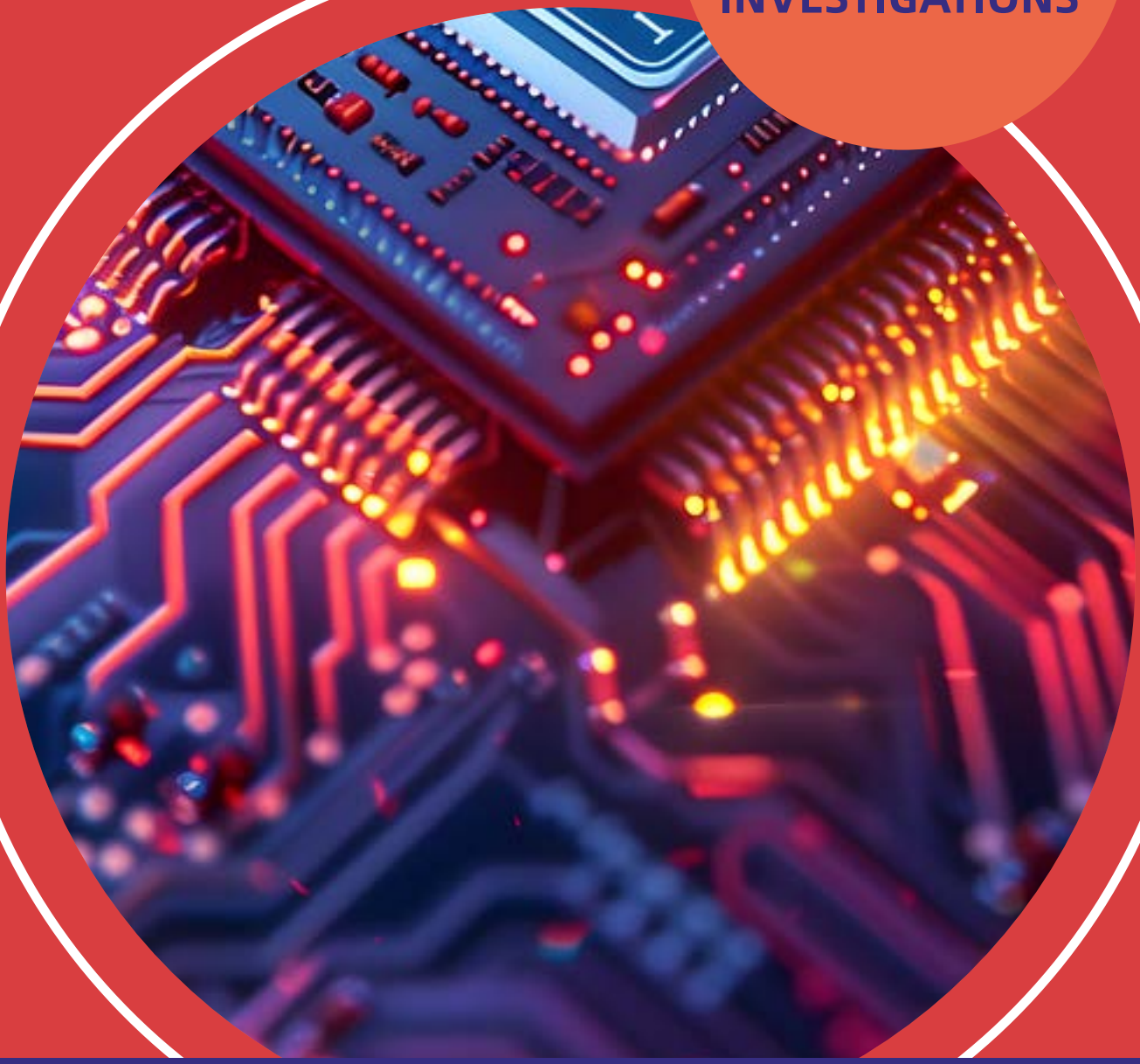
# THE U.S. TECHNOLOGY FUELING RUSSIA'S WAR IN UKRAINE:

## EXAMINING THE BUREAU OF INDUSTRY AND SECURITY'S ENFORCEMENT OF SEMICONDUCTOR EXPORT CONTROLS

**PERMANENT SUBCOMMITTEE ON INVESTIGATIONS**



# Table of Contents

## Executive Summary

Export controls have emerged as one of the United States' leading tools to advance its geopolitical goals, used both to cripple China's access to technologies that would give it an edge in emerging technologies, and to prevent Russia from obtaining the technology it needs to continue its war against Ukraine. Despite these efforts, these tools have consistently fallen short in constraining China's ambitions and Russia's war. China has created vast, barely disguised smuggling networks which enable it to continue to harness U.S. technology. Meanwhile, U.S. microchips continue to guide and power the Russian weapons that kill Ukrainians daily.

The Permanent Subcommittee on Investigations ("PSI" or "the Subcommittee") initiated an inquiry in September 2023 to better understand why U.S. semiconductor export controls have continued to fail. The Subcommittee initially focused its inquiry on four U.S.-based semiconductor manufacturers whose products have consistently been discovered in Russian weapons: Advanced Micro Devices Inc. ("AMD"), Analog Devices Inc. ("Analog Devices"), Intel Corporation ("Intel"), and Texas Instruments Inc. ("Texas Instruments"). On September 10, 2024, the Subcommittee's majority staff released the first report in the Subcommittee's investigation, explaining how U.S. semiconductor manufacturers' export control compliance efforts have been abjectly lacking. The Subcommittee also held a hearing that day at which representatives from these four companies testified regarding the flaws in their export controls compliance programs.

In addition to examining the export control programs at Analog Devices, Intel, Texas Instruments, AMD, and in the U.S. semiconductor manufacturing industry more broadly, the Subcommittee's inquiry also considered the role of government enforcement in the effectiveness of U.S. export controls. Enforcement of export controls on semiconductors is principally the responsibility of the Department of Commerce's Bureau of Industry and Security (BIS).

The Subcommittee's inquiry has revealed that enforcement of export controls is a shadow of what it should be, and inadequate at every level. BIS is asked to fulfill a key national security function on a shoestring budget, forcing it to trace increasingly sophisticated distribution networks while relying on laughable technology that has not been meaningfully updated for nearly two decades.

But, even with these constraints, BIS's enforcement efforts have been inadequate. BIS has largely left the decision of how to comply with the law to semiconductor companies themselves, imposing no requirements for specific components an export control program must contain and mandating no meaningful outside review of semiconductor companies' export control programs. Even when violations are present, BIS has not charged companies with sufficiently serious violations or imposed fines sufficiently robust to compel better compliance.

Specifically, the Subcommittee's inquiry found:

- **Congress has not provided BIS with adequate funding to fulfill its mission.**
    - BIS's workload and responsibilities tied to national security have drastically increased since 2010, but its funding has remained mostly stagnant.
    - BIS lacks funding to conduct enough international end-use checks, a critical tool in enforcing export controls. This has resulted in limited end-use checks in countries which (1) are known to have entities engaged in transshipment of semiconductors to Russia, and (2) were identified in the Subcommittee's September 10, 2024 report as having substantial increases in imports of U.S.-manufactured semiconductors in 2022 and 2023.
    - BIS's core IT systems were created in 2006 and have received only patchwork fixes in the nearly two decades since. BIS cannot afford the modern IT infrastructure needed to analyze the full range of data available to combat efforts at export control diversion.
- **BIS has failed to fully use its existing authority to enforce export controls.**
    - The Export Administration Regulations (EAR) and Export Control Reform Act of 2018 (ECRA) give BIS robust and unique powers to implement and enforce export controls.
    - Despite its significant authority, BIS does not require that semiconductor companies' export control programs contain any specific components.
    - BIS has not adequately charged companies for "knowing" violations of the EAR.
    - BIS has not imposed significant fines for export control violations despite publicly acknowledging the need for larger penalties.

Accordingly, this report makes the following recommendations:

**(1) Congress should provide BIS adequate funding to manage its increased workload and responsibilities.**

**(2) BIS should accelerate plans to impose higher fines on companies who violate export controls.**

**(3) BIS should charge companies with "knowing" violations when they fail to sufficiently investigate red flags or other strong indicia of potential diversion and violations occur.**

**(4) BIS should rely less on voluntary compliance from semiconductor companies and instead mandate specific components an export control compliance program must contain.**

**(5) BIS should require periodic, routine reviews of semiconductor companies' export control plans by outside entities.**

# Part I: Background

## A. The Subcommittee's Inquiry

In September 2023, the Subcommittee launched an inquiry into the continued appearance of U.S.-manufactured semiconductors in Russian weapons despite U.S. export controls. The Subcommittee requested documents and information from AMD, Analog Devices, Intel, and Texas Instruments, four of the largest U.S. semiconductor manufacturers whose technology had been repeatedly found in Russian weapons used against Ukraine.[1] The Subcommittee requested information and records concerning each company's export control compliance procedures and processes, evidence of their handling of reports of their products in Russian weapons, and data on their exports from 2021 to the present to Russia and 10 other countries that have been identified as countries with entities that have assisted or potentially assisted the Russian Federation in acquiring semiconductors (Armenia, Belarus, China, Finland, Georgia, Hong Kong, Kazakhstan, Kyrgyzstan, Turkey, and Uzbekistan).[2] The Subcommittee also requested information and records from the Department of Commerce's Bureau of Industry and Security (BIS), which is the principal government agency responsible for export controls on semiconductors. The Subcommittee sought records from BIS concerning enforcement efforts, the presence of U.S.-manufactured semiconductors in Russian

[1] As detailed in the Subcommittee's September 10, 2024 majority staff report, multiple public reports have consistently named these four companies as having the most foreign-made products found in Russian weapons examined on the battlefield. *See* MAJORITY STAFF OF S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 118TH CONG., THE U.S. TECHNOLOGY FUELING RUSSIA'S WAR IN UKRAINE: EXAMINING SEMICONDUCTOR MANUFACTURERS' COMPLIANCE WITH EXPORT CONTROLS (2024), https://www.hsgac.senate.gov/wp-content/uploads/09.10.2024-Majority-Staff-Report-The-U.S.-Technology-Fueling-Russias-War-in-Ukraine.pdf [hereinafter PSI September 2024 Report]; *see also, e.g.*, JAMES BYRNE ET AL., ROYAL UNITED SERVS. INST., SILICON LIFELINE: WESTERN ELECTRONICS AT THE HEART OF RUSSIA'S WAR MACHINE (2022), https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf [hereinafter Byrne et al., SILICON LIFELINE]; CONFLICT ARMAMENT RSCH., IDENTIFYING POST-INVASION COMPONENTS IN RUSSIAN WEAPONS (Emily Youers ed., 2023), https://storymaps.arcgis.com/stories/00594bef40bc4148b16dc7267172d033; OLENA BILOUSOVA ET AL., KSE INST., RUSSIA'S MILITARY CAPACITY AND THE ROLE OF IMPORTED COMPONENTS (2023), https://kse.ua/wp-content/uploads/2023/06/Russian-import-of-critical-components.pdf [hereinafter Bilousova et al., RUSSIA'S MILITARY CAPACITY]; JAMES BYRNE ET AL., ROYAL UNITED SERVS. INST., IN PLAIN SIGHT: OPERATIONS OF A RUSSIAN MICROELECTRONICS DYNASTY (2023), https://rusi.org/explore-our-research/publications/commentary/report-plain-sight-operations-russian-microelectronics-dynasty [hereinafter Byrne et al., IN PLAIN SIGHT] OLENA BILOUSOVA ET AL., KSE INST., CHALLENGES OF EXPORT CONTROLS ENFORCEMENT: HOW RUSSIA CONTINUES TO IMPORT COMPONENTS FOR ITS MILITARY PRODUCTION (2024), https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf [hereinafter Bilousova et al., CHALLENGES OF EXPORT CONTROL ENFORCEMENT].

[2] *See, e.g.*, Nathaniel Taplin, *How Russia Supplies Its War Machine*, WALL ST. J. (March 10, 2023), https://www.wsj.com/articles/russia-ukraine-tech-chips-exports-china-f28b60ca; Georgi Kantchev, Paul Hannon & Laurence Norman, *How Sanctioned Western Goods Are Still Flowing Into Russia*, WALL ST. J. (May 14, 2023), https://www.wsj.com/articles/how-sanctioned-western-goods-are-still-flowing-into-russia-916db262; Natalia Drozdiak, *EU Backs More Sanctions on Belarus Over Aiding Russia's War*, BLOOMBERG (Aug. 3, 2023), https://www.bloomberg.com/news/articles/2023-08-03/eu-backs-more-sanctions-on-belarus-over-aiding-russia-s-war#xj4y7vzkg; Gaya Gupta, *U.S. Aims New Sanctions at Russian Military Supply Chains*, N.Y. TIMES (Sept. 14, 2023), https://www.nytimes.com/2023/09/14/world/europe/us-sanctions-russia.html.

weapons, and guidance provided to semiconductor manufacturers, including Analog Devices, Intel, Texas Instruments, and AMD.[3]

During the subsequent 15 months, the Subcommittee reviewed thousands of pages of documents and data from AMD, Analog Devices, Intel, Texas Instruments, and BIS, and received briefings from representatives from AMD, Analog Devices, Intel, non-governmental organizations focused on tracing the technology utilized in weapons in the Russia-Ukraine war, and current and former government officials at BIS and the Department of State.

On February 27, 2024, the Subcommittee held a hearing with experts from Royal United Services Institute (RUSI), Conflict Armament Research (CAR), and KSE Institute at the Kiev School of Economics, organizations that have done significant work tracking and tracing the flow of U.S.-manufactured semiconductors to Russia and the continued appearance of U.S.-manufactured semiconductors in Russian weapons.[4]

On September 10, 2024, the Subcommittee's majority staff released a report regarding the failure of the export control compliance programs at Analog Devices, Intel, Texas Instruments, AMD, and in the U.S. semiconductor industry more generally.[5] That same day the Subcommittee held a hearing with representatives from each of these four companies to discuss their inability to consistently stop their products from appearing in Russian weapons, and ways they could improve their export controls compliance programs.[6]

## B. The increasing use of semiconductor export controls as a tool of national security

Over the last fifteen years, export controls have emerged as a defining tool of national security.[7] They are increasingly relied on to both hamper U.S. adversaries' present military

[3] Letter from the Hon. Richard Blumenthal, Chairman, Permanent Subcomm. on Investigations (hereinafter "Chairman Blumenthal") to U.S. Dep't of Com. Sec'y Gina Raimondo (Feb. 27, 2024), https://www.hsgac.senate.gov/wp-content/uploads/2024-2-27-Blumenthal-to-Secretary-Raimondo-002.pdf.

[4] The U.S. Technology Fueling Russia's War in Ukraine: How and Why: Hearing Before the Permanent Subcomm. on Investigations, 118th Cong. (2024), https://www.hsgac.senate.gov/subcommittees/investigations/hearings/the-u-s-technology-fueling-russias-war-in-ukraine-how-and-why/ [hereinafter PSI February 2024 Hearing].

[5] PSI September 2024 Report, *supra* note 1.

[6] The U.S. Companies' Technology Fueling the Russian War Machine: Hearing Before the Permanent Subcomm. on Investigations, 118th Cong. (2024), https://www.hsgac.senate.gov/subcommittees/investigations/hearings/the-us-companies-technology-fueling-the-russian-war-machine/.

[7] *See, e.g.*, CTR. FOR A NEW AM. SEC., *Export Controls Are a Defining Instrument of U.S. National Security*, https://www.cnas.org/export-controls-are-a-defining-instrument-of-u-s-national-security (last accessed Dec. 16, 2024); Anthony Rapa, *Export Controls Are a New National Security Focus — What That Means for Banks*, BLANKROME

production, and to create a strategic technology barrier to prevent these countries from gaining a military advantage in the future.[8] One of the principal export controls meant to carry out these goals is the Foreign Direct Product Rule (FDPR).[9] Originally conceived during the Cold War,[10] FDPRs were revitalized in 2013 and 2014 to restrict exports of products made abroad with American technology if they were destined for military use or the development of satellites in China.[11] In 2020, BIS crafted an FDPR specifically targeting Huawei, a Chinese multinational digital communications technology corporation.[12] A year earlier, BIS had added Huawei to the Entity List, banning it from receiving exports or transfers of items subject to the EAR in part because of its access to American 5G technology.[13]

The theoretical effectiveness of FDPRs to accomplish these goals relies on the preeminent place of U.S. manufactured semiconductors in global technology. American companies dominate the global semiconductor manufacturing industry, holding nearly half the global market share.[14] American semiconductor companies also have a leading position in research and development,

---

(Mar. 19, 2024), https://www.blankrome.com/publications/export-controls-are-new-national-security-focus-what-means-banks#:~:text=The%20U.S.%20maintains%20two%20sets,defense%20articles%20and%20defense%20services.

[8] PSI February 2024 Hearing, *supra* note 4.

[9] *See, e.g.*, THE ECONOMIST, *Chains of Control: The History and Limits of America's Favourite New Economic Weapon*, (Feb. 11, 2023), https://www.economist.com/united-states/2023/02/08/the-history-and-limits-of-americas-favourite-new-economic-weapon.

[10] Exportations of Technical Data, 24 Fed. Reg. 3987, 3989 (May 16, 1959) (codified at 15 C.F.R. § 385.2), https://www.govinfo.gov/content/pkg/FR-1959-05-16/pdf/FR-1959-05-16.pdf. Now called the "National Security FDPR." 15 CFR § 734.9(b).

[11] Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform, 78 Fed. Reg. 22,660, 22,667-68 (Apr. 16, 2013) (codified at 15 C.F.R. §§ 736, 764), https://www.govinfo.gov/content/pkg/FR-2013-04-16/pdf/2013-08352.pdf; THE ECONOMIST, *Chains of Control: The History and Limits of America's Favourite New Economic Weapon*, (Feb. 11, 2023), https://www.economist.com/united-states/2023/02/08/the-history-and-limits-of-americas-favourite-new-economic-weapon; Revisions to the Export Administration Regulations (EAR): Control of Spacecraft Systems and Related Items the President Determines No Longer Warrant Control Under the United States Munitions List (USML), 79 Fed. Reg. 27,418 (May 13, 2014) (codified at 15 C.F.R. §§ 740, 748), https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2014/934-79fr27417-commerce-spacecraft-systems-and-related-items-rule/file.

[12] Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51,596 (Aug. 20, 2020) (codified at 15 C.F.R. §§ 736, 744, 762), https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2593-85-fr-51596/file/.

[13] Paul K. Kerr & Christopher A. Casey, *The US Export Control System and the Export Control Reform Act of 2018*, CONG. RSCH. SERV. 28 (June 7, 2021), https://crsreports.congress.gov/product/pdf/R/R46814.

[14] SEMICONDUCTOR INDUS. ASS'N, *2023 Factbook* 3 (2023), https://www.semiconductors.org/wp-content/uploads/2023/05/SIA-2023-Factbook_1.pdf.

design, and semiconductor process technology.[15] This includes the development and production of cutting edge A.I. chips.[16]

The U.S. enacted export controls against Russia to try to undermine Russia's ability to bolster its present military production. In announcing these measures in 2022, President Biden stated they were designed to cut off more than half of Russia's high-tech imports and impair "their ability to continue to modernize their military."[17] BIS similarly noted that the focus of the restrictions was to "severely restrict Russia's access to technologies and other items that it needs to sustain its aggressive military capabilities."[18]

Export controls against China, by contrast, demonstrate an attempt to leverage U.S. semiconductor manufacturing dominance to create a strategic technology barrier to prevent China from gaining a future military advantage. BIS issued an FDPR on October 7, 2022, to restrict the production of semiconductors and advanced computing items with AI applications in China.[19] The logic of this measure was that advanced chips, and the supercomputers and A.I. systems they power, enable the production of new weapons and surveillance apparatuses.[20] The FDPR was designed to maintain the United States' technological primacy on the development and production of those chips.[21]

## C. BIS has expansive authority to regulate the export of dual use goods such as semiconductors

BIS is the principal U.S. government body responsible for export controls on dual use goods (those having both a civil and military application) such as semiconductors. BIS's stated mission is to "[a]dvance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic

[15] *Id.*

[16] Alex W. Palmer, *'An Act of War': Inside America's Silicon Blockade Against China*, N.Y. TIMES (Aug. 11, 2023), https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html.

[17] President Joseph Biden, Remarks on Russia's Unprovoked and Unjustified Attack on Ukraine (Feb. 24, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/.

[18] Press Release, Dep't of Com., Commerce Implements Sweeping Restrictions on Exports to Russia in Response to Further Invasion of Ukraine (Feb. 24, 2022), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2914-2022-02-24-bis-russia-rule-press-release-and-tweets-final/file.

[19] Palmer, *supra* note 16.

[20] *Id.*

[21] *Id.*

technology leadership."[22] BIS implements and enforces the Export Administration Regulations (EAR), which are based on the Export Administration Act of 1979. Recently, BIS's authority was enhanced and expanded by the Export Control Reform Act (ECRA) of 2018, which (among other things) made BIS's authority to control dual use exports permanent.[23]

The resulting legal framework has left BIS exceptional among executive agencies because it is relatively unconstrained in the exercise of its authority. For instance, the ECRA created new interagency procedures to identify and control emerging and foundational technologies "essential to the national security of the United States."[24] In addition to broadly setting forth the sources of information and considerations BIS must weigh, the ECRA requires these determinations to undergo an informal notice and comment period.[25] Otherwise, BIS selects for control dual-use items that are detrimental to the national security of the United States[26] by "rely[ing]" on "the Secretary of Defense, the Secretary of State, the Secretary of Energy, the Director of National Intelligence, and the heads of other Federal agencies *as appropriate*."[27] BIS is largely free to implement export control policy as it sees fit, so long as controls are administered transparently and predictably, coordinated with multilateral regimes as much as possible, and directed at preserving military, scientific, and technological advantages.[28]

Similarly, BIS enforcement actions are relatively unencumbered by the procedural prescriptions that attach to other agencies. BIS is almost entirely exempt from Administrative Procedure Act requirements.[29] Because Presidential exercises of authority in foreign affairs are owed deference,[30] denials of export privileges were initially unreviewable by the courts.[31] Following Congressional amendment, BIS adjudications of control violations are now required to undergo

---

[22] BUREAU OF INDUS. AND SEC., *About BIS*, https://www.bis.doc.gov/index.php/about-bis (last accessed Dec. 16, 2024).

[23] 50 U.S.C. § 4826(a).

[24] 50 U.S.C. § 4817(a) (1).

[25] 50 U.S.C. § 4817(a) (2). It also requires BIS to, at minimum, issue a license requirement for such technology exported, re-exported, or transferred to a country embargoed by the United States. § 4817(b)(2)(C).

[26] *See* 50 U.S.C. § 4811(1) (A).

[27] 50 U.S.C. § 4814(a) (emphasis added).

[28] *See* 50 U.S.C. § 4811(3)-(11). One additional constraint on this authority is that BIS entity listings are subject to review and approval by the End User Review Committee, composed of representatives of the Departments of State, Defense, Energy, and Commerce. *See* 15 CFR § 748 supp. 9.

[29] 50 U.S.C. § 4821(a).

[30] Zivotofsky ex rel. Zivotofsky v. Kerry, 576 U.S. 1, 20-21 (2015) (discussing U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304, 315-29 (1936)).

[31] In 1965, Commerce was given authority to initiate suits to collect civil penalties for export violations, at which point the denial could be reviewed. Export Control Act of 1965, Pub. L. No. 89-63, § 2, 79 Stat. 209, 209-10 (1965); https://www.congress.gov/89/statute/STATUTE-79/STATUTE-79-Pg209.pdf.

formal administrative proceedings.[32] Appeals of license denials, however, are handled by BIS itself through the Under Secretary for Industry and Security.[33] When issuing licenses, BIS must now "provide for the assessment of the impact of a proposed export of an item on the United States defense industrial base."[34] Applications that "would have a significant negative impact" must be denied.[35] Furthermore, the Departments of State, Defense, and Energy receive and review the majority of license applications to BIS.[36] Outside of these interagency collaborative benchmarks, however, BIS retains substantial enforcement discretion.

The ECRA also expanded BIS's enforcement power in significant ways. BIS may issue orders and guidelines, inspect books and records, issue subpoenas, conduct domestic and international investigations, perform pre-license inspections and post-shipment verifications, execute warrants, and make arrests.[37] Now, BIS may run undercover operations and fund them by a host of newly authorized activities.[38] BIS can also deny export privileges to anyone convicted of conspiracy, smuggling, espionage, disclosing classified information, or making false statements.[39] The ECRA increased civil penalties, stipulating that they not exceed $300,000 or an amount that is twice the value of the transaction in question, whichever is greater.[40]

## D. Semiconductor export controls against China and Russia have been ineffective

BIS has issued a host of semiconductor export control restrictions over the last four years meant to cripple Russia's war effort and constrain China's technological advances. As to Russia, BIS has (1) added thousands of entities believed to provide U.S. semiconductors to Russia to the Entity List—a list maintained by BIS to identify "persons reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States"—(2) issued two FDPRs meant to restrict the ability of Russia and Belarus to acquire certain items, and (3) provided companies with a variety of guidance meant to provide red flags pointing to possible risks of Russian diversion in transactions.[41] As to

[32] 50 U.S.C. § 4819(c)(2).

[33] 15 CFR § 756.2. A challenge to a denial of such an appeal would likely be subject to ultra vires review. *See* Changji Esquel v. Raimondo, 40 F.4th 716 (D.C. Cir. 2022).

[34] 50 U.S.C. § 4815(d)(1).

[35] 50 U.S.C. § 4815(d)(1).

[36] Exec. Order No. 12981, Administration of Export Controls, 60 Fed. Reg. 62,981 (Dec. 5, 1995). A three-level interagency process exists to resolve agency disputes. *Id.*

[37] 50 U.S.C. § 4820(a).

[38] 50 U.S.C. § 4820(b).

[39] 50 U.S.C. § 4819(e).

[40] 50 U.S.C. § 4819(c).

[41] *See, e.g.*, Press Release, Bureau of Indus. and Sec., Commerce Tightens Export Controls, Targets Illicit Procurement Networks For Supplying Russian War Machine (Aug. 23, 2024), https://www.bis.gov/press-

China, semiconductor export controls have included (among others) the FDPR issued against Huawei in 2020, the October 2022 FDPR meant to restrict the production of semiconductors and advanced computing items with A.I. applications in China, and an additional round of restrictions on advanced chip technology announced just this month.[42]

These export controls have been ineffective at constraining the Russian war effort. As detailed in the Subcommittee's September 10, 2024 report, while export controls initially hampered Russia's ability to acquire the most critical battlefield goods, reporting from KSE Institute showed that imports of battlefield goods to Russia largely rebounded to their pre-war numbers by the end of 2023.[43] Reporting from KSE Institute and other entities focused on tracking and tracing the flow of U.S.-manufactured semiconductors to Russia has consistently found that Russia's continued success in acquiring necessary goods lies in the use of entities located in third-party countries who

release/commerce-tightens-export-controls-targets-illicit-procurement-networks-supplying; 15 CFR § 744.16; Press Release, Bureau of Indus. and Sec., U.S. Department of Commerce & Bureau of Industry and Security Russia and Belarus Fact Sheet (Feb. 22, 2022), https://www.commerce.gov/news/fact-sheets/2022/02/us-department-commerce-bureau-industry-and-security-russia-and-belarus. In February 2023, after the discovery of Iranian made UAVs deployed by Russia in Ukraine, BIS simultaneously added the Iran FDPR, 15 CFR § 734.9(j), subjecting a category of EAR99 items destined to Iran to licensing requirements, and amended the Russia/Belarus FDPR to reference those EAR99 items. Export Control Measures Under the Export Administration Regulations (EAR) To Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine, 88 Fed. Reg. 12,150 (Feb. 24, 2023) (codified at 15 CFR § 734, 15 CFR § 746), https://www.federalregister.gov/documents/2023/02/27/2023-03930/export-control-measures-under-the-export-administration-regulations-ear-to-address-iranian-unmanned; FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT ALERT: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY URGE INCREASED VIGILANCE FOR POTENTIAL RUSSIAN AND BELARUSIAN EXPORT CONTROL EVASION ATTEMPTS (2022), https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT ALERT: SUPPLEMENTAL ALERT: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY URGE CONTINUED VIGILANCE FOR POTENTIAL RUSSIAN EXPORT CONTROL EVASION ATTEMPTS (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT NOTICE: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY ANNOUNCE NEW REPORTING KEY TERM AND HIGHLIGHT RED FLAGS RELATING TO GLOBAL EVASION OF U.S. EXPORT CONTROLS (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf; BUREAU OF INDUS. AND SEC., GUIDANCE TO INDUSTRY ON BIS ACTIONS IDENTIFYING TRANSACTION PARTIES OF DIVERSION RISK (2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

[42] Addition of Huawei Non-U.S. Affiliates to the Entity List, *supra* note 12; Palmer, *supra* note 16; Press Release, Bureau of Indus. and Sec., Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications (Dec. 2, 2024), https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced.

[43] PSI September 2024 Report, *supra* note 1 (citing OLENA BILOUSOVA ET AL., KSE INST., RUSSIA'S MILITARY CAPACITY AND THE ROLE OF IMPORTED COMPONENTS (2023)), https://kse.ua/wp-content/uploads/2023/06/Russian-import-of-critical-components.pdf; OLENA BILOUSOVA ET AL., KSE INST., CHALLENGES OF EXPORT CONTROLS ENFORCEMENT: HOW RUSSIA CONTINUES TO IMPORT COMPONENTS FOR ITS MILITARY PRODUCTION (2024), https://kse.ua/wpcontent/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf; and ATLANTIC COUNCIL *Russian Sanctions Database*, (Nov. 1, 2023), https://www.atlanticcouncil.org/blogs/econographics/russia-sanctions-database-november-2023).

then ship those goods onto Russia, a process referred to as transshipment.[44] Hong Kong, China, Turkey, the United Arab Emirates, Kazakhstan, Armenia, Belarus, Finland, Georgia, Kyrgyzstan, and Uzbekistan have been identified as countries with entities that are being used for transshipment.[45] Consistent with this reporting, the Subcommittee's inquiry revealed that there have been substantial increases in exports of semiconductors from the Analog Devices, Intel, Texas Instruments, and AMD to countries known to have entities engaged in transshipment to Russia since the start of Russia's war in Ukraine.[46]

Public reporting has also highlighted that China has exploited significant gaps in export controls to continue to acquire U.S. technology. A recently completed investigative report by the *New York Times* revealed that Chinese companies have found straightforward workarounds to the U.S. government's restrictions, that many American companies have actively looked for workarounds to keep selling their products to China, and that, in addition, "an underground marketplace of smugglers, backroom deals, and fraudulent shipping labels is funneling A.I. chips into China."[47] As a result of these evasive efforts, prohibited chips are widely available in China.[48]

---

[44] *See, e.g.*, James Byrne et al., ROYAL UNITED SERVS. INST., SILICON LIFELINE: WESTERN ELECTRONICS AT THE HEART OF RUSSIA'S WAR MACHINE, (2022), https://rusi.org/explore-our-research/publications/specialresources/silicon-lifeline-western-electronics-heart-russias-war-machine; CONFLICT ARMAMENT RSCH. IDENTIFYING POST-INVASION COMPONENTS IN RUSSIAN WEAPONS, ( Emily Youers ed., 2023), https://storymaps.arcgis.com/stories/00594bef40bc4148b16dc7267172d033; Olena Bilousova et al., *Russia's Military Capacity and the Role of Imported Components*, KSE INST. (June 2023), https://kse.ua/wp-content/uploads/2023/06/Russian-import-of-critical-components.pdf; James Byrne et al., *In Plain Sight: Operations of a Russian Microelectronics Dynasty*, ROYAL UNITED SERVS. INST. (DEC. 2023), https://rusi.org/explore-our-research/publications/commentary/report-plain-sightoperations-russian-microelectronics-dynasty; Olena Bilousova et al., *Challenges of Export Controls Enforcement: How Russia Continues to Import Components for its Military Production*, KSE INST. (Jan. 2024), https://kse.ua/wpcontent/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf.

[45] *Supra* note 44.

[46] PSI September 2024 Report, *supra* note 1.

[47] Ana Swanson & Claire Fu, *With Smugglers and Front Companies, China is Skirting American A.I. Bans*, N.Y. TIMES (Aug. 4, 2024), https://www.nytimes.com/2024/08/04/technology/china-ai-microchips.html.

[48] *Id*.

# Part II: Findings

## A. Congress has not provided BIS with adequate funding to fulfill its mission.

BIS's budget for core export control functions has remained essentially flat since 2010 when adjusted for inflation.[49] At the same time, U.S. exports have increased drastically: going from 1,278,493 million in 2010 to 2,018,059 million in 2023, a 58% increase.[50] This has correspondingly increased BIS's workload, with exports subject to BIS license requirements increasing approximately 126 percent since 2014, and BIS's licensing workload doubling from approximately 20,000 licenses per year in 2012 to over 40,000 per year in 2023.[51]

In addition to a drastically larger workload due to increases in exports, BIS's national security responsibilities have significantly increased since 2010. As explained above, this is due to the increasing use of FDPRs and similar export control tools to constrain the military efforts of major adversaries such as China and Russia.[52] Yet, despite its increasing role in the national security apparatus, BIS's budget pales in comparison to other national security spending: Its budget of $191 million is less than the cost of two fighter jets.[53]

The Subcommittee's inquiry found that BIS's current budget is insufficient given its increased workload and significantly enlarged national security responsibilities. The inadequacy of BIS's budget can be seen in two critical places: (1) BIS's limited funds reduce its ability to perform international end-use checks; and (2) BIS has been hindered by outdated information technology systems that cannot synthesize the vast array of data it has at its disposal to identify Russian and Chinese diversion efforts.

### i. BIS's budget limits its ability to conduct the number of international end-use checks needed to catch Russian and Chinese diversion.

BIS's current budget restricts the number of international end-use checks BIS can undertake. An end-use check requires BIS officials overseas to conduct physical verification at distributors or companies that are the intended end users of products regulated by the EAR.[54] These checks are completed in-person by BIS enforcement personnel, typically Export Control Officers

[49] Letter from Bureau of Indus. and Sec., to the Hon. Richard Blumenthal, Chairman, Permanent Subcomm. on Investigations (May 1, 2024) (on file with the Subcommittee) [hereinafter BIS May 1 Letter].

[50] U.S. CENSUS BUREAU, *Trade in Goods with World, Seasonally Adjusted*, https://www.census.gov/foreign-trade/balance/c0004.html (last access Dec. 5, 2024).

[51] BIS May 1 Letter, *supra* note 49.

[52] *See supra* Section I.B.

[53] Swanson & Fu, *supra* note 47.

[54] Kevin Kurland, Deputy Assistant Sec'y. for Export Enf't, Briefing with Senate Permanent Subcomm. on Investigations Staff (June 13, 2024) [hereinafter Kurland June 2024 Briefing].

(ECOs).[55] BIS has one analyst in Canada and 11 ECOs in 9 countries around the world: (1) Germany, (2) United Arab Emirates, (3) Finland, (4) Taiwan, (5) Turkey, (6) Singapore, (7) Hong Kong, (8) China, and (9) India.[56] Each ECO carries out export control checks in their assigned country and area of responsibility (AOR).[57] An AOR covers only the geographic area surrounding an ECO's location, meaning some countries fall outside of any ECO's AOR.[58] In such cases, BIS conducts end-use checks through a Sentinel team—two BIS agents who travel to the country and perform expedited checks, usually 25-30 in a week.[59]

End-use checks are an incredibly important tool for BIS as it works to enforce U.S. export controls.[60] In an end-use check, BIS officials verify the bona fides of the party, whether the party has received the item it ordered, and, if it has, whether the item was consumed or reexported.[61] BIS officials then evaluate this information and place the party into one of three buckets: unverified, favorable, or unfavorable.[62] "Unfavorable" means BIS has identified a violation, or that the company has provided false information.[63] "Unverified" means BIS could not confirm whether a violation occurred.[64] For instance, BIS may not have been able to find or contact the company or could not verify the disposition of items subject to the EAR.[65] A "favorable" determination indicates that no violations have been detected.[66] On average, about 25% of checks are unfavorable or unverified, and the remainder are favorable.[67]

Depending on the circumstances, an "unfavorable" end-use check can result in several possible outcomes. First, BIS will add the party's license application to a watch list.[68] BIS enforcement personnel do not have the resources to conduct a detailed review of every license

[55] *Id*.

[56] *Id*.

[57] *Id*.

[58] *Id*.

[59] *Id*.

[60] *See e.g.*, James E. Bartlett III & Jonathan C. Poling, *Defending the Higher Walls - The Effects of U.S. Export Control Reform on Export Enforcement*, 14 SANTA CLARA J. INT'L L. 1 (2016) (noting the importance of reviews by Office of Export Enforcement agents).

[61] Kurland June 2024 Briefing, *supra* note 54.

[62] *Id*.

[63] *Id*.

[64] *Id*.

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] *Id*.

application, and the watch list helps prioritize applications for more in-depth analysis.[69] BIS's subsequent research could prompt it to deny the license application and/or add the company to the Unverified List (a list of parties whose bona fides BIS has been unable to verify)[70] or the Entity List.[71] BIS will also dispatch agents from the nearest field office to visit the company and establish what it knew about the party in violation.[72] A knowing violation can trigger stricter penalties, including fines as provided in the EAR.[73] Even if the exporter unwittingly violated the EAR, BIS would attempt to "knowledge them up" regarding the violation and indicate that it expected the company to be more diligent going forward.[74]

[69] *Id*.

[70] BUREAU OF INDUS. AND SEC., *Lists of Parties of Concern*, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern (last accessed Dec. 16, 2024).

[71] Kurland June 2024 Briefing, *supra* note 54.

[72] *Id*.

[73] *Id*. Knowledge is not required for the imposition of fines, as BIS can take administrative enforcement action on a strict liability basis. *See* 15 C.F.R. 764.2(a). However, BIS explained to the Subcommittee that a knowing violation would likely lead to higher penalties (including larger fines) than a strict liability violation. Attachment to Email from Bureau of Indus. and Sec. to Permanent. Subcomm. on Investigations Staff (Dec. 10, 2024) (on file with the Subcommittee) [hereinafter BIS December Email Attachment].

[74] Kurland June 2024 Briefing, *supra* note 54.

BIS's current resources severely limit the number and frequency of end-use checks related to Russia diversion concerns. BIS conducted 1,304 end-use checks related to Russia diversion in fiscal year 2022 and 2023 in the following countries:

**Figure 1: Fiscal Year 2022 and 2023 BIS Russia Diversion End-Use Checks**[75]

| Country | End-Use Checks |
|---|---|
| Armenia | 5 |
| Bahrain | 2 |
| Brazil | 12 |
| Bulgaria | 7 |
| Canada | 106 |
| China | 68 |
| Colombia | 13 |
| Costa Rica | 4 |
| Croztia | 13 |
| Czech Republic | 5 |
| Estonia | 16 |
| Finland | 165 |
| France | 13 |
| Germany | 16 |
| Honduras | 19 |
| Hungary | 10 |
| India | 25 |
| Israel | 13 |
| Italy | 5 |
| Jamaica | 7 |
| Japan | 79 |
| Kazakhstan | 51 |
| Kyrgyzstan | 54 |
| Latvia | 12 |
| Lithuania | 10 |
| Malaysia | 1 |
| Maldives | 31 |
| Mexico | 33 |
| Morocco | 12 |
| Netherlands | 3 |
| Pakistan | 14 |
| Philippines | 5 |
| Poland | 133 |
| Serbia | 12 |
| Singapore | 9 |
| Slovakia | 14 |
| South Africa | 5 |
| South Korea | 53 |
| Spain | 1 |
| Sweden | 5 |
| Taiwan | 94 |
| Thailand | 2 |
| Turkey | 64 |
| UAE | 45 |
| United Kingdom | 5 |
| Uzbekistan | 21 |
| Vietnam | 1 |
| Zambia | 11 |
| Total | 1,304 |

The Subcommittee's previous work demonstrates that the current end-use checks are insufficient. Specifically, the Subcommittee's September 10, 2024 report found that aggregated exports from Analog Devices, AMD, Intel, and Texas Instruments nearly doubled from 2021 to 2022 to Armenia and Georgia—countries which public reporting had identified as having entities known to assist Russia in acquiring U.S. semiconductors despite export controls.[76] Exports to Armenia were still nearly 12 times greater in 2023 than they were in 2021.[77] Yet Figure 1 demonstrates that BIS could only conduct 5 end-use checks in Armenia in Fiscal Year 2022 and 2023, and none in Georgia.

[75] BIS May 1 Letter, *supra* note 49.

[76] PSI September 2024 Report, *supra* note 1.

[77] *Id*.

Resource issues also constrain BIS's review of Chinese diversion efforts through end-use checks. The House Foreign Affairs Committee released a 90-day review report of BIS in January 2024 which noted the resource issue in the context of China, highlighting specifically that BIS has "a severe lack of subject matter experts and linguists focused on the PRC."[78] According to the Committee's report, this included the fact that a former BIS official informed the Committee's majority staff that "the bureau had one employee proficient in Mandarin during their tenure."[79]

BIS officials acknowledged to the Subcommittee that they could and would conduct significantly more checks if they had the resources to hire additional international ECOs.[80] Reports suggest that entities in countries outside ECO AORs have been diverting sanctioned products to Russia and China.[81] BIS can only detect those shipments through the Sentinel program described above, in which BIS agents travel to the country and perform expedited checks.[82] However, the Sentinel program has no line item in the agency's budget.[83] Instead, BIS must carve funds from its existing allotments and deploy teams selectively based on available resources.[84]

As a result, BIS can only conduct end-use checks in a country outside ECO AORs every two to three years.[85] The recent Ukraine supplemental afforded BIS some latitude to increase Sentinel checks in countries prone to Russian diversion, but the frequency could still improve with better funding.[86] These resources also have not (and cannot) go to increases needed to combat China's efforts.[87] Additional assets would allow BIS to (1) hire more international ECOs and place them in more countries, expanding the regions covered by an ECO's AOR and (2) conduct more frequent Sentinel checks in any country that remained outside of an ECO's AOR.

---

[78] H. FOREIGN AFFAIRS COMMITTEE, 118TH CONG., BUREAU OF INDUSTRY AND SECURITY: 90-DAY REVIEW REPORT 39 (2024), https://foreignaffairs.house.gov/wp-content/uploads/2024/01/1.2.24-BIS-Report.pdf [hereinafter House BIS Report].

[79] *Id*.

[80] Kurland June 2024 Briefing, *supra* note 54.

[81] Georgi Kantchev, Paul Hannon & Laurence Norman, *How Sanctioned Western Goods Are Still Flowing Into Russia*, WALL ST. J. (May 14, 2023), https://www.wsj.com/articles/how-sanctioned-western-goods-are-still-flowing-into-russia-916db262;

[82] Kurland June 2024 Briefing, *supra* note 54. BIS noted to the Subcommittee that 20% of the end use checks targeting Russia in Figure 1 were due to the Sentinel program, and that 9 of the 48 countries where checks were conducted fell outside of an export control officers' AOR. BIS December Email Attachment, *supra* note 73.

[83] Kurland June 2024 Briefing, *supra* note 54.

[84] *Id*.

[85] *Id*.

[86] *Id*.

[87] House BIS Report, *supra* note 78.

### ii. BIS's limited budget inhibits its ability to update its woefully outdated information technology systems.

Years of inadequate funding, minimal upgrades, and increasing obligations have exacerbated the flaws in BIS's aging information technology systems. In November 2022, the Center for Strategic & International Studies (CSIS) released a report outlining significant deficiencies in BIS's then-current information technology.[88] Current and former BIS officials, other government employees, industry executives, and technology experts all emphasized to CSIS the abysmal state of BIS's technology infrastructure.[89]

CSIS's 2022 report highlighted a number of significant flaws with BIS's information technology, which CSIS concluded significantly hampered BIS in effectively implementing and enforcing export controls. BIS reviews tremendous volumes of data from three main sources to perform its functions: internal Commerce Department data, data shared from other government agencies, and open-source data.[90] However, CSIS found that BIS's technology created obstacles in each of those key sectors.[91] BIS could not reliably search its own data, government agencies struggled to share information with it, and its tools to process open-source data were remedial.[92] Instead of more advanced technology, like knowledge graph databases or machine learning, BIS analysts were relying on Google searches and an old version of Microsoft Excel to perform the bulk of their work.[93] As a result, BIS personnel estimated to CSIS that they spent roughly 80% of their time looking for relevant data, and just 20% analyzing it.[94]

The Subcommittee requested a briefing and in-person demonstration of BIS's current information technology systems to understand if the problems CSIS identified in 2022 were still present. This review confirmed that all of the problems identified by CSIS still existed, and identified additional, specific issues with BIS's information technology.

BIS's core IT systems were originally created in 2006 and have not changed or been updated much since then, such that there have been no improvements to the issues CSIS identified.[95] BIS explained that although patchwork fixes over the years have kept its systems running, its IT remains

---

[88] GREGORY C. ALLEN, EMILY BENSON & WILLIAM ALAN REINSCH, CTR. FOR STRATEGIC AND INT'L STUDIES, IMPROVED EXPORT CONTROLS ENFORCEMENT TECHNOLOGY NEEDED FOR U.S. NATIONAL SECURITY (2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221130_Allen_Export_Controls.pdf?VersionId=xmB4Pqusa5lsBnQzNBh1RqebwJKcQvmr.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (Aug. 16, 2024) [hereinafter BIS August 2024 Briefing]; Permanent Subcomm. on Investigations Staff Review of Bureau of Indus. and Sec. Information Technology Systems (Aug. 16, 2024) [hereinafter PSI August 2024 BIS IT Review].

significantly outdated.[96] This is particularly glaring when compared to the modern systems available in the private sector, but BIS's IT even lags significantly behind that of other, similar government agencies.[97]

The Subcommittee's review of BIS's information technology systems identified additional, specific deficiencies beyond simply the outdated nature of the technology. The first IT system that causes significant problems is BIS's CUESS-Licensing Officer Application system (LOA). Licensing officers and export analysts use LOA to review export applications, search for entities or previously granted licenses, and manage interagency referrals.[98] Officers have no way to sort cases in the database: the oldest cases always appear first.[99] The system has sparse notifications, so officers are not informed when another office transfers a case to BIS, when officers disagree about whether to elevate a case for further review, or when any other case action occurs.[100] The system does not have the capacity to generate updated case indicators, so licensing officers cannot designate cases as Russian sanctions related.[101]

LOA's search functions are also cumbersome and counterintuitive.[102] The system only allows personnel to search for one entity at a time, and some search fields require an exact match—meaning even a misplaced period, such as searching for Inc. rather than Incorporated, could fail to find a hit for an entity already located in the database.[103] Results are inconsistent, and relevant data is often excluded.[104] The system often fails to fully export search results to Excel, further limiting the data's accessibility.[105] To form a complete data set for a given query, multiple analysts run overlapping searches, export the fragmented data to Excel, then combine their respective spreadsheets and compare the results to try to arrive at a complete search.[106]

Similar issues plague BIS's Investigative Management system (IMS-R). The IMS-R is a file association system housing digital case files, links to witness information, documents uploaded to support investigations, resources, and records of actions like arrests.[107] BIS law enforcement personnel use IMS-R to follow up on leads, manage entity investigations, and conduct additional

---

[96] BIS August 2024 Briefing, *supra* note 95.

[97] ALLEN, BENSON & REINSCH, *supra* note 88.

[98] PSI August 2024 BIS IT Review, *supra* note 95.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] BIS August 2024 Briefing, *supra* note 95.

screening.[108] Navigating the system can be challenging. It has no advanced search functions or standardized document naming convention.[109] The search feature cannot locate text contained within a document: each file must be opened manually.[110] Document uploads must be completed individually because there are no batch upload options.[111] The system does not support popular document types like Excel files and PDF portfolios.[112] Officers spend significant time converting documents to acceptable formats for upload.[113]

The Subcommittee's review indicates that BIS needs to bring in additional IT staff and modernize its technology to adequately update its systems and processes.[114] Agency officials told PSI they estimated that these changes would require $25 million annually over four years, or a one-time increase of $100 million.[115]

## B. BIS has failed to fully use its existing authority to enforce export controls.

Congress has given BIS broad discretion in export control implementation and enforcement. The EAR and the ECRA provide BIS wide latitude to implement export control policy as it sees fit, without many of the constraints that other agencies commonly encounter. In briefings with the Subcommittee, BIS officials repeatedly acknowledged the broad scope and reach of their authority.[116] This reality was acknowledged in briefings both with BIS officials who deal with policy and those who focus on enforcement.[117]

But BIS has not adequately used the scope of its broad authority to implement and enforce

---

[108] PSI August 2024 BIS IT Review, *supra* note 95.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] BIS August 2024 Briefing, *supra* note 95.

[114] In addition to the Subcommittee's findings based on its review of BIS's IT systems, both current and former officials at the Department of Commerce have publicly reiterated the need for additional funds for BIS. *See, e.g.*, Ana Swanson, *Lawmakers Press Biden Administration for Tougher Curbs on China Tech*, N.Y. TIMES (Dec. 7, 2023) (quoting Commerce Secretary Raimondo asking that Congress fund BIS "like it needs to be funded so we can do what we need to do to protect America"), https://www.nytimes.com/2023/12/07/us/politics/lawmakers-biden-china-tech.html; *Reviewing the Bureau of Industry and Security, Part I: U.S. Export Controls in an Era of Strategic Competition*: *Hearing before the H. Foreign Affairs Subcomm. on Oversight and Accountability*, 118th Cong. (2023) (Statement of Kevin Wolf, Former Assistant Sec'y of Com. for Export Admin., highlighting the need for significant resource investment in BIS information technology, particularly to permit the use of commercially available datasets), https://foreignaffairs.house.gov/hearing/reviewing-the-bureau-of-industry-and-security-part-i-u-s-export-controls-in-an-era-of-strategic-competition/.

[115] BIS August 2024 Briefing, *supra* note 95.

[116] Kurland June 2024 Briefing, *supra* note 54; Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (July 18, 2024) [hereinafter BIS July 18 Briefing].

[117] *Supra* note 116.

semiconductor export controls. This failure can be seen in at least three ways: (1) BIS has relied on semiconductor companies to develop their own export control programs rather than requiring that companies include any specific components in their export control programs; (2) BIS has not used its full authority to prosecute "knowing" violations of the EAR; and (3) BIS has not to date increased fines for export control violations, despite publicly acknowledging that higher penalties are necessary to compel more proactive compliance.

### i. BIS does not require that semiconductor companies' export control programs contain any specific components, or that companies' export control programs undergo outside review.

BIS has full authority through the EAR and ECRA to compel semiconductor manufacturers and other exporters of U.S. semiconductors (such as distributors) to include specific elements in their export control compliance programs, or to require that such entities permit BIS to review their export programs on a regular basis—it has simply chosen not to do so.[118] Instead, BIS offers best practices for export controls on its website in a manual entitled *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program* and offers to review companies export control programs on a voluntary basis and provide nonbinding suggestions for improvement.[119] BIS explained to the Subcommittee that the preference for allowing companies to develop their own compliance programs stems from a historical trend of not relying on legal requirements but instead working with companies so that they understand the outcome BIS needs and can adopt the best practice to get there.[120] BIS told the Subcommittee that it believes voluntary adoption and cooperation works better than formulating a regulation to determine how to craft a rule to get at, for example, differences in the business considerations of manufacturers vs distributors.[121]

The Subcommittee's inquiry has demonstrated multiple ways in which this preference for voluntary cooperation is leading to inadequate export controls in the semiconductor industry. The Subcommittee's inquiry revealed that (as of September 10, 2024) Analog Devices, Intel, Texas Instruments, and AMD each lacked an export control compliance program which complied fully with BIS best practices.[122] BIS had not reviewed any of these four companies' export control compliance programs in the over two years since Russia's invasion of Ukraine, and the Subcommittee obtained

---

[118] *See supra* Section I.C. BIS officials acknowledged this to Subcommittee staff in two separate briefings during the course of the Subcommittee's inquiry on June 13, 2024 and July 18, 2024, explaining their understanding that the EAR and ECRA are broad grants of authority and that there is no legal or legislative constraint which compels them to rely on companies' voluntary cooperation rather than compelling compliance.

[119] *See* BUREAU OF INDUS. AND SEC., EXPORT COMPLIANCE GUIDELINES: ELEMENTS OF AN EFFECTIVE EXPORT COMPLIANCE PROGRAM (2017), https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file; Bureau of Indus. and Sec., *How Can You Create an Effective Export Compliance Program?,* https://www.bis.gov/articles/how-can-you-create-effective-export-compliance-program (last accessed Dec. 16, 2024).

[120] BIS July 18 Briefing, *supra* note 116.

[121] *Id*.

[122] PSI September 2024 Report, *supra* note 1.

information demonstrating that BIS had reviewed hardly any semiconductor companies export control compliance program in that timeframe.[123] Specifically, information obtained by the Subcommittee shows that, from fiscal year 2022 to May 2024, BIS only reviewed 4 export control plans for semiconductor-related companies.[124]

Further, BIS expressed concern to the Subcommittee that the Subcommittee requesting information and records regarding export controls from Analog Devices, Intel, Texas Instruments, and AMD may chill these four companies' voluntary cooperation with BIS.[125] BIS explained to the Subcommittee that BIS itself did not have any concerns regarding the Subcommittee's review of the requested information, but that the Subcommittee's request for and review of certain information regarding BIS's interactions with the companies may chill the companies' ongoing voluntary cooperation with BIS regarding export controls.[126] The Subcommittee strongly objected to limiting its requests in the manner suggested by BIS and did not do so.

### ii. BIS has not adequately charged companies for "knowing" violations of the EAR.

Under the EAR, BIS may impose more significant penalties for "knowing" violations.[127] The regulation defines "knowing" as:

> Knowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe") includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. This definition does not apply to part 760 of the EAR (Restrictive Trade Practices or Boycotts).[128]

BIS officials acknowledged in briefings to Subcommittee staff that this regulation gives BIS the authority to bring enforcement actions for "knowing" violations where the conduct by the company

---

[123] *Id*.

[124] Letter from Bureau of Indus. and Sec., to the Hon. Richard Blumenthal, Chairman, Permanent Subcomm. on Investigations (July 3, 2024) (on file with the Subcommittee) [hereinafter July 3 BIS Letter].

[125] Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (May 28, 2024); Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (June 7, 2024); Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (July 10, 2024) [hereinafter BIS July 10 Briefing]; BIS July 18 Briefing, *supra* note 116.

[126] BIS July 10 Briefing, *supra* note 125; BIS July 18 Briefing, *supra* note 116.

[127] BIS may also take enforcement action on a strict liability basis. *See* 15 C.F.R. 764.2(a). However, BIS explained to the Subcommittee that a knowing violation would likely lead to higher penalties (including larger fines) than a strict liability violation. BIS December Email Attachment, *supra* note 73. A "knowing" violation may also lead to criminal action under the ECRA. *Id*.

[128] 15 C.F.R. § 772.1.

in question evidenced "an awareness of a high probability of [the] existence or future occurrence" of a violation of the EAR, rather than positive knowledge of a violation.[129] Commentators have noted that such conduct might occur where, for example, a semiconductor company conducts no additional due diligence on a transaction despite indicators from BIS that the transaction presents red flags suggesting a risk of Russian or Chinese diversion, enters into the transaction, and the transaction results in the diversion of the semiconductor company's products to Russia or China.[130]

Despite possessing this authority, BIS acknowledged to the Subcommittee that it has never brought an enforcement action for a "knowing" violation based on "an awareness of a high probability of [the] existence or future occurrence" of a violation.[131]

### iii. BIS has acknowledged the need for larger fines for violations of the EAR but has not yet imposed them.

BIS and other government officials have publicly acknowledged the need for larger fines to incentivize robust, proactive corporate compliance with export controls. In January 2024, Assistant Secretary for Export Enforcement Matthew S. Axelrod announced enhancements to BIS's voluntary self-disclosure program, publicly explaining that this was meant to "clear out the underbrush of lower level administrative cases" in order for BIS "to focus more of our time and attention on the bigger ticket items on which we're now going to be imposing higher penalties."[132] Assistant Secretary Axelrod explained that such penalties were needed to "get everyone's attention" and echoed comments Deputy Attorney General Lisa Monaco made in 2023 about export controls as the new Foreign Corrupt Practices Act (FCPA), explaining that companies should be "thinking about their national security risk the way they think about this FCPA risk."[133]

---

[129] Kurland June 2024 Briefing, *supra* note 54.

[130] Brent Carlson & Michael Huneke, *How Not to Stand Out Like a Sore Thumb (Part 2): A Fresh Look at the "High Probability" Definition of Knowledge Applied to Export Controls and Sanctions Enforcement*, N.Y.U. PROGRAM ON CORP. COMPLIANCE AND ENF'T., https://wp.nyu.edu/compliance_enforcement/2024/02/21/how-not-to-stand-out-like-a-sore-thumb-part-2-a-fresh-look-at-the-high-probability-definition-of-knowledge-applied-to-export-controls-and-sanctions-enforcement/ (last visited Dec. 16, 2024).

[131] Bureau of Indus. and Sec. Officials, Briefing with Permanent Subcomm. on Investigations Staff (March 11, 2024); *Improving Export Controls Enforcement, Hearing Before the Subcomm. on Emerging Threats and Spending Oversight, S. Comm. on Homeland Security and Governmental Affairs*, 118th Cong. (April 10, 2024) (responses to questions for the record from Kevin J. Kurland, Deputy Assistant Secretary of Commerce for Export Enforcement) (on file with the Subcommittee).

[132] Karen Freifeld, *Higher penalties coming for export control violations – US Commerce Official*, REUTERS (Jan. 17, 2024), https://www.reuters.com/markets/us/higher-penalties-coming-export-control-violations-us-commerce-official-2024-01-17/.

[133] *Id*.

BIS officials reiterated to the Subcommittee in briefing that more significant penalties for export violations were needed, are in process, and would be forthcoming.[134] However, the BIS officials who spoke with the Subcommittee could not place firm timetables on the imposition and announcement of any larger fines, instead simply stating that enforcement actions take time.[135] No such fines have been announced in the 11 months since Assistant Secretary Axelrod emphasized their necessity and noted that BIS was on the "cusp" of publicly announcing them.[136]

[134] Kurland June 2024 Briefing, *supra* note 54.

[135] *Id*.

[136] Freifeld, *supra* note 132.

# PART III: RECOMMENDATIONS

## A. Congress should provide BIS with adequate funding to manage its increased workload and responsibilities.

BIS has taken on a dramatically larger workload and significantly greater national security responsibilities over the last 15 years with essentially no change in its enforcement budget. As detailed above, these funding decisions have left BIS unable to provide international end-use checks in all the countries it needs to in order to combat Russian and Chinese diversion. This includes insufficient end-use checks in countries which (1) the Subcommittee identified in September 10, 2024 report as having substantial increases in imports of semiconductors and (2) have been publicly reported to have entities engaged in transshipment to Russia.

Budget issues have also left BIS's information technology woefully lagging and insufficient for it to meet its mission. The technology deficit is a particularly acute issue given the massive amount of data available regarding Russian and Chinese diversion and the ability of modern analytics programs to quickly synthesize data and highlight connections among seemingly unrelated entities.

BIS has provided the Subcommittee with its proposal outlining the funding needed to meet its enforcement mission. This proposal calls for approximately $75 million in additional annual funding, along with a one-time increase of $100 million to immediately address information technology issues.[137] BIS explained to the Subcommittee that these additional funds would permit BIS to (1) hire sufficient enforcement, policy, and technological personnel to increase its enforcement efforts, and (2) build a modern data integration program to help it efficiently further its mission.[138] Given the increasing importance of BIS's export enforcement mission in the U.S. national security landscape, this seems like a relatively modest sum which Congress should provide to BIS.

## B. BIS should utilize its robust authority to require more of semiconductor manufacturers.

Although Congress has provided BIS a robust grant of authority to implement and enforce export controls, BIS is not using all the authority it has been given to ensure that U.S. semiconductor companies are complying fully with the letter and spirit of U.S. export controls. There are a number of steps BIS could take with its existing authority to improve semiconductor companies' compliance.

---

[137] PowerPoint, Bureau of Indus. and Sec., BIS Overview and Needs for House and Senate Members/Staff (2024) (on file with the Subcommittee); BIS August 2024 Briefing, *supra* note 95.

[138] *Supra* note 137.

### i. BIS should accelerate plans to impose higher fines on companies who violate export controls.

As noted above, BIS officials have publicly acknowledged the need for larger fines for export control violations in order to compel companies to be more proactive regarding export controls compliance.[139] Assistant Secretary Axelrod did so in January of this year and stated then that BIS was on the "cusp" of publicly announcing such fines.[140] Other BIS officials similarly told the Subcommittee that such fines are in the works, but could not provide any concrete timeline for their finalization and announcement.[141]

Assistant Secretary Axelrod explained that such fines are needed as a step towards compelling companies to think of export controls as the "new FCPA," and the FCPA is a good analog for the utility and necessity of robust, public fines.[142] In 2008, the Department of Justice announced a settlement of a wide-ranging FCPA investigation into Siemens AG which included a combined $800 million in fines from DOJ and the Securities and Exchange Commission, along with additional fines from German regulators—making Siemens total penalties for its violations $1.6 billion.[143] Before then, the largest U.S. monetary sanction in an FCPA case had been $44 million.[144] As Assistant Secretary Axelrod acknowledged, "Siemens got everyone's attention on the FCPA."[145] The settlement led practitioners to note the need for companies to have vigorous internal controls and also highlighted the importance the government placed on voluntary cooperation, causing many companies to invest in robust FCPA controls.[146]

Similar fines for export control violations would likely yield similar results, but the fines need to be finalized and announced rather than just publicly hinted at. While the Subcommittee is

---

[139] *See supra* Section II.B.iii.

[140] Freifeld, *supra* note 132.

[141] Kurland June 2024 Briefing, *supra* note 54.

[142] Freifeld, *supra* note 132.

[143] Dep. of Just., Press Release, Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations and Agree to Pay $450 Million in Combined Criminal Fines (Dec. 15, 2008) https://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html.

[144] WILMERHALE, *Siemens Agrees to Record-Setting $800 Million in FCPA Penalties*, (Dec. 22, 2008), https://www.wilmerhale.com/insights/publications/siemens-agrees-to-record-setting-800-million-in-fcpa-penalties-december-22-2008.

[145] Freifeld, *supra* note 132; *see also, e.g.*, CLAUDIUS O. SOKENU & TIFFANY A. ARCHER, ARNOLD & PORTER, ALARMING LESSONS FROM SIEMENS: THE US IS AGGRESSIVELY PURSUING CORRUPTION, EVERYWHERE (2009), https://www.arnoldporter.com/-/media/files/perspectives/publications/2009/07/alarming-lessons-from-siemens/files/publication/fileattachment/arnoldporterllpiflrjulyaugust-2009.pdf?rev=8666f136bc3945e2972210f706b9d12a&sc_lang=en&hash=680B85B389E9961C3321C942BE5FDBD9.

[146] *See, e.g.*, WILMERHALE, *supra* note 144; MICHAEL HUNEKE & DUNIN-WASOWICZ, WESTLAW TODAY, PART I - CONVERGING PRACTICES FOR BRIBERY, EXPORT CONTROLS AND SANCTIONS ANTI-EVASION REGIMES (2023), https://files.hugheshubbard.com/files/Converging-practices-for-bribery-export-controls.pdf.

cognizant of the time needed to finalize such actions, it has been nearly a year since BIS stated such fines were forthcoming and, particularly in the context of preventing Russian diversion, time is of the essence.

### ii. BIS should charge companies with "knowing" violations when they fail to sufficiently investigate red flags or other strong indicia of potential diversion and violations occur.

Just as it has not issued robust enough fines, BIS has not used the full parameters of its authority to punish "knowing" violations of the EAR. BIS has authority to punish export control violations under the "knowing" standard not only where an entity had positive knowledge of an export control violation, but also where an entity had "an awareness of a high probability of [the] existence or future occurrence" of a violation of the EAR.[147] But BIS has never brought such an enforcement action.[148]

The history of the FCPA again provides a useful analog for why such enforcement actions would likely compel more proactive compliance. In the years following Siemens, DOJ and the SEC continued robust enforcement with significant fines.[149] They also began to more frequently charge companies under the FCPA's analogous "awareness of a high probability" knowledge standard, leading to a number of practical realities for companies that included (1) no longer "avoid[ing] potential consequences by simply taking steps not to acquire actual knowledge" of corruption and (2) "develop[ing] practices for identifying, assessing, and mitigating corruption risks."[150] DOJ and the SEC assisted in these efforts by issuing published guidance that includes common "red flags" indicating a high probability of corruption, helping companies to develop anti-corruption compliance programs that appropriately assess third-party risks.[151]

Through its public list of "Red Flag Indicators" and joint alerts and notices with FinCEN, BIS has already provided companies with significant indicators of what to be on the lookout for regarding a "high probability" of export evasion.[152] BIS could easily make clear to companies that it will

[147] *See supra* Section II.B.ii.

[148] *Supra* note 131.

[149] *See* Joseph Yockey, *FCPA Settlement, Internal Strife, and the "Culture of Compliance,"* 2012 WISC. L. REV. 690 (2012), https://wlr.law.wisc.edu/wp-content/uploads/sites/1263/2012/04/15-Yockey.pdf.

[150] MICHAEL HUNEKE & DUNIN-WASOWICZ, *supra* note 146.

[151] See DEP'T OF JUST., CRIM. DIV. & U.S. SEC. AND EXCH. COMM'N, ENF'T DIV., *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2d ed. 2020), https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl?inline.

[152] BUREAU OF INDUS. AND SEC., *Red Flag Indicators*, https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators (last accessed Dec. 16, 2024); FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT ALERT: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY URGE INCREASED VIGILANCE FOR POTENTIAL RUSSIAN AND BELARUSIAN EXPORT CONTROL EVASION ATTEMPTS (2022), https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT ALERT: SUPPLEMENTAL ALERT: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY URGE CONTINUED VIGILANCE FOR POTENTIAL RUSSIAN EXPORT

consider transactions entered into despite these "red flags" to have circumstantial evidence of a "high probability" of evasion.[153] BIS can and should punish companies under the current "knowing" standard for transactions that they enter into which (1) have red flags, (2) lack additional, significant due diligence despite the existence of red flags and (3) result in violations of U.S. export controls.

### iii. BIS should rely less on voluntary compliance from semiconductor companies and instead mandate specific components an export control compliance program must contain.

The Subcommittee's findings demonstrate that BIS relies too significantly on voluntary compliance with its suggested practices to ensure that semiconductor companies implement robust export controls programs. BIS officials explained to the Subcommittee that BIS has historically relied on voluntary compliance because it permits enforcement to be nimbler in a rapidly changing environment, such as Russian diversion efforts.[154] BIS explained that it believes that this allows it to quickly ask companies to do specific things and have them implemented efficiently.[155]

But the Subcommittee's findings demonstrate that the pendulum has swung too far. The Subcommittee's September 10, 2024 report provided findings demonstrating that the current enforcement regime has yielded export controls at Analog Devices, Intel, Texas Instruments, and AMD (and, likely, in the semiconductor manufacturing industry more generally) which are too reactive.[156] While the records provided to the Subcommittee demonstrate that these four companies quickly respond and implement specific asks made by BIS, some of BIS's asks seem like straightforward things that companies like Analog Devices, Intel, Texas Instruments, and AMD—sophisticated, multibillion dollar technology firms—could and should have been doing themselves. Making more components of export control programs mandatory could remedy these issues, and larger fines would likely compel more proactive compliance.

BIS's interactions with the Subcommittee also demonstrate another, similar issue with a regime too focused on voluntary controls: a fear of robust oversight chilling compliance. BIS repeatedly expressed to the Subcommittee its worry that the Subcommittee's requests to the four companies investigated for certain, limited records would chill their voluntary compliance.[157] BIS's

---

CONTROL EVASION ATTEMPTS (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; FIN. CRIMES ENF'T NETWORK & BUREAU OF INDUS. AND SEC., FINCEN & BIS JOINT NOTICE: FINCEN AND THE U.S. DEPARTMENT OF COMMERCE'S BUREAU OF INDUSTRY AND SECURITY ANNOUNCE NEW REPORTING KEY TERM AND HIGHLIGHT RED FLAGS RELATING TO GLOBAL EVASION OF U.S. EXPORT CONTROLS (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf.

[153] Carlson & Huneke, *supra* note 130.

[154] BIS July 18 Briefing, *supra* note 116.

[155] *Id*.

[156] PSI September 2024 Report, *supra* note 1.

[157] *See supra* Section II.B.i.

preference for voluntary compliance thus put it in the position of a regulator asking Congress for less scrutiny of regulated entities. Nothing requires BIS to rely on voluntary compliance to this degree, and having this type of relationship with its regulated entities makes BIS a less effective regulator.

### iv. BIS should require periodic, routine reviews of semiconductor companies' export control plans by outside entities.

As noted above, since Russia's invasion of Ukraine only 4 semiconductor related companies have had BIS review their export control compliance plans.[158] BIS informed the Subcommittee that usually only small to medium-sized companies and startups that do not have sizeable, specialized compliance teams ask BIS to review their export control plans.[159] These reviews by BIS are voluntary, and any recommended improvements from BIS are nonbinding.

The Subcommittee's findings show that these reviews should be compulsory for all semiconductor companies and any recommendations for improvement in export control compliance programs mandatory. The Subcommittee's September 10, 2024 report showed that Analog Devices, Intel, Texas Instruments, and AMD were not complying with BIS's best practices.[160] Had BIS required periodic external review of company's export control plans—by BIS or other qualified individuals—these issues could have been earlier highlighted and remedied. And there is little question BIS could require routine reviews—where any suggestions for improvement were required—under its existing authority.

BIS could either conduct these reviews itself, making them compulsory and annual rather than voluntary, or it could require companies to have independent annual reviews and document and report the results. A good model for what the second alternative might look like can be found in the Bank Secrecy Act's requirements for independent review of anti-money laundering programs. There are numerous provisions in the Bank Secrecy Act regarding this issue. As one example, the Bank Secrecy Act requires that money services businesses establish anti-money laundering programs that include "an independent audit function to test programs."[161] The Treasury Department's Financial Crimes Enforcement Network (FinCEN) provides guidance to money services businesses on what this review should look like—including examining compliance with certain policies, procedures, and best practices.[162] It explains who should conduct the review, how

---

[158] *Id.*

[159] July 3 BIS Letter, *supra* note 124.

[160] PSI September 2024 Report, *supra* note 1.

[161] 31 U.S.C. § 5318(h)(1)(D).

[162] DEPT. OF TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-20006-G012, GUIDANCE, FREQUENTLY ASKED QUESTIONS: CONDUCTING INDEPENDENT REVIEWS OF MONEY SERVICES BUSINESSES ANTI-MONEY LAUNDERING PROGRAMS (2006), https://www.fincen.gov/sites/default/files/shared/Guidance_MSB_Independent_Audits9-21.pdf.

often reviews should occur, and what documentation should accompany such a review.[163] BIS could and should implement such a requirement for, at a minimum, companies facing a high risk of diversion, such as semiconductor manufacturers and distributors. It should also take steps to publicize and punish companies who these reviews show consistently lack diligence in supporting enforcement of export controls.

[163] *Id*.

## Conclusion

Over the last 15 years, the role of export controls in the U.S. national security arsenal has undergone a dramatic enhancement. Export controls are now looked at as a key tool to halt the advance of adversaries at war. They are also increasingly relied upon to maintain U.S. strategic technological dominance.

The Subcommittee's inquiry makes clear that more must be done for export controls to accomplish these goals. Congress must fund BIS like the critical national security cog it has become. And BIS must use the full scope of its authority to ensure compliance with U.S. export control law. Absent these improvements, the U.S. export control regime will remain in its current state: strong on paper, weak in practice.