List²⁰ and asserting that it is a foreign policy interest of the U.S. to restrain the global proliferation of these weapons.

2. Publicly posting requirements for end-use certification of exported semi-automatic firearms and committing to pre- and post-shipment transparency and end-use monitoring. The most recent public information from Commerce on firearms exports end-use monitoring is outdated, dating back to January 2020 (with slight updates in May 2021).²¹

*(*Continued On The Following Column)*

3. Adding “crime control” to the list of criteria systematically considered by Commerce prior to approving a firearms export license. The “crime control” factor specifically.

14 Washington Post, “Israel wants civilians to arm up. Gun permit applications are soaring,” Claire Parker, Jon Gerberg, Judith Sudilovsky, and John Hudson, December 8, 2023, <https://www.washingtonpost.com/world/2023/12/08/israel-gun-carry-permits/>.

15 Haaretz, “Head of Firearm Licensing Department Resigns After Ben Gvir’s Appointees Cut Corners on Gun Permits,” Yael Freidson, December 4, 2023, <https://www.haaretz.com/israel-news/2023-12-04/ty-article/.premium/top-firearms-official-resigns-after-ben-gvirs-appointees-cut-corners-on-gun-permits/0000018c-33cb-da74-afceb7fb542b0000>.

16 Bloomberg, “How Hundreds of US Government Employees Became Gun Industry Sales Reps,” Jessica Brice, Michael Smith, and Christopher Cannon, October 19, 2023, <https://www.bloomberg.com/graphics/2023-us-madegun-exports-shot-show-latin-america/?sref=8p3ICO8E>.

17 Id.

18 Id.

19 Id.

20 Bureau of Industry and Security, “Regulations,” <https://www.bis.doc.gov/index.php/regulations/exportadministration-regulations-ear>.

21 Bureau of Industry and Security, “FAQs for the Commerce Categories I-III (final rule),” updated May 28, 2021, <https://www.bis.doc.gov/index.php/documents/policy-guidance/2572-faqs-for-the-commerce-category-i-iii-firearmsrule-posted-on-bis-website-7-7-20/file>.

3. Accounts for the potential for exported firearms (including semiautomatic pistols equipping police forces) to be used by security forces for human rights violations and abuses.²²

4. Taking advantage of existing, comprehensive sources (such as the State Department’s International Vetting and Security Tracking-cloud system) when reviewing license applications to identify problematic proposed end users.

5. Encouraging countries of particular concern to fully participate in the Bureau of Alcohol, Tobacco, Firearms and Explosives’ (ATF’s) eTrace system to better track the use of U.S.-sourced firearms in criminal activity and facilitating programs to develop such capacities in countries of concern.

6. Reducing export license validity from four years to one year, particularly for destinations of concern.

7. Systematically reviewing licenses approved for export to countries importing very high numbers of firearms and confirming the identities of end users of these weapons. If the Department cannot verify the end user, it should consider revoking or amending the licenses.

*(*Continued On The Following Page)*

8. Capping exports of firearms to civilian buyers, and aggressively enforcing policies prohibiting transfers to security forces with an elevated risk of human rights abuse.

9. Capping the number of exported firearms that can be covered by any single export license, particularly for destinations of concern, and distinguishing between firearms destined for security forces of trusted allies versus civilians or commercial retailers.

10. Ending Commerce’s involvement in the SHOT Show and other firearms export promotion activities that can lead to, and even enable, gun violence and death abroad.

11. Using its authority under the Export Control Reform Act of 2018 to issue all policy changes stemming from the review process as final rules to ensure prompt implementation.²³

The Commerce Department’s decision to pause new firearm export approvals and promotion is welcome news. We urge the Commerce Department to implement our recommendations in its review of its export policies, and if necessary, to extend the temporary pause as needed to reconsider its export policies as rigorously as possible. Additionally, we request responses to the following questions no later than February 7, 2024:

1. Has Commerce consulted with external non-industry stakeholders (e.g., academics, survivors of gun violence) as part of its policy review?
2. Will Commerce release the findings of its review publicly, including which specific policies will be changed and how? If not, why not?
3. How long does Commerce anticipate implementing the policy changes stemming from its review this implementation process will take?

22 15 C.F.R. 742.7.

23 50 U.S.C. 4821. Commerce has previously used this authority to issue final rules amending firearms export controls: See e.g., Bureau of Industry and Security, Federal Register Notice, “Amendment to Licensing Policy for Items Controlled for Crime Control Reasons,” October 6, 2020, <https://www.federalregister.gov/documents/2020/10/06/2020-21815/amendment-to-licensing-policy-for-itemscontrolled-for-crime-control-reasons>.

4. How will Commerce engage with U.S. gun exporters to apprise them of the policy review’s findings and any resulting changes exporters will need to make to their pending or future applications?

Thank you for your attention to this important matter.
Sincerely,
Elizabeth Warren
United States Senator
Joaquin Castro
Member of Congress
Richard J. Durbin
United States Senator
Norma J. Torres
Member of Congress

FACT SHEET: Biden-Harris Administration Announces Temporary Pause on Pending Approvals of Liquefied Natural Gas Exports

President Biden has been clear that climate change is the existential threat of our time – and we must act with the urgency it demands to protect the future for generations to come. That’s why, since Day One, President Biden has led and delivered on the most ambitious climate agenda in history, which is lowering energy costs for hardworking Americans, creating millions of good-paying jobs, safeguarding the health of our communities, and ensuring America leads the clean energy future.

Today, the **Biden-Harris Administration is announcing a temporary pause on pending decisions on exports of Liquefied Natural Gas (LNG) to non-FTA countries until the Department of Energy can update the underlying analyses for authorizations.** The current economic and environmental analyses DOE uses to underpin its LNG export authorizations are roughly five years old and no longer adequately account for considerations like potential energy cost increases for American consumers and manufacturers beyond current authorizations or the latest assessment of the impact of greenhouse gas emissions. Today, we have an evolving understanding of the market need for LNG, the long-term supply of LNG, and the perilous impacts of methane on our planet. We also must adequately guard against risks to the health of our communities, especially frontline communities in the United States who disproportionately shoulder the burden of pollution from new export facilities. The pause, which is subject to exception for unanticipated and immediate national security emergencies, will provide the time to integrate these critical considerations.

The U.S. is already the number one exporter of LNG worldwide – with U.S. LNG exports expected to double by the end of this decade. At the same time, the U.S. remains unwavering in our commitment to supporting our allies around the world. Today’s announcement will not impact our ability to continue supplying LNG to our allies in the near-term. Last year, roughly half of U.S. LNG exports went to Europe, and the U.S. has worked with the E.U. to successfully economize consumption and manage its storage to ensure that unprovoked acts of aggression cannot threaten its supply. Furthermore, in 2022, the E.U and U.S. pledged to work toward the goal of ensuring additional LNG volumes for the E.U. market – with the U.S. exceeding our annual delivery targets to the E.U. in each of the past two years. Through existing LNG production and export infrastructure, the U.S. has – and will continue – to deliver for our allies.

Firearms Export Control Pause & Review October 27, 2023

International Trade Administration
Effective immediately, the U.S. Department of Commerce (the Department) is pausing for approximately 90 days the issuance of new export licenses involving certain firearms, related components, and ammunition under its jurisdiction and the provision of new export assistance activities for such products to all non-governmental end users worldwide, apart from those in certain destinations.

*(*Continued On The Following Page)*

During this “pause” period, the Department will further assess current firearm export control review policies to determine whether any changes are warranted to advance U.S. national security and foreign policy interests. The review will be conducted with urgency and will enable the Department to more effectively assess and mitigate risk of firearms being diverted to entities or activities that promote regional instability, violate human rights, or fuel criminal activities. ITA simultaneously will review its export assistance policy to ensure that ITA export assistance is consistent with applicable export controls and does not undermine U.S. policy interests. This pause applies to the Bureau of Industry and Security’s (BIS) issuance of new licenses involving certain firearms, related components, and ammunition controlled on the Commerce Control List, Supp. No. 1 to part 774 of the Export Administration Regulations, 15 CFR parts 730-774 (EAR), specifically, the following four Export Control Classification Numbers (ECCNs): ECCN 0A501, ECCN 0A502, ECCN 0A504, and ECCN 0A505, that are destined for non-governmental end users worldwide apart from those located in Ukraine, Israel, or a country in Country Group A:1 (Wassenaar Arrangement Participating States), Supp. No. 1 to part 740 of the EAR.

Consistent with the above, the Department’s International Trade Administration (ITA), Global Markets and U.S. & Foreign Commercial Service is pausing acceptance of new requests for export assistance (fee or non-fee-based) for firearms and ammunition to non-governmental end users worldwide, apart from those located in Ukraine, Israel, and Country Group A:1. The ITA pause applies to semi-automatic and non-automatic firearms, shotguns, and receivers (frames) and ammunition.

Additional information may be found at <https://www.bis.doc.gov/index.php/documents/policy-guidance/3374-2023-10-27-bis-faqs-firearms-pause-and-review/file>.

BIS May Be Drafting New Firearms Export Restrictions, Document Shows

27 Dec 2023 by [Ian Cohen](#)

The Bureau of Industry and Security may be preparing to introduce new export rules for certain firearms, gun parts and ammunition, including one change that would require certain end-users to submit their passports to BIS and another that would shorten the validity period of certain licenses from four years to one year. Other changes could introduce new Export Control Classification Numbers for certain firearms and parts, require exporters to first obtain an import certificate from the importing country, and create a new working group to review firearms-related license applications.

FOR IMMEDIATE RELEASE

January 30, 2024

www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

BIS IMPOSES \$153,175 PENALTY AGAINST WABTEC CORPORATION TO RESOLVE ALLEGED VIOLATIONS OF ANTIBOYCOTT REGULATIONS

WASHINGTON, D.C.-- Yesterday, the Department of Commerce’s Bureau of Industry and Security (BIS) imposed a civil penalty of \$153,175 against Wabtec Corporation (Wabtec), a global manufacturer and supplier of rail technology headquartered in Pittsburgh, Pennsylvania, to resolve 43 violations of the antiboycott provisions of the Export Administration Regulations (EAR) (antiboycott regulations) alleged in BIS’s Proposed Charging Letter. Wabtec voluntarily disclosed the conduct to BIS, cooperated with the investigation by BIS’s Office of Antiboycott Compliance (OAC), and took remedial measures after discovering the conduct at issue, which resulted in a significant reduction in the penalty.

“This settlement involves failures to report Pakistan-origin boycott-related requests, underscoring the need for companies to be vigilant for boycott-related language regardless of the country of origin,” said **Assistant Secretary for Export Enforcement Matthew S. Axelrod**. “It’s not enough just to decline boycott-related requests – our rules require companies to come tell us that certain requests were made.”

BIS Case Background:

As part of the BIS settlement, Wabtec admitted to the conduct set forth in a Proposed Charging Letter, which alleged 43 violations of Section 760.5 of the EAR (Failing to Report the Receipt of a Request to Engage in a Restrictive Trade Practice or Foreign Boycott Against a Country Friendly to the United States). Specifically, between February 2018 and July 2022, on forty-three occasions, Wabtec received a request from a customer in Pakistan to refrain from importing Israeli-origin goods into Pakistan in fulfillment of its orders. Wabtec failed to report to BIS the receipt of these requests, as required by Section 760.5 of the EAR, thereby giving rise to the 43 alleged violations.

The Order, Settlement Agreement, and Proposed Charging Letter are available [here](#).

Additional Information:

These BIS actions were taken under the authority of the Anti-Boycott Act of 2018, a subpart of the Export Control Reform Act of 2018, and its implementing regulations, the EAR. The antiboycott provisions set forth in Part 760 of the EAR discourage, and in certain circumstances prohibit, U.S. persons from taking certain actions in furtherance or support of a boycott maintained by a foreign country against a country friendly to the United States (an unsanctioned foreign boycott).

*(*Continued On The Following Page)*

In addition, U.S. persons must report to OAC their receipt of certain boycott-related requests. Reports may be filed electronically or by mail on form BIS 621-P for single transactions or on form BIS 6051P for multiple transactions involving boycott requests received in the same calendar quarter. U.S. persons located in the United States must postmark or electronically date stamp their reports by the last day of the month following the calendar quarter in which the underlying request was received. For U.S. persons located outside the United States, the postmark or date stamp deadline is the last day of the second month following the calendar quarter in which the request was received. Forms for both electronic transmission and mail submission may be accessed on the forms request page.

Pursuant to Section 764.8 of the EAR, a party may submit a voluntary self-disclosure if it believes that it may have violated Parts 760 or 762 of the EAR (recordkeeping requirements relating to Part 760).

For information regarding the application of the antiboycott regulations, please contact the OAC Advice Line at (202) 482-2381 or through the [online portal](#).

Ocean State tapped as tech hub **By [ohtadmin](#) | on October 26, 2023**

Building on decades of investment, research and innovation in oceanography, the Ocean State is being recognized for driving American global competitiveness in technology.

The U.S. Department of Commerce has designated Rhode Island as a regional tech hub. The announcement of the 31 inaugural sites was made Monday by Gina Raimondo, secretary of the agency.

“Each of these consortia will help us ensure the industries of the future, and their good-paying jobs, start, grow and remain in the United States,” said the former governor.

According to U.S. Sen. Jack Reed’s office, Rhode Island was selected for the first-of-its-kind designation due to its potential for rapid growth in undersea robotics, automation and advanced materials. The designation also positions the state to compete for the next phase of money through the program, which will invest between \$50 to \$75 million in at least five regional hubs.

The Ocean Tech Hub, a consortium led by the Rhode Island Commerce Corporation, will leverage the state’s unique coastal assets, including seven commercial ports, to establish digital and physical testing and manufacturing environments for rapid prototype testing and delivery to meet the growing commercial demand. In doing so, the hub will seek to advance innovative maritime technology and become a global leader in the growing blue economy.

“The Ocean State is a leader in ocean tech and the blue economy,” said Reed, a Jamestown resident. “This tech hub designation, paired with federal funding for Rhode Island, will help foster more collaboration and development across our region to position the Ocean State as a global leader in undersea automation and technological development.”

*(*Continued On The Following Column)*

This designation is part of the first phase of the novel tech hubs program that will invest directly in high-potential U.S. regions and aims to transform these sites into globally competitive innovation centers. Designation is an endorsement of the region’s strategy to supercharge its respective technological industry to create jobs and strengthen U.S. economic and national security, according to Reed’s office.

In addition to being named home to the nation’s first Ocean Tech Hub, Rhode Island also is receiving a grant of \$346,496 to help the consortium increase coordination and planning across Southern New England. This money will help strengthen the region’s capacity to manufacture, commercialize and deploy critical ocean technologies that have wide-ranging applicability for industries ranging from aquaculture to shipping to climate mitigation and telecommunications.

The 31 hubs were selected from 400 applications from regional consortia that include industry, academia, governments, economic developers and labor unions. The hubs span regions across 32 states and Puerto Rico.

“Ocean technology and the ocean economy has been part of the innovation ecosystem in Rhode Island for decades,” Gov. Dan McKee said. “This designation validates Rhode Island’s national position in this growing global market and gives us the fuel to build critical infrastructure that will further drive U.S. economic and national security.”

Members of the Ocean Tech Hub include Brown University, Rhode Island College, the University of Rhode Island, the University of Massachusetts at Dartmouth, RI-AFLCIO, 401 Tech Bridge, IBM, Infused Innovations, New Bedford Ocean Cluster, Rhode Island Department of Labor & Training, Rhode Island Marine Trades Association, the city of Providence and the Southeastern Regional Planning & Economic Development District. Jaia Robotics, co-founded by Jamestown resident Ian Estaphan Owen, also is a member.

The program is paid for by the bipartisan CHIPS and Science Act, signed into law by President Joe Biden in August 2022. Reed supported the bill, which he said protects taxpayers by ensuring they get the best return on investment.

“The CHIPS Act is about strengthening our national security, economy and supply chains,” he said. “It’s not a free handout for multi-billion-dollar tech companies ... Upside sharing ensures taxpayers will fairly and rightly get a piece of unexpected profits from smart U.S. investments. There is no downside for companies that participate because they only have to share a portion of future profits if they do exceedingly well.”

*(*Continued On The Following Page)*

WASHINGTON POST REPORTS

Feb 1, 2024

Since January 2023, I Machine Technology (in Russia) has imported over \$20 million of sophisticated equipment called CNC machine tools made in Taiwan, a U.S. strategic partner, according to trade records and Russian tax documents obtained by The Washington Post. The computer-controlled machines are used for the complex and precise manufacturing that is critical in many industries, including weapons production.

Chinese Nationals Charged with Illegally Exporting U.S.-Origin Electronic Components to Iran and Iranian Military Affiliates

Four Chinese nationals are charged in an indictment in the District of Columbia with various federal crimes related to a years-long conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran.

According to court documents, Baoxia Liu, aka Emily Liu; Yiu Wa Yung, aka Stephen Yung; Yongxin Li, aka Emma Lee; and Yanlai Zhong, aka Sydney Chung, unlawfully exported and smuggled U.S. export controlled items through China and Hong Kong ultimately for the benefit of entities affiliated with the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Defense and Armed Forces Logistics (MODAFL), which supervises Iran's development and production of missiles, weapons, and military aerial equipment to include Unmanned Aerial Vehicles (UAVs).

"For more than a decade, the defendants allegedly orchestrated a scheme to smuggle U.S. manufactured parts to the IRGC and the Iranian agency charged with developing ballistic missiles and UAVs," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "Such efforts to unlawfully obtain U.S. technology directly threaten our national security, and we will use every tool at our disposal to sever the illicit supply chains that fuel the Iranian regime's malign activity."

"Aggressively combating illicit procurement networks that support Iranian military systems like radars and UAVs is essential to U.S. national security," said Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Department of Commerce. "Today's indictment, tied to the work of the Disruptive Technology Strike Force, reaffirms that proliferators cannot hide behind front companies in third countries to funnel technology to our adversaries."

"Our indictment alleges a years-long, complex conspiracy to violate U.S. laws by procuring U.S. technology with military uses for entities in Iran who would do us harm – a serious offense that endangers our national security," said U.S. Attorney Matthew M. Graves for the District of Columbia. "Our office, along with our federal law enforcement partners, will continue to turn over every stone to find those who break our laws and put us at risk. We are committed to making sure that U.S. technology is kept out of the hands of those taking aim at the United States and its citizens through robust enforcement of U.S. sanctions."

(*Continued On The Following Column)

"Our foreign adversaries use many tactics to gain access to critical U.S. technologies and innovation," said Executive Assistant Director Larissa L. Knapp of the FBI's National Security Branch. "In this instance, it is alleged that U.S.-origin equipment was smuggled by front companies to the benefit of end users in Iran. Any circumvention of U.S. export control law is simply unacceptable – the FBI will work diligently with its partners across the globe to hold all accountable who jeopardize our national security."

According to the indictment, beginning as early as May 2007 and continuing until at least July 2020, the defendants utilized an array of front companies in the People's Republic of China (PRC) to funnel dual-use U.S.-origin items, including electronics and components that could be utilized in the production of UAVs, ballistic missile systems, and other military end uses, to sanctioned Iranian entities with ties to the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Defense and Armed Forces Logistics (MODAFL) such as Shiraz Electronics Industries (SEI), Rayan Roshd Afzar, and their affiliates.

Throughout the course of the conspiracy, the defendants concealed the fact that the goods were destined for Iran and Iranian entities and made material misrepresentations to U.S. companies regarding the end destination and end users. These deceptive practices caused the U.S. companies to export goods to the defendants' PRC-based front companies under false pretenses and under the guise that the ultimate destination of these products was China as opposed to Iran. As a result, a vast amount of dual-use U.S.-origin commodities with military capabilities were exported from the United States to Iran in violation of U.S. sanctions and export control laws and regulations.

The defendants are charged with conspiring to violate the International Emergency Economic Powers Act (IEEPA), violating IEEPA, smuggling goods from the United States, and one count of submitting false or misleading export information. If convicted, the defendants face a maximum penalty of 20 years in prison for violating the IEEPA; up to 10 years in prison for smuggling goods from the United States; and up to five years in prison for each count of conspiracy and submitting false or misleading export information. Arrest warrants have been issued for Liu, Yung, Li and Zhong who all remain fugitives.

The FBI's Detroit Field Office and Commerce Department's Office of Export Enforcement Chicago Field Office are investigating the case. Assistant U.S. Attorney Jack F. Korba for the District of Columbia and Trial Attorneys Heather Schmidt and Yifei Zheng of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

In June 2023, the Department of Justice joined with the Departments of Commerce, State, and Treasury to issue [an advisory](#) to share information about the threat posed by Iran's procurement, development, and proliferation of UAVs. Four months later, in October 2023, the department joined with the same interagency partners to issue [an advisory](#) describing the threat posed by Iran's ballistic missile procurement activities.

(*Continued On The Following Page)

The advisories gave an overview of the key components sought by Iran, the regime's use of deceptive practices to acquire certain types of technologies, and recommendations for implementing effective compliance controls to minimize sanctions and export control risk.

Today's action was coordinated through the Disruptive Technology Strike Force, an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation-states. Under the leadership of the Assistant Attorney General for National Security and the Assistant Secretary of Commerce for Export Enforcement, the Strike Force leverages tools and authorities across the U.S. government to enhance the criminal and administrative enforcement of export control laws.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated February 1, 2024

MISSION STATEMENT:

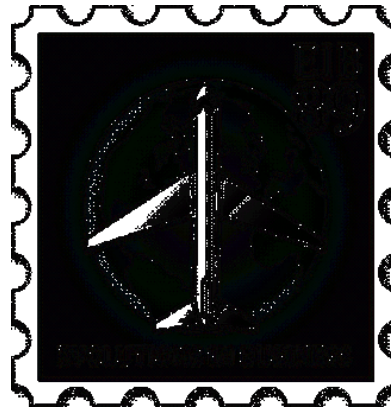
Given the geopolitical state of affairs with China, Russia, and Crimea, the Occupied territories of UKRAINE, Donetsk and Luhansk Oblast, embargoed countries and other specific threatening end users and entities, located in the United States and around the globe;

Evolutions in Business and the companies we serve, armed with robust compliance to the Export Administration Regulations, will adhere to best practices to protect our revenue and yours, and ensure the national security interests of the United States.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Evolutions in Business

*Celebrating more
than 30 Years*



Keep up to date with latest trade news at:

www.eib.com

Check out our latest podcast:

New BIS Rules for Freer Trade
<https://www.buzzsprout.com/1592353/14400490>