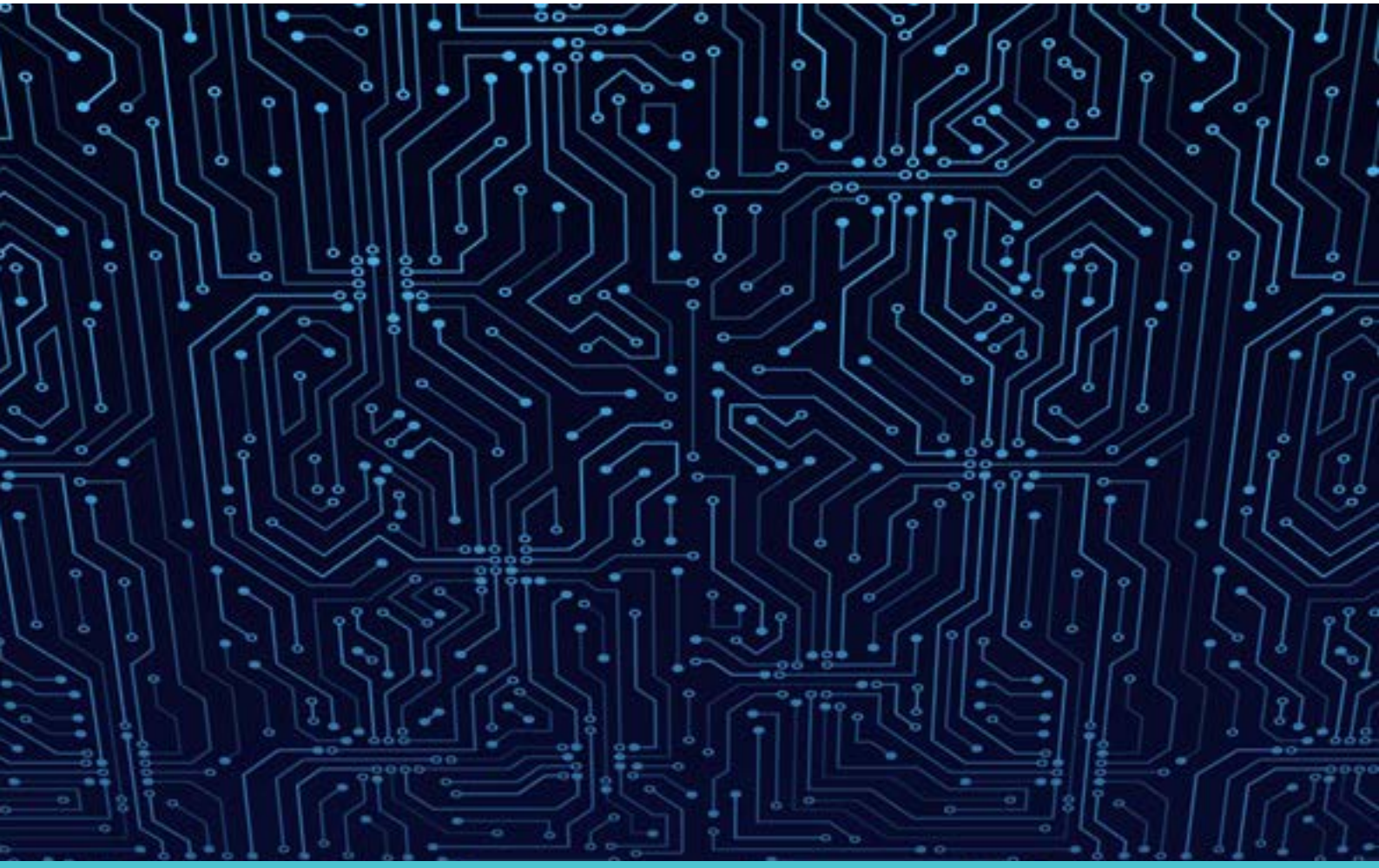
United States Senate

Permanent Subcommittee on Investigations



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

Examining Semiconductor Manufacturers' Compliance with Export Controls

Chairman Richard Blumenthal
Directeur général

Majority Staff Report

September 10, 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On Monday July 8, 2024, a Russian Kh-101 cruise missile struck Kyiv's largest children's hospital, Okhmatdyt Children's Hospital, during a daytime barrage of Russian missiles that killed at least 42 people throughout Ukraine.[1]

Figure 1: Russian Cruise Missile Strike on a Children's Hospital in Kyiv[2]

Kh-101 cruise missiles like the one that struck Okhmatdyt Children's Hospital are critical to Russia's continued assault on Ukraine.[3] These savage weapons could not be made or fired without electronics from U.S. manufacturers, including semiconductors from Analog Devices Incorporated (Analog Devices), Intel Corporation (Intel), and Texas Instruments Incorporated (Texas Instruments).[4] The export of these and other semiconductors to Russia has been subject to a host of increasing restrictions since Russia launched its war in Ukraine in 2022. Yet, more than two years later, they still continue to appear in Russian weapons and help inflict terror on the Ukrainian people.

While export control compliance may seem remote and technical, the strike on Okhmatdyt Children's Hospital—and many others like it—shows that the risks of U.S.

---

[1] Samya Kullab and Illia Novikov, *Ukraine mourns as rescuers search the rubble of a Kyiv children's hospital struck by a missile*, ASSOCIATED PRESS (July 9, 2024), https://apnews.com/article/russia-ukraine-war-missiles-children-hospital-kyiv-0a33ed16baf2c509b205705bdd1155db.

[2] *Russia hits Kyiv children's hospital, casualties reported*, KYIV INDEPENDENT (July 8, 2024), https://kyivindependent.com/russian-missile-attack-hits-okhmatdyt-children-hospital-casualties-reported/.

[3] Christopher Miller, *Type of Russian missile that struck Kyiv's children's hospital uses Western components*, FINANCIAL TIMES (July 9, 2024), https://www.ft.com/content/ef463ac9-4804-4ad7-b9a2-c113590f2f96/.

[4] *Id.*

export controls failing could not be more real for Ukraine. The need for robust compliance and vigorous enforcement of export controls extends far beyond the Russia-Ukraine war: export controls have emerged as a critical tool of U.S. national security over the last 15 years, central not only to efforts to constrain Russia's advances but also attempts to slow China's push to match the U.S. in artificial intelligence. Export controls are a particularly important tool for constraining access to critical technologies in which U.S. companies maintain dominance. This includes semiconductors, which are needed to run electronic devices such as Kh-101 cruise missiles and other complex weapons systems.

The Permanent Subcommittee on Investigations ("PSI" or "the Subcommittee") initiated an inquiry in September 2023 to better understand efforts of American semiconductor manufacturers to prevent U.S.-manufactured semiconductors from ending up in Russian weapons. The Subcommittee focused its inquiry on four U.S.-based semiconductor manufacturers whose products have reportedly appeared in Russian weapons (including Kh-101 cruise missiles) on a consistent basis: Analog Devices, Intel, Texas Instruments, and Advanced Micro Devices Incorporated (AMD) (collectively, the "Four Companies").

The U.S. export control regime for semiconductors relies heavily on corporate compliance and diligence, asking that companies implement practices to ensure that their products do not wind up in the wrong hands. The federal government has provided companies with a number of tools to further this mission while emphasizing that companies must develop their own systems to identify questionable transactions and continuously adapt to confront adversaries focused on acquiring their products. Corporate success in these efforts necessitates proactive controls and visibility up-and-down the distribution chain. But, while maintaining this visibility may be challenging for manufacturers of highly fungible products, these are not unprecedented demands: Financial institutions have been asked to implement similar programs to combat money laundering, requiring them to follow the path of items even more fungible than semiconductors. U.S. companies across a wide-range of industries have also been asked to integrate robust processes to guard against violations of the Foreign Corrupt Practices Act (FCPA) in their business dealings across the globe. Both efforts have required industries to develop proactive corporate compliance regimes, but have been critical in stamping out corruption and fraud around the globe.

This report represents the Subcommittee's findings on the role that the four selected semiconductor manufacturers play in ensuring that their products do not continue to fuel Russia's aggression in Ukraine; however, these findings can be applied more broadly to export control compliance efforts across the semiconductor manufacturing industry.

The Subcommittee's investigation found that U.S. semiconductor manufacturer efforts have been abjectly lacking. Some companies have done the bare minimum required by law, conducting cursory checks on their customers while trying to wash their hands of any real responsibility for their distributors' role in Russian diversion. Few have looked under the hood to see what they could do better. However, willful ignorance also violates the law, and models from other industries show that proactive compliance is readily doable and affordable. Changing this laissez-faire attitude towards export control compliance will help guard against Russian diversion efforts and also pay dividends in ongoing efforts to use semiconductor export controls to constrain China's ambitions in artificial intelligence.

The Subcommittee's inquiry found:

- The semiconductor manufacturing industry has not increased its compliance efforts effectively or fast enough to combat Russian diversion efforts.

- Exports from AMD, Analog Devices, Intel, and Texas Instruments to multiple countries with entities identified as assisting in Russian diversion efforts were significantly elevated in 2023 compared to exports prior to Russia's war in Ukraine.

- Since the start of 2024, AMD, Analog Devices, Intel, and Texas Instruments have each identified and blocked sales to entities potentially involved in Russian diversion. However, these sales could have been identified and blocked earlier and faster with more proactive compliance regimes.

- Export controls compliance policies at AMD, Analog Devices, Intel, and Texas Instruments fail to meet best practices and recommendations from the Department of Commerce and non-governmental organizations. All (except for AMD) have failed to timely respond to external tracing efforts, and each presently lacks sufficient internal auditing and distributor auditing related to export controls compliance.

The Subcommittee chose the Four Companies—among the largest semiconductor companies in the United States—as representative examples of the industry's export compliance efforts. It does not assume that the compliance efforts at these companies are better or worse than any other, but rather that their flaws point to larger industry issues. Based on these findings, the Subcommittee has identified multiple ways that U.S. semiconductor manufacturers could improve their compliance with export controls

and assist the larger goal of trying to prevent their products from being used by hostile adversaries.

Accordingly, this report makes the following recommendations:

1. Semiconductor manufacturers should respond to external tracing efforts thoroughly and in a timely manner.

2. Semiconductor manufacturers should annually audit their entire export controls compliance programs, and audit targeted processes more frequently—particularly when problems arise or regulations change.

3. Semiconductor manufacturers should implement policies to provide increased visibility into export controls compliance in their distribution chain, including yearly auditing of all of their distributors' export controls compliance.

4. Semiconductor manufacturers should routinely submit export control compliance plans for review and comment by the Department of Commerce's Bureau of Industry and Security (BIS).

PART I: BACKGROUND

A. Semiconductors are essential to Russia's war effort in Ukraine

Semiconductors are essential components of most electronic devices, ranging from computers and smartphones to household appliances. The terms microchip, electronic integrated circuit, and semiconductor are generally used interchangeably to refer to electronic components made using semiconductors.[5] However, semiconductor technology also reaches far beyond consumer goods. Cutting-edge microchips have applications in both civilian and military products, such as weapons and air guidance systems for military aircraft.[6] U.S. companies dominate the global semiconductor manufacturing industry, representing nearly half the global market share.[7]

Both before and since the beginning of Russia's war in Ukraine, U.S.-manufactured semiconductors have been found in a range of military equipment—including weapons and other military support technology—used by the Russian military.[8] This includes drones, radios, missiles, and armored vehicles.[9] It also includes some of Russia's most modern military systems, such as cruise missiles, communications systems, and electronic warfare complexes.[10] Russia needs U.S. semiconductors because there are few ready substitutes for the U.S.-manufactured semiconductors that power Russian military technology, and attempts to substitute for or replicate them have been

---

[5] *See, e.g.*, *What Is a Semiconductor?*, SEMICONDUCTOR INDUS. ASS'N, https://www.semiconductors.org/semiconductors-101/what-is-a-semiconductor/ (last visited Sept. 3, 2024) ("Semiconductors, sometimes referred to as integrated circuits (ICs) or microchips. . .").

[6] Matthew Schleich, *Securing Semiconductors: How to Scale-up Global Semiconductor Production and Protect U.S. National Security at the Same Time*, OFFICE OF THE UNDER SEC'Y FOR ARMS CONTROL AND INT'L SEC., U.S. DEP'T OF STATE (May 15, 2023), https://www.state.gov/securing-semiconductors-how-to-scale-up-global-semiconductor-production-and-protect-u-s-national-security-at-the-same-time/; William Alan Reinsch et al., *Securing Semiconductor Supply Chains: An Affirmative Agenda for International Cooperation,* CTR FOR STRATEGIC AND INT'L STUDIES, (Aug. 2, 2022) https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220802_Reinsch_Semiconductors.pdf?VersionId=WMGKge29KFMOBw9BkvwzkxomJ4mUtsr.

[7] *2023 Factbook*, SEMICONDUCTOR INDUS. ASS'N, https://www.semiconductors.org/wp-content/uploads/2023/05/SIA-2023-Factbook_1.pdf (last visited Sept. 3, 2024).

[8] *See, e.g.*, Kristina Partsinevelos, *The chip industry's open secret: Adversaries' military tech relies on U.S. components,* CNBC (Apr. 17, 2023), https://www.cnbc.com/2023/04/17/us-components-found-in-russian-iranian-military-tech.html.

[9] Karen Gilchrist, *How U.S. microchips are fueling Russia's military — despite sanctions*, CNBC (Aug. 7, 2023), https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html.

[10] *Id.*

unsuccessful.[11] Owing to this reality, the United States and a host of partner nations have imposed export controls meant to restrict the flow of the semiconductors critical to Russian military technology.[12]

B. 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 these restrictions. 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.[13] The Subcommittee requested information and records concerning each company's export control compliance procedures and processes, their responses to any reports of their products in Russian weapons, and data on their exports from 2021 to the present to Russia and 10 other countries (Armenia, Belarus, China, Finland, Georgia, Hong Kong, Kazakhstan, Kyrgyzstan, Russia, Turkey, and Uzbekistan) that have been identified as countries with entities that have assisted or potentially assisted the Russian Federation in acquiring semiconductors.[14] The Subcommittee also requested information and records from the Department of Commerce's Bureau of Industry and Security (BIS) concerning enforcement efforts, the presence of U.S.-

---

[11] *See, e.g.*, Pavel Urusov, *Vital Microchip Sanctions Will Hit Russian Computing Power Hard*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 25, 2023), https://carnegieendowment.org/politika/90250.

[12] *See, e.g.*, Press Release, Bureau of Indus. and Sec., U.S. Dep't of Commerce, 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#:~:text=To%20restrict%20Russia%20and%20Belarus,certain%20plants%20or%20major%20components; Press Release, Bureau of Indus. and Sec., U.S. Dep't of Commerce, Commerce, International Partners Continue Cooperation in Response to Russia's Illegal Invasion of Ukraine (Sept. 19, 2023), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3332-2023-09-14-bis-pressrelease-quad-meeting-hs-code-update-final/file; Press Release, Bureau of Indus. and Sec., U.S. Dep't of Commerce, United States-Australia-Canada-New Zealand-United Kingdom Release Joint Guidance on Countering Russia Evasion (Sept. 26, 2023), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3337- final-2023-09-22-bis-press-release-quint-seal-ee-ocpa-clean-ajb-osb/file.

[13] *See supra* Section I.C for a more detailed description of the reports which have consistently named products from these four companies.

[14] *See, e.g.*, Nathaniel Taplin, *How Russia Supplies Its War Machine*, WALL STREET J. (March 10, 2023), https://www.wsj.com/articles/russia-ukraine-tech-chips-exports-china-f28b60ca; Georgi Kantchev, Paul Hannon, and Laurence Norman, *How Sanctioned Western Goods Are Still Flowing Into Russia*, WALL STREET 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.

manufactured semiconductors in Russian weapons, and guidance provided to semiconductor manufacturers, including the Four Companies.[15]

During the subsequent 12 months, the Subcommittee reviewed thousands of pages of documents and data from AMD, Analog Devices, Intel, Texas Instruments, and BIS. The Subcommittee received briefings from representatives from AMD, Analog Devices, Intel, and non-governmental organizations focused on tracing the technology utilized in weapons in the Russia-Ukraine war as well as 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.[16]

C. Reports from non-governmental organizations have shown the continued presence of U.S.-manufactured semiconductors in Russian weapons.

Numerous reports since Russia's invasion of Ukraine have consistently identified U.S.-manufactured semiconductors in Russian military supplies recovered on the battlefield,

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

[16] *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].

demonstrating Russia's continued ability to acquire these products.[17] These reports demonstrate that, despite increased export controls, U.S. technology continues to fuel Russia's war in Ukraine.[18] Reporting on the contents of Russian military technology has consistently shown that the vast majority of the foreign components found in Russian weapons are U.S.-manufactured. RUSI, a U.K-based defense and security tank which has been visiting Ukraine and charting the origins of components from Russian weapons since the start of the war, worked in August 2022 to document 450 foreign components in Russian weapons systems and identified 318 as having U.S. origins, with Texas Instruments and Analog Devices as the two U.S. companies with the most components.[19] KSE Institute, an analytical center at the Kyiv School of Economics which has worked since the start of the war to analyze the effectiveness of sanctions and export controls, issued a report in June 2023 that considered 1057 foreign components in Russian weapons and found that two-thirds had U.S. origins.[20] Elina Ribakova, Director of the International Affairs Program and vice president for foreign policy at the Kyiv School of Economics, testified to the Subcommittee in February 2024 that Ukraine's National Agency for Corruption Prevention had document 2,797 foreign components in Russian weapons systems and found 2,007 (72%) has U.S. origins.[21]

Reports indicate that export controls have become less effective at constraining Russia's ability to acquire semiconductors and other battlefield goods as the war in Ukraine has progressed. While export controls initially constrained Russian efforts to acquire the

---

[17] *See, e.g.*, James Byrne et al., *Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine*, ROYAL UNITED SERVS. INST. (Aug. 2022), https://rusi.org/explore-our-research/publications/specialresources/silicon-lifeline-western-electronics-heart-russias-war-machine [hereinafter Byrne et al., *Silicon Lifeline*]; *Identifying Post-Invasion Components in Russian Weapons*, CONFLICT ARMAMENT RESEARCH (Apr. 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 [hereinafter Bilousova et al., *Russia's Military Capacity*]; 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 [hereinafter Byrne et al., *In Plain Sight*]; 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 [hereinafter Bilousova et al., *Challenges of Export Control Enforcement*].

[18] *Supra* note 17; *see also infra* text accompanying notes 19-21.

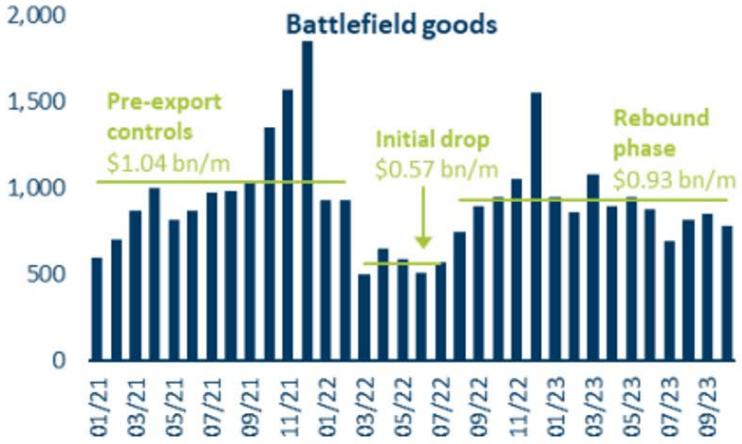
[19] Byrne et al., *Silicon Lifeline*, *supra* note 17.

[20] Bilousova et al., *Russia's Military Capacity*, *supra* note 17.

[21] *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/wp-content/uploads/Ribakova-Testimony-Feb.-27-2024-Updated.pdf (testimony of Elina Ribakova, Director of the International Affairs Program and vice president for foreign policy at the Kyiv School of Economics) [hereinafter Ribakova Testimony].

components (including semiconductors) most critical to its war effort, Russia's ability to import these materials recovered significantly in 2023.[22] KSE Institute's January 2024 report analyzed certain customs data and found that, prior to the imposition of sanctions, Russia imported $1.04 billion in battlefield goods per month.[23] This number dropped to a monthly average of $565 million in the six months after the imposition of sanctions and export controls in February 2022 (a 45% decrease), but rebounded in the six months following to approximately the same amount as pre-sanctions.[24] For the months of January to October 2023, these imports were $932 million a month—only a 10% decrease.[25] These numbers are detailed below in Figure 2.

Figure 2: Russian Imports of Battlefield Goods in $ Millions, January 2021 to October 2023



Source: KSE Institute, Challenges of Export Controls Enforcement

Reports over the last two years have consistently shown that the reason for Russia's continued success in acquiring necessary goods lies in the use of entities located in third-party countries who then ship those goods onto Russia, a process referred to as transshipment. 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.[26] Entities in Hong Kong and China—which receive substantially more U.S. semiconductor imports than the other

[22] Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17.

[23] *Id.*

[24] *Id.*

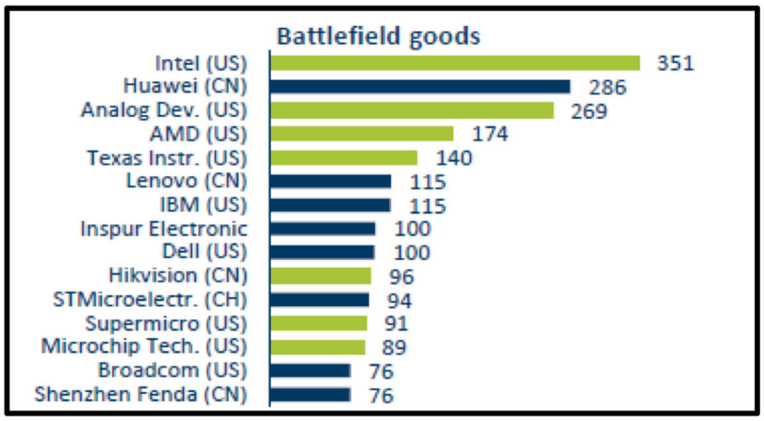
[25] Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17; *See also, e.g.*, Bilousova et al., *Russia's Military Capacity*, *supra* note 17; *Russian Sanctions Database November 2023 edition*, ATLANTIC COUNCIL, https://www.atlanticcouncil.org/blogs/econographics/russia-sanctions-database-november-2023/.

[26] *Supra* note 17.

countries noted—are understood to be responsible for the vast majority of the continuing flow of semiconductors to Russia.[27]

Since Russia's invasion of Ukraine, products from four U.S. semiconductor manufacturers—AMD, Analog Devices, Intel, and Texas Instruments—have been the most prevalent in Russian weapons. Products from Analog Devices and Texas Instruments were the most prominent in the 450 components analyzed by RUSI in August 2022, with Intel and AMD (including its subsidiary Xilinx) both in the top 10.[28] KSE Institute's June 2023 report listed AMD, Analog Devices, Intel, and Texas Instruments as four of the five U.S. companies which accounted for the most technology imports found in Russian weapons systems.[29] KSE Institute's January 2024 report, which evaluated more recent data, determined that these four companies were the top producers of battlefield goods imported to Russia that were also found in Russian weapons from January to October 2023.[30] These numbers are shown below in Figure 3.

Figure 3: Top Producers of Battlefield Goods Imported to Russia, January to October 2023



Source: KSE Institute, Challenges of Export Controls Enforcement

Note: Figures shown are in millions of dollars. Green bars are for companies whose components have been found on the battlefield.[31]

Representatives from RUSI, CAR, and KSE Institute testified at the Subcommittee's February 2024 hearing and reaffirmed many of the details that have appeared in these reports. Damien Spleeters, Deputy Director of Operations at CAR, an organization that works on the ground in Ukraine (and other active conflicts) to document weapons at

[27] Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17.
[28] Byrne et al., *Silicon Lifeline*, *supra* note 17.
[29] Bilousova et al., *Russia's Military Capacity*, *supra* note 17.
[30] Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17.
[31] *Id.*

the point of use and track their sources back through chains of distribution, explained that analyses of downed Russian weapons have showed an increasing percentage of U.S.-manufactured semiconductors produced after Russia's invasion of Ukraine, indicating that Russia has been able to acquire newly manufactured semiconductors despite increased export controls.[32] James Byrne, then-Director of Open-Source Intelligence and Analysis at RUSI, described to the Subcommittee how Russia has increasingly acquired semiconductors through third-party countries including, most prominently, Hong Kong, China, Turkey, Uzbekistan, and the UAE.[33] Finally, Ms. Ribakova and Mr. Spleeters emphasized that U.S. manufacturers have a critical role to play in stopping this flow by proactively identifying and halting transactions which raise red flags and making available to tracing organizations robust documentation of sales down their distribution chains (including requesting and verifying point-of-sale data from their distributors) so that new paths Russia may seek can be identified and blocked.[34] All three witnesses emphasized that engagement from manufacturers to assist their organizations in their tracing efforts had been limited.[35] Ms. Ribakova contrasted the significant outreach KSE Institute had received from the financial sector soon after its June 2023 report, in which financial institutions asked important questions like "how can we cooperate, how they can obtain similar data, what are the red flags [KSE Institute] is picking up," with the complete lack of contact KSE Institute had received from any semiconductor manufacturer.[36]

[32] PSI February 2024 Hearing, *supra* note 16.

[33] *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/wp-content/uploads/Testimony-Byrne-Feb.-27-2024.pdf (testimony of James Byrne, Director of Open-Source Intelligence and Analysis at Royal United Services Institute) [hereinafter Byrne Testimony].

[34] PSI February 2024 Hearing, *supra* note 16.

[35] *Id.*

[36] *Id*.

D. The Success of U.S. Export Controls Requires Proactive Corporate Compliance

i. The U.S. Government has implemented a host of new export controls in response to Russia's invasion of Ukraine.

A host of new regulations regarding the export of semiconductors have been added since Russia's invasion of Ukraine. Semiconductors are among the products whose export are regulated by the Department of Commerce's Bureau of Information and Security (BIS), charged with ensuring "that appropriate export controls are placed on dual-use and certain military items through the Export Administration Regulation (EAR)."[37] Since Russia's invasion of Ukraine, BIS has sought to constrain Russia's war effort by, among other measures:

1. adding over 1,000 entities from over thirty-five countries believed to be connected to Russian military activity 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";[38]

2. issuing two Foreign Direct Product Rules (FDPR), which subject U.S. items overseas and items produced overseas using U.S.-origin components or made using U.S. technology to the EAR, "[t]o restrict Russia and Belarus' abilities to acquire certain foreign-produced items;[39]

3. issuing multiple joint notices with the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) to highlight red flags in transactions which might alert companies to increased concerns regarding Russian

---

[37] *See, e.g.*, *Annual Report to Congress for Fiscal Year 2020*, U.S. DEP'T OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY (BIS), https://www.bis.doc.gov/index.php/documents/pdfs/2711-2020-bis-annual-report-final/file.

[38] Press Release, Bureau of Indus. and Sec., U.S. Dep't of Commerce, Commerce Tightens Export Controls, Targets Illicit Procurement Networks For Supplying Russian War Machine (Aug. 23, 2024), https://www.bis.gov/press-release/commerce-tightens-export-controls-targets-illicit-procurement-networks-supplying; 15 CFR § 744.16.

[39] Press Release, Bureau of Indus. and Sec., U.S. Dep't of Commerce, 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#:~:text=To%20restrict%20Russia%20and%20Belarus,certain%20plants%20or%20major%20components. In February 2023, after the discovery of Iranian made UAVs deployed by Russia in Ukraine, BIS simultaneously added the Iran FDPR, § 734.9(j), subjecting a category of EAR99 items destined to Iran to licensing requirements, and amended the Russia/Belarus FDPR to reference those ER99 items. 88 Fed. Reg. 12150 (Feb. 24, 2023) (codified in 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.

diversion;[40] and

4. providing companies with "supplier list" letters, "red flag" letters, and "is informed" letters to explain to them that certain of their customers may pose high risks of diversion of goods to Russia, and asking them to take additional steps before engaging in any transactions with these entities.[41]

Companies are ultimately responsible for developing compliance programs to ensure that they comply with U.S. export controls. These compliance programs need to, among other things, ensure that the company obtains appropriate export licenses for certain items and ensure that the company does not send restricted items to sanctioned parties or countries.[42] Individual companies have the discretion to determine how to create compliance programs and processes to ensure that they adhere to export controls. BIS offers guidance to companies concerning best practices that they can choose to follow.[43] This guidance, including that housed in a manual on BIS's website entitled *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program*, offers recommendations regarding the principal components an export control compliance program should having as well as information, tools, and templates for developing one.[44] In addition to providing *Export Compliance Guidelines*, BIS also offers companies a voluntary and free review of the company's export compliance

[40] *See, e.g.*, FinCEN & BIS, *FinCen & BIS Joint Alert: FIN-2022-Alert003*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (June 28, 2022), https://www.fincen.gov/sites/default/files/202206/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; FinCEN & BIS, *FinCen & BIS Joint Alert: FIN-2023-Alert004*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (May 19, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; *FinCen & BIS Joint Alert: FIN-2023-NTC2*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (Nov. 6, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf.

[41] BIS, *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*, U.S. DEP'T OF COMMERCE (July 10, 2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

[42] *U.S. Export Licenses Navigating Issues & Resources*, INT'L TRADE ADMINISTRATION (last viewed Sept. 5, 2024), https://www.trade.gov/us-export-licenses-navigating-issues-and-resources; BIS, *Introduction to Commerce Department Export Control*, U.S. DEP'T OF COMMERCE (Nov. 2018), https://www.bis.doc.gov/index.php/documents/regulations-docs/142-eccn-pdf/file. Items may need export licenses from BIS depending on where they are going, to whom they are going, or their intended end-use. *Comply with U.S. Export Regulations*, INT'L TRADE ADMINISTRATION, https://www.trade.gov/us-export-regulations, (last accessed Sept. 5, 2024).

[43] *See* BIS, *Export Compliance Guidelines: Elements of an Effective Export Compliance Program*, U.S. DEP'T OF COMMERCE (Jan. 2017), https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file [hereinafter BIS Export Control Guidelines].

[44] *See id.*

program.[45] Since the start of Russia's war on Ukraine, numerous non-governmental organizations have offered additional proposed policies and procedures companies could consider to help stem the flow of goods to Russia.[46]

The current system of export controls relies on robust corporate compliance for maximum effectiveness. As such, the majority of U.S. government export control actions aimed at stopping Russia's war effort are geared towards corporate actors proactively finding and halting suspicious transactions. BIS places certain suspicious companies on the Entity List, imposing additional licensing requirements on transactions with these groups because these are "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".[47] While placement of a company on the Entity List carries with it specific additional license requirements, BIS also sends companies "supplier list" letters, which identify entities that do not appear on BIS's screening list but who BIS has reason to believe have exported to or facilitated transactions with destinations or end users of national security or foreign policy concern, and "red flag" letters, which inform a company that one of their customers may have violated the EAR by reexporting or transferring the same type of item the company previously exported to the customer.[48] "Red flag" and "supplier list" letters are meant to alert companies that certain customers pose a higher risk of diversion so that the companies can conduct additional diligence about those customers prior to fulfilling any orders.[49] BIS and FinCEN joint notices are geared towards providing companies with certain criteria that might cause them to independently conduct additional diligence in any given transaction prior to completing it.[50] All of these actions

[45] BIS, *How Can You Create an Effective Export Compliance Program?,* U.S. DEP'T OF COMMERCE, https://www.bis.gov/articles/how-can-you-create-effective-export-compliance-program (last accessed Sept. 5, 2024).

[46] *See, e.g.*, Hilgenstock, B., E. Ribakova, A. Vlasyuk and G. Wolff (2024) "Using the Financial System to Enforce Export Controls", (Bruegl Working Paper, 2024), https://www.bruegel.org/working-paper/using-financial-system-enforce-export-controls (last accessed Sept. 5, 2024); "Export Controls: A Key G-7 Tool to Halt Russia's War", (The International Working Group on Russian Sanctions Working Paper #20, 2024), https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2024-06/working_paper_20_export_controls_june_12_2024_final_update.pdf; Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17.

[47] 15 CFR § 744.16.

[48] BIS, *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*, U.S. DEP'T OF COMMERCE, (July 2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

[49] *Id.*

[50] *See, e.g.*, FinCEN & BIS, *FinCen & BIS Joint Alert: FIN-2022-Alert003*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (June 28, 2022), https://www.fincen.gov/sites/default/files/202206/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; *FinCen & BIS Joint Alert: FIN-2023-Alert004*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (May 19, 2023) https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf; *FinCen & BIS Joint Alert: FIN-2023-NTC2*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF

are ultimately predicated on the effectiveness and robustness of company due diligence, either in thoroughly checking transactions with entities BIS highlights or independently identifying and halting transactions with entities BIS may not yet be aware pose diversion risks.

ii. The use of export controls to constrain Russia's war effort is part of a larger trend towards the increased use of export controls for national security purposes.

In addition to complying with updated export controls regarding Russia, companies that export highly valuable dual-use goods like semiconductors also must create adequate compliance structures to address an export control regime that continues to grow in complexity and national security importance. Export controls are increasingly being used not only to undermine the ability of malign actors to bolster their military production, but also to create a strategic technology barrier to prevent these countries from gaining a military advantage in the future.[51]

The most prominent manifestation of this trend is the increased use of FDPRs.[52] Originally conceived during the Cold War,[53] the FDPR was 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.[54] In 2020, BIS crafted a FDPR specifically targeting Huawei, a Chinese multinational digital communications technology corporation.[55] A year earlier, BIS had added Huawei to the

---

COMMERCE (Nov. 6, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf.

[51] PSI February 2024 Hearing, *supra* note 16.

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

[53] 24 Fed. Reg. 3989 (May 16, 1959) (codified at 15 C.F.R. pt 385.2), https://www.govinfo.gov/content/pkg/FR-1959-05-16/pdf/FR-1959-05-16.pdf. Now called the "National Security FDPR."

[54] Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform, 78 Fed. Reg. 22660 (Apr. 16, 2013) (codified at 15 C.F.R. pts 736, 764), https://www.govinfo.gov/content/pkg/FR-2013-04-16/pdf/2013-08352.pdf; *Chains of Control: The History and Limits of America's Favourite New Economic Weapon*, *supra* note 52; 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 Red. Reg. 27418 (May 13, 2014) (codified at 15 C.F.R. pts 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.

[55] 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. 51596 (Aug. 20, 2020) (codified at 15 C.F.R. pts. 736, 744, 762),

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.[56]

Export controls on semiconductors have also figured prominently in recent efforts to halt China's advances in artificial intelligence. BIS issued an FDPR on October 7, 2022, to restrict the production of semiconductors and advanced computing items with AI applications in China.[57] 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.[58] The U.S. currently has technological primacy on the development and production of those chips and the FDPR was designed to maintain that advantage over China.[59]

Like the increased export controls against Russia, the success of these new export controls as a tool of national security hinges on corporate compliance, and federal officials have made clear that companies will be expected to develop robust compliance programs or face consequences. From January to October 2023, Russia imported $8.8 billion in high-priority goods recorded in more than 800,000 individual transactions, a volume that government investigators simply do not have the resources to monitor and scrutinize without robust corporate compliance efforts.[60] The need for corporate compliance is even more striking when considering the volumes at issue in China, which (even after a significant drop from the year before) imported $349.38 billion in semiconductors in 2023.[61] Senior Justice Department officials have recently warned companies that export controls violations will be an increased focus, that companies should think of their export control compliance like they think of FCPA compliance, and that companies across all industries must be "pressure-testing [their] sanctions

---

https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2593-85-fr-51596/file/.

[56] 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.

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

[58] *Id.*

[59] *Id*.

[60] Ribakova Testimony, *supra* note 21. Here, high-priority goods refers to goods on the Common High Priority List (CHPL), a list BIS developed which includes 50 items identified by six-digit Harmonized System (HS) Codes that Russia seeks to procure for its weapons programs. *Common High Priority List,* BUREAU OF INDUS. AND SEC., U.S. DEP'T OF COMMERCE, (Feb.2024), https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items.

[61] Jingyue Hsiao, *China sees the largest annual drop in chip import value in 2023*, DIGITIMES ASIA (Jan. 16, 2024), https://www.digitimes.com/news/a20240116VL200/2023-china-memory-chips-semiconductors.html.

compliance program, for instance through risk assessments, technology upgrades and industry benchmarking."[62]

[62] Speech, Deputy Attorney General Lisa O. Monaco Delivers Keynote Remarks at 2022 GIR Live: Women in Investigations (June 16, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-remarks-2022-gir-live-women.

PART II: FINDINGS

A. Exports of U.S.-manufactured semiconductors to countries of concern have increased since Russia's invasion of Ukraine

The Subcommittee's inquiry and review of data submitted by each of the Four Companies found that there have been substantial increases in exports of semiconductors to countries known to have entities engaged in transshipment. As part of its inquiry, the Subcommittee received complete 2021, 2022, and 2023 export data for AMD, Analog Devices, Intel, and Texas Instruments to Armenia, Belarus, China, Finland, Georgia, Hong Kong, Kazakhstan, Kyrgyzstan, Russia, Turkey, and Uzbekistan.[63] These countries have been identified as having entities that have assisted or potentially assisted the Russian Federation in acquiring semiconductors.[64]

Figure 4: Number of Exports by Individual Product Units to Armenia, Belarus, Finland, Georgia, Kazakhstan, Kyrgyzstan, Russia, Turkey, and Uzbekistan, 2021 to 2023[65]

	2021	2022	2023
Armenia	13, 259	372,414	156,052
Belarus	1,086,395	156,160	0
Finland	86,435,802	140,633,056	100,714,825
Georgia	375	13,014	470
Kazakhstan	1,936	1,918,771	1,070,916
Kyrgyzstan	0	0	0
Russia	44,771,637	10,081,470	-7,058
Turkey	14,523,007	31,574,164	34,599,586
Uzbekistan	23	0	0

[63] Prior to the Subcommittee's February 27, 2024 hearing, the Subcommittee's Majority Staff shared a memorandum with Subcommittee members regarding the status of the Subcommittee's inquiry. In that memorandum, the Subcommittee released data that it had received regarding exports from the Four Companies to Armenia, Finland, Georgia, Kazakhstan, and Turkey for 2021 and 2022. The Subcommittee has since received complete 2023 data for exports from the Four Companies to those countries, as well as the additional countries listed here.

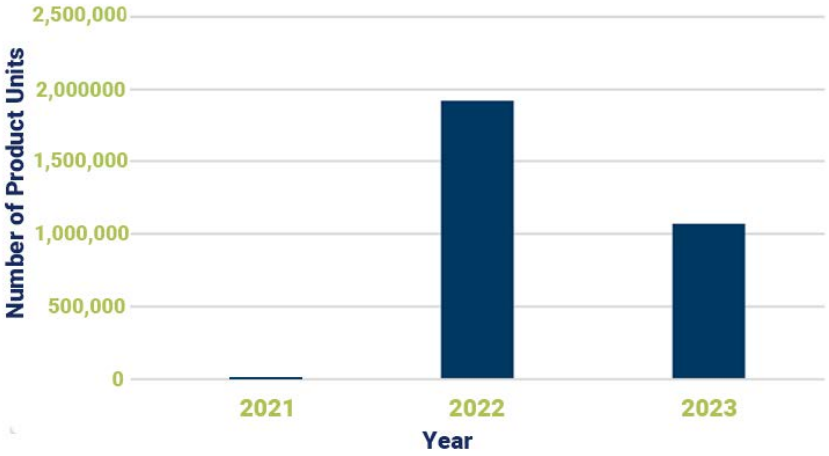
[64] *Supra* note 17.

[65] The Subcommittee summed the number of exports per year across the Four Companies. These data should also not be read to suggest that each company distributed products to each country listed during the years in question, or that the increases detailed herein exist or are uniform across each of the four companies. Letter from Counsel for AMD to Chairman Blumenthal (Mar. 22, 2024), AMD00621 – 45; Letter and Attachment from Counsel for Analog Devices to the Subcommittee (Dec. 22, 2023),

Company data showed a near doubling in exports of semiconductors (recorded in individual product units) to 5 of the identified countries from 2021 to 2022, including Armenia, Finland, Georgia, Kazakhstan, and Turkey.

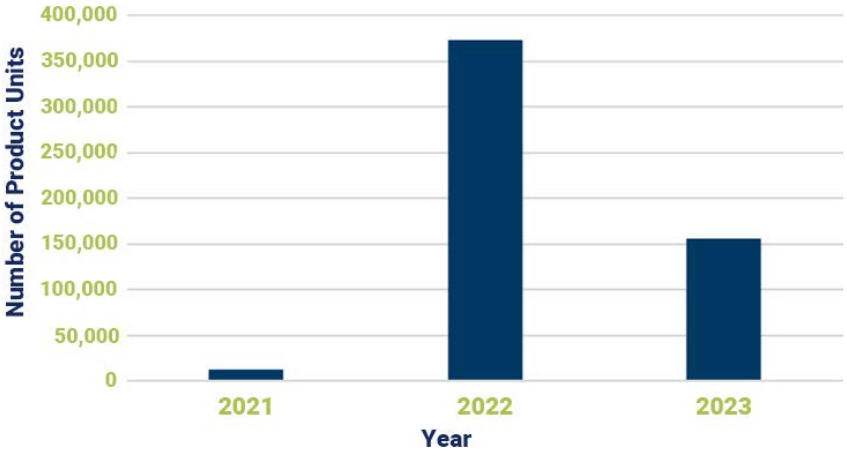
Although data obtained by the Subcommittee indicates decreases from 2022 to 2023, the 2023 data continues to show significant and meaningful increases in semiconductor exports to many of these countries compared to exports prior to Russia's invasion of Ukraine, as shown in the figure above. In particular, semiconductor exports to Kazakhstan in 2023 were still over 550 times greater than they were in 2021:

Figure 5: Number of Exports by Individual Product Units to Kazakhstan, 2021 to 2023



Semiconductor exports to Armenia were nearly 12 times greater in 2023 than they were 2021:

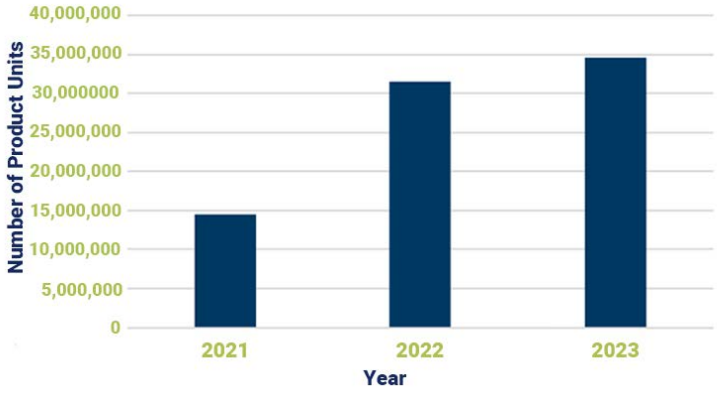
Figure 6: Number of Exports by Individual Product Units to Armenia, 2021 to 2023



Analog_PSI_00000418; Letter and Attachment from Counsel for Analog Devices to the Subcommittee (Feb. 2, 2024), Analog_PSI_00000420; Letter and Attachment from Intel to Chairman Blumenthal, (Jan. 22, 2024); and Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (Mar. 7, 2024), TI_PSI_00000290.

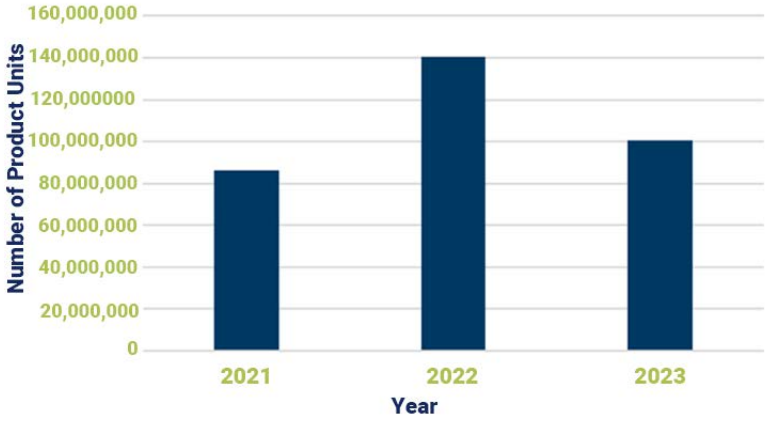
Semiconductor exports to Turkey were 2.4 times greater in 2023 than they were 2021, and increased from 2022:

Figure 7: Number of Exports by Individual Product Units to Turkey, 2021 to 2023



Semiconductor exports to Finland were 1.2 times greater in 2023 than they were 2021:

Figure 8: Number of Exports by Individual Product Units to Finland, 2021 to 2023



The rapid surge in volume of transactions to certain countries has few ready explanations other than the war in Ukraine. Countries such as Kazakhstan, Armenia, and Turkey have been identified by numerous experts as a pathway for Russia's acquisition of battlefield goods despite export controls.[66]

[66] *See* Clarence Leong and Liza Lin, *Russia's Backdoor for Battlefield Goods from China: Central Asia*, WALL STREET J. (Mar. 4, 2024), https://www.wsj.com/world/russias-backdoor-for-battlefield-goods-from-china-central-asia-bd88b546; Nathaniel Taplin, *How Russia Supplies Its War Machine*, WALL STREET J. (Mar. 10, 2023), https://www.wsj.com/articles/russia-ukraine-tech-chips-exports-china-f28b60ca; Georgi Kantchev, Paul Hannon, and Laurence Norman, *How Sanctioned Western Goods Are Still Flowing Into Russia*, WALL STREET J. (May 14, 2023), https://www.wsj.com/articles/how-sanctioned-western-goods-are-still-flowing-into-russia-916db262.

The same cannot be said of the numbers regarding trade with China and Hong Kong, which are orders of magnitude higher than exports to any other country on the list:

Figure 9: Number of Exports by Individual Product Units to China and Hong Kong, 2021 to 2023[67]

	2021	2022	2023
China	18,323,153,534	16,840,358,024	11,718,912,998
Hong Kong	21,206,339,681	17,274,958,990	13,141,110,227

Exports to Hong Kong and China from the Four Companies have decreased year-to-year from 2021 to 2023, but reports regarding Russia's ability to evade U.S. sanctions have repeatedly highlighted Hong Kong and China as the two largest continuing sources of semiconductors to Russia.[68] The number of exports to Hong Kong and China accordingly do not appear to have the same relationship to the war in Ukraine as those of other countries which are part of the Subcommittee's findings: The number of exports to these countries were already exponentially larger than exports to any other country on the Subcommittee's list (China and Hong Kong are among the top destinations globally for U.S. semiconductors), and have decreased as the war has progressed.[69]

B. Texas Instruments, Intel, Analog Devices, and AMD were slow to detect sales of products to entities of concern.

The Subcommittee's inquiry demonstrates that the Four Companies have failed to quickly identify entities of concern due to a lack of proactive efforts at identification. In the first quarter of 2024, BIS provided each of the Four Companies with certain customs data and asked each to check the data against their distribution chain records (including records of direct customers, records of customers of distributors, or records

[67] The Subcommittee summed the number of exports per year across the Four Companies. Letter from Counsel for AMD to Chairman Blumenthal (Mar. 22, 2024), AMD00621 – 45; Letter and Attachment from Counsel for Analog Devices to the Subcommittee (Dec. 22, 2023), Analog_PSI_00000418; Letter and Attachment from Counsel for Analog Devices to the Subcommittee (Feb. 2, 2024), Analog_PSI_00000420; Letter and Attachment from Intel to Chairman Blumenthal, (Jan. 22, 2024); and Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (Mar. 7, 2024), TI_PSI_00000290.

[68] *See, e.g.*, Byrne et al., *In Plain Sight*, *supra* note 17; Bilousova et al., *Challenges of Export Control Enforcement, supra* note 17.

[69] Observatory of Economic Complexity, *Semiconductor Devices in the United States*, OEC, https://oec.world/en/profile/bilateral-product/semiconductor-devices/reporter/usa (last accessed: Sept. 5, 2024).

of additional users down the line if available).[70] This resulted in each of the Four Companies identifying entities within their distribution chain that presented risk of Russian diversion and taking steps regarding ending sales to those entities at BIS's request.[71] Importantly, similar data to that provided by BIS formed the basis of KSE Institute's report in June 2023 and has been integrated into a number of commercial risk management service providers.[72] This means that the Four Companies could have acquired similar data and utilized it themselves prior to the request from BIS if they'd either reached out to KSE Institute after its June 2023 report (as multiple financial institutions did) or utilized the full functionality of commercially available risk management software.[73] Indeed, after receiving this information from BIS, AMD was able to identify 11 additional entities that may be diverting its products to Russia by running a special report through a global risk analytics program.[74] AMD immediately provided information concerning these 11 entities to BIS after discovering them in June 2024.[75]

While the failure to detect these entities earlier at AMD, Analog Devices, and Intel may stem from a failure to use the full functionality of risk management software, the failure at Texas Instruments seems attributable to its decision to only use commercially available risk management databases significantly later in the customer screening process, and sometimes not at all. Unlike the three other companies, Texas Instruments does not appear to incorporate any of these databases into its initial customer screening: it simply screens its customers against a consolidated list of all U.S. and non-U.S. restricted parties, and "manual lists" of additional entities to not sell to that appear to rely largely on reports from law enforcement, red flags raised during the course of Texas Instruments' interactions with the business, and media reports.[76] Only if there is a potential hit on an entity based on these methods of screening does Texas Instruments have its employees or contractors use modern risk analytics software to investigate that entity, and even then not always.[77] Modern risk analytics software utilizes many more sources than those relied upon by Texas Instruments in making its "manual lists"—including, for example, corporate structures and customer relationships of Russian military-end use entities, trading partners, and distribution

[70] Briefing from BIS to the Subcommittee (July 18, 2024).

[71] *Id.*

[72] Briefing from KSE Institute to the Subcommittee (Nov. 9, 2023); Briefing from BIS to the Subcommittee (July 18, 2024); Bilousova et al., *Russia's Military Capacity*, *supra* note 17.

[73] PSI February 2024 Hearing, *supra* note 16.

[74] Letter and Attachment from Counsel for AMD to Chairman Blumenthal (July 12, 2024), AMD002652—AMD002671.

[75] *Id.*

[76] Letter from Counsel for Texas Instruments to Chairman Blumenthal (March 8, 2024).

[77] *Id.*

chains.[78] Failing to use this type of software to screen all customers likely exposes Texas Instruments's distribution chain to heightened risks of diversion not present at the other companies.[79]

The failure to quickly detect sales to entities of concern at Texas Instruments may also be due in part to lax controls on online direct sales. Texas Instruments does not appear to require that customers provide an end-user for direct sales on its website, allowing individuals and entities to purchase semiconductors without requiring any attestation for whom these are ultimately intended—complicating tracing efforts. In at least one instance, BIS provided Texas Instruments with information regarding purchases made from its website by an individual who appeared to be involved in Russian diversion efforts and asked company personnel whether they could provide any sort of end-user information regarding these products, presumably so that BIS could trace the path of these products to Russia.[80] Texas Instruments could only provide BIS with the certifications required for online purchases, which simply include a check-box asking an individual to confirm that they are not a military end user or that the product is not for military end use.[81]

C. Significant gaps remain in Texas Instruments, Intel, Analog Devices, and AMDs' export control compliance policies and procedures.

The Subcommittee's review of each of the Four Companies' export control compliance programs demonstrated that significant gaps remain that could allow their products to reach suspicious or flagged entities. While each company's export control compliance policies varied, the Subcommittee found that each of the Four Companies: (1) failed (other than AMD) to provide timely responses containing operational information to organizations focused on tracing the flow of U.S.-manufactured semiconductors to Russia; (2) failed to annually conduct comprehensive audits of their own internal export control processes; and (3) failed (prior to the Subcommittee's inquiry) to

[78] *See, e.g*, Kharon, *Data-Russia*, https://www.kharon.com/data/russia.

[79] Texas Instruments provided additional information to the Subcommittee on Sunday, September 8 noting that it also uses data maintained by the Trade Integrity Project to screen customers. Email from Counsel for Texas Instruments to the Subcommittee (Sept. 8, 2024). It is unclear at what stage of the screening process Texas Instruments uses this data, and whether it is used to screen all customers. Further, the Trade Integrity Project only became available earlier this year, suggesting that this is a very recent addition to Texas Instruments's customer screening. *See infra* Section III.C.

[80] Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (Mar. 22, 2024), TI_PSI_00000303.

[81] *Id.* Texas Instruments noted to the Subcommittee that its website also communicates the requirements of the EAR with respect to end user and end use, and requires acceptance by the customer. Email from Counsel for Texas Instruments to the Subcommittee (Sep. 8, 2024).

routinely audit the export control policies and procedures of all of their distributors yearly.[82]

i. Analog Devices, Intel, and Texas Instruments provided insufficient responses to external tracing efforts showing their products in Russian weapon systems.

Intel, Texas Instruments, AMD, and Analog Devices have all received trace requests from external groups showing that their semiconductors have been found in Russian weapon systems.[83] Responses from Intel, Texas Instruments, and Analog Devices to these trace requests, which seek to help understand how Russia is continuing its war efforts in Ukraine, have been delayed, nonresponsive, or nonexistent.[84] A trace request is sent to a company after an external tracing organization believes that it has identified a company's product in a downed Russian weapon, such as a drone or other device.[85] Trace requests are critical in preventing diversion as they involve efforts at charting the path of specific U.S.-manufactured semiconductors that end up in Russian weapons and helping governments block sales to the entities that helped facilitate those sales.[86] Recovered weapons are analyzed by manufacturer, model number, and any other readily identifiable markings to discover the path that each specific component took to

[82] The Subcommittee's inquiry analyzed the export control compliance programs at each of the Four Companies based on standards and recommendations set forth by BIS and advocated for by non-governmental organizations. The Subcommittee looked at the following aspects of each of the Four Companies' export control compliance programs: (1) BIS review of export control plan since February 2022; (2) evidence of internal leadership structure specifically for export control; (3) specific policies and procedures related to export control; (4) requirements for customers and distributors, including customer/distributor outreach explaining expectations for compliance; (5) "Know-Your-Customer" and Due Diligence Processes; (6) Maintenance of an internal "Do-Not-Sell"-type list and appropriate standards for the list; (7) Employee training on export controls; (8) responsiveness to external tracing efforts; (9) routine audits of export controls processes and implementation of corrective action; (10) routine audits of distributor export control processes and processes for corrective action.

[83] Letter and Attachment from Counsel for AMD to the Subcommittee (June 18, 2024), AMD000700-AMD000709; Letter from Conflict Armament Research to Chairman Blumenthal (Mar. 26, 2024); Intel, *Intel CAR Trace Request 3.*3, (Apr. 12, 2024); Intel, *Intel CAR Trace Request 1.*3, (Apr. 12, 2024); Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (July 22, 2024), TI_PSI_00001450 to TI_PSI_00001601; and *id.* at TI _PSI_00001711 to TI_PSI_00001796.

[84] Based on Subcommittee analysis discussed below.

[85] PSI February 2024 Hearing, *supra* note 16; Conflict Armament Research appears to be the principal external organization utilizing trace requests in the war in Ukraine. It works directly with the Ukrainian military to acquire and analyze downed Russian weapons. *Id.* It employs a methodology endorsed by the European Union and the State Department and has been charged by the European Union with the maintenance of iTrace, a global information management system on diverted or trafficked conventional arms and their ammunition. *Id.* Its work has resulted in the identification and addition of new entities to the Entity List and similar sanctions lists in other countries. *Id.*

[86] *Id.*

end up in a Russian weapon.[87] Receiving any information the manufacturer has about end users, distributors, and batch numbers are critical to these efforts.

Responsiveness to tracing requests is one critical way that entities involved in transshipment to Russia can be identified. Their importance supersedes the war in Ukraine, however, as U.S. adversaries worldwide have been shown to take lessons from other's successes in evading export control restrictions.[88] Damien Spleeters from CAR testified at the Subcommittee's February 27, 2024 hearing that CAR had recently found a North Korean missile in Ukraine containing a majority of U.S. components, and that CAR's work suggested North Korea and Iran utilized the global semiconductor market to evade restrictions in a manner similar to Russia.[89] These efforts will only increase in intensity as export controls grow in use as a tool of national security.

The Subcommittee's inquiry found that Analog Devices has not engaged with CAR to conduct requested trace requests as of March 2024.[90] CAR has sent Analog Devices 20 trace requests since the outbreak of the war in Ukraine.[91] Records provided to the Subcommittee do not show any rationale behind Analog Device's decision to not engage with CAR.[92]

Texas Instruments has not responded to any trace requests as of July 18, 2024, and only began to take substantive action to respond to external tracing organizations after the Subcommittee noticed a hearing which included a CAR witness.[93] Records obtained by the Subcommittee demonstrate that, since Russia's invasion of Ukraine, Texas Instruments received over 100 trace requests dating back to August 2022.[94] These included requests for more information about Texas Instruments's products found in downed Russian drones,[95] Russian cruise missiles,[96] and other Russian missiles which had been used on the battlefield in Ukraine and whose pieces had been recovered by the Ukrainian military.[97] Texas Instruments did not respond to the substance of its trace requests until February 2024.[98] Records obtained by the Subcommittee

---

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] Letter from Conflict Armament Research to Chairman Blumenthal (Mar. 26, 2024).

[91] *Id.*

[92] *Id.* Analog Devices informed the Subcommittee that "after learning that CAR is a trusted partner of the USG, ADI reached out to CAR in July 2024 to better understand its partnership with the U.S. government and ask CAR to re-send its requests." Email from Counsel for Analog Devices to the Subcommittee (Sept. 4, 2024).

[93] Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (July 22, 2024), TSI_PSI_00002244; and *id.* at TI_PSI_00002248-00002249.

[94] *Id.* at TI_PSI_00001450 - TI_PSI_00001601; and *id.* at TI _PSI_00001711- TI_PSI_00001796.

[95] *Id.* at TI_PSI_00001656-1657.

[96] *Id.* at TI_PSI_00001666-1667; and *id.* at TI_PSI_00001668-1669.

[97] *Id.* at TI_PSI_00001672-1673.

[98] *Id.* at TSI_PSI_00002244; and *id.* at TI_PSI_00002248-00002249.

demonstrate that since the Subcommittee's February hearing, Texas Instruments has undertaken research to locate information responsive to pending trace requests.[99] However, it appears that, as of July 18, 2024, Texas Instruments has not provided any responses to CAR concerning its internal findings.[100]

It took AMD 3 to 4 months to respond to trace requests. When they were provided, they included important information including the manufacture date and, for those products where it was available, date of shipment, distributor the shipment was sent to, and end user for whom the product was intended. Responses provided to the Subcommittee by AMD including information of this nature were sent on March 7, 2024 in response to 16 trace requests made in November 2023, and in early June 2024 in response to 7 trace requests made in late March 2024.[101]

Intel has been inconsistent in its response to external trace requests. While the number of trace requests submitted to Intel is unclear, records produced to the Subcommittee demonstrate that it has responded to 31 trace requests received since the Russian invasion of Ukraine.[102] These include for example, requests for more information about Intel and Altera (acquired by Intel in 2015) products found in a downed Russian helicopter, downed Russian cruise missiles, and other Russian missiles used on the battlefield in Ukraine and whose pieces were recovered by the Ukrainian military.[103] The timeliness of Intel's responses to trace requests varied from 1 month to 14 months; with more than two-thirds of Intel's responses taking 6 months or longer.[104] While Intel responded to inquiries from CAR, the utility of the information provided is unclear.[105] For example, in response to a request for information on distributors to help determine chain of distribution, Intel simply pointed to the list of all authorized distributors that could be found on Intel's public facing website.[106]

---

[99] *Id.* at TI_PSI_00001809.

[100] *See id.* at TI_PSI_00001809.

[101] Letter and Attachment from Counsel for AMD to the Subcommittee (June 18, 2024), AMD000700-AMD000709.

[102] Intel, *Intel CAR Trace Request 3.*3, (Apr. 12, 2024).

[103] *Intel Completes Acquisition of Altera: Altera Now Part of Intel*, (Dec. 28, 2015), https://www.intc.com/news-events/press-releases/detail/302/intel-completes-acquisition-of-altera; Intel, *Intel CAR Trace Request 3.*3, (Apr. 12, 2024); and Intel, *Intel CAR Trace Request 1.*3, (Apr. 12, 2024).

[104] The Subcommittee calculated the number of months for Intel's response by comparing the date trace requests were received to when a response was provided. Intel, *Intel CAR Trace Request 3.*3, (Apr. 12, 2024).

[105]Intel, *Intel CAR Response 1.2*, (Apr. 12, 2024).

[106] Intel, *Intel CAR Response 1.2*, (Apr. 12, 2024).

ii. None of the Four Companies conduct sufficient internal auditing for export controls.

AMD, Texas Instruments, Intel, and Analog Devices all fail to maintain audit programs that analyze their entire export control compliance programs on a yearly or more frequent basis. All (except for Analog Devices) fail to maintain a program that has more regular, targeted audits of specific export control processes. This is contrary to BIS's recommendation that companies audit their entire export control compliance program annually and conduct more frequent, targeted auditing of specific areas of the export control compliance process.[107]

Regular internal auditing is critical to identifying and eliminating deficiencies in day-to-day processes that can lead to products being shipped to entities involved in transshipment. The Subcommittee's inquiry found that, when companies did perform audits, they identified areas of risk which could have been addressed sooner had more routine audits taken place. This was true at both Analog Devices and Texas Instruments, which since Russia's invasion undertook a stand-alone review of its entire compliance program (Analog Devices) and a stand-alone review of its internal processes for preventing sales to restricted parties and certain additional aspects of its compliance program (Texas Instruments). These audits both led to significant findings and corrections:

- Analog Devices' review of its entire export control compliance program identified sales by brokers to distributors, resale of products on the open market, and resale of products on third party websites as posing significant risks of diversion.[108] Analog Devices addressed these risks by prohibiting these types of sales, creating red flag policies, and forming a Grey Market Mitigation Team to proactively analyze point-of-sale, end customer backlog, and inventory data for red flags and prevent these questionable transactions.[109]

- Texas Instruments's audit identified three areas that could potentially lead to Texas Instruments' products being sent to an entity despite that entity being on either a sanctioned list or one of Texas Instruments' internal do-not-sell lists.[110] The audit offered corrective action to remedy each issue, and records provided to the Subcommittee indicate that corrective action to address these issues was intended to be completed by September 30, 2023.[111]

---

[107] BIS, *Export Control Guidelines*, *supra* note 43.

[108] Letter from Counsel for Analog Devices to the Subcommittee (Jun. 4, 2024).

[109] Letter from Counsel for Analog Devices to the Subcommittee (Apr. 22, 2024).

[110] Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal (June 14, 2024), TI_PSI_1408-1409.

[111] *Id.*

Despite the plain benefits identified by the stand-alone audits detailed above, none of the Four Companies presently has an internal audit program which annually audits its full export control program:

- AMD's program is the most lacking, as it does not have a system for conducting routine, annual audits of its own internal export controls.[112] AMD explained that its audits are designed to address specific issues or risks, and it has not audited its internal compliance department since Russia's invasion of Ukraine because it has not identified any specific issues or risks.[113]

- Texas Instruments has no annual program in place to audit its entire export control program and has not conducted such an audit since Russia's invasion of Ukraine.[114] Texas Instruments did conduct the stand-alone audit described above and explained that its Global Trade Compliance (GTC) organization, which houses the committee responsible for overseeing export controls, conducts formal reviews of each of Texas Instruments' 15 GTC sites worldwide to assess the effectiveness and operation of each site's compliance program at a defined interval.[115] Information provided to the Subcommittee shows that, from January 1, 2022 to September 15, 2023, Texas Instruments reviewed less than one-third of its 15 GTC sites.[116]

- While Intel stated that it "conducts multiple audits and self-assessments each year to evaluate Intel's trade compliance policies and procedures," it is not clear whether they have performed an audit of their export program in the two-and-a-half years since Russia's invasion of Ukraine.[117]

- Analog Devices has the most robust program of any of the companies, but it does not conduct annual, comprehensive, audits of its export control program.[118] Analog Devices audits aspects of its compliance program on a quarterly basis with the goal of reviewing the entire program annually,

[112] Letter from Counsel for AMD to Chairman Blumenthal (April 26, 2024); Briefing from AMD to the Subcommittee (June 21, 2024).

[113] Letter from Counsel for AMD to Chairman Blumenthal (April 26, 2024); Briefing from AMD to the Subcommittee (June 21, 2024).

[114] *See* Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal, (Apr. 26, 2024), TI_PSI_00001400 to TI_PSI_00001403.

[115] Letter from Counsel for Texas Instruments to Chairman Blumenthal (Oct. 25, 2023).

[116] Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal, (Apr. 26, 2024), TI_PSI_00001400 to TI_PSI_00001403.

[117] Letter and Attachment from Intel to Chairman Blumenthal (Apr. 1, 2024).

[118] Call between Counsel for Analog Devices and the Subcommittee (Sept. 5, 2024).

but does not conduct any comprehensive annual review.[119] It also reviews its procedures whenever there is a change to a legal regulation or policy.[120]

Stand-alone audits such as those done by Analog Devices and Texas Instruments, while better than nothing, are inadequate to address rapidly changing export controls meant to counteract new efforts by adversaries such as Russia and China to acquire critical U.S. technology. BIS has adopted new enforcement mechanisms over the last 15 years to confront new challenges—including the increase use of FDPRs,[121] and requests for companies to increase their proactive compliance after BIS provides them supplier lists and red flag letters.[122] BIS directly cautions companies to this reality, explaining that "export compliance managers will need to keep the program dynamic – altering the program with changes in operations, products, and export control regulations."[123] These dynamic changes require regular audits to assess the effectiveness of new processes and check for inconsistencies between those processes and day-to-day operations.[124]

iii. None of the Four Companies presently audits all of its distributors for export controls on a yearly basis.

The Subcommittee found that Intel, Texas Instruments, AMD, and Analog Devices do not presently audit the export controls for all of their distributors on a yearly basis. Texas Instruments and Intel do not conduct routine audits of their distributors for export controls at all. Analog Devices and AMD audit their distributors' export controls, but using different approaches and different levels of frequency. Last week, Analog Devices informed the Subcommittee that it now intends to invest in a further team expansion for fiscal year 2025 to enable it to audit all of its distributors' export controls annually.[125]

Routinely auditing export control compliance processes in place at distributors is important for the same reasons that companies should routinely audit their own internal export compliance controls. U.S. manufacturers' responsibility to ensure their products

---

[119] *Id.*

[120] *Id.*

[121] *Chains of Control: The History and Limits of America's Favourite New Economic Weapon*, *supra* note 52.

[122] BIS, *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*, U.S. DEP'T OF COMMERCE (July 10, 2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

[123] BIS *Export Control Guidelines*, *supra* note 43.

[124] *Id.*

[125] Email from Counsel for Analog Devices to the Subcommittee (Sept. 4, 2024).

do not wind up being diverted to Russia, China, or other adversaries does not end when they are sent to a distributor—the EAR defines a knowing violation of export controls to include not only positive knowledge, but also "an awareness of a high probability of its existence."[126] And the EAR permits the inference of such awareness from "evidence of the conscious disregard of facts" or "willful avoidance of facts."[127] Companies who continue to send products to distributors who have inadequate export controls compliance may be in violation of law. Further, if (as each of the Four Companies has explained to the Subcommittee) transshipment is not principally the result of direct customers of U.S. manufacturers providing goods to illicit actors, it must come from customers of customers. Therefore, it is important that manufacturers know that their distributors have in place appropriate export control compliance (including providing manufacturers with accurate end-user information) to protect distribution chains from illicit diversion.

Texas Instruments does not conduct routine audits of its distributors regarding export controls and has not conducted any such audits since Russia's invasion of Ukraine despite evidence of potential transshipment.[128] Texas Instruments' distributor agreements include export control provisions and permit Texas Instruments to audit for compliance and conduct routine business audits of its distributors, including annual inventory audits.[129] But audits for particularized issues such as export control compliance are considered through a risk assessment process and only occur only if a heightened or particularized concern about a distributor is raised or observed.[130] Records provided to the Subcommittee show that Texas Instruments was given information concerning potential diversion to Russia at one of the customers of its largest worldwide distributor in July 2023, but never conducted an audit of the distributor despite this evidence.[131] This information, which was sent to a Senior Investigator at Texas Instruments via email, included the names of the specific part families being diverted, the companies they were meant for, and pictures of boxes of shipments which the reporting individual stated were destined for Russia.[132] Texas Instruments investigated this communication and ultimately blocked the customer (as did its largest distributor), but this incident did not trigger an audit for export control compliance at Texas Instruments' largest distributor.[133]

Intel also does not conduct routine audits of its distributors regarding exports controls, and has not provided records or information to the Subcommittee demonstrating that

[126] 15 C.F.R. § 772.1.
[127] 15 C.F.R. § 772.1.
[128] Letter from Counsel for Texas Instruments to Chairman Blumenthal (June 7, 2024).
[129] *Id.*
[130] *Id.*
[131] Letter and Attachment from Counsel for Texas Instruments to Chairman Blumenthal, (May 30, 2024), TI_PSI_00001367_T - TI_PSI_00001375_T.
[132] *Id.*
[133] Email from Counsel for Texas Instruments to the Subcommittee (Sept. 3, 2024).

any distributor audits since Russia's invasion of Ukraine included review of export controls.[134] Intel stated that it "conducts regular audits of our distributors to ensure compliance with contractual terms and conditions, pricing agreements, and other commercial matters. While the primary purpose of the audits is not focused on export compliance, it is a component of the auditor's review."[135] However, Intel also stated to the Subcommittee that not every distributor audit includes a review of a distributor's export controls.[136] It is unclear from documents produced to the Subcommittee the extent to which there are audit procedures, if any, specifically geared towards export controls, or if detection of possible export control issues relies upon auditors recognizing red flags as they execute commercially focused procedures.[137] Further, it is unclear how many, if any, audits of distributors conducted by Intel since the Russian invasion of Ukraine have touched on export controls, and what, if any, corrective actions were identified.[138]

AMD and Analog Devices both include export controls as a portion of all of their distributor audits, but do not presently audit all of their distributors yearly. Analog Devices made the decision to include a review of export controls as a portion of its distributor audits following Russia's invasion of Ukraine;[139] AMD decided to expand the export control portion of its distributor audits in the fall of 2023.[140] This timing suggests both companies view an enhanced look at distributors' export controls as an important tool to prevent Russian diversion efforts. While the Subcommittee understands the commercial sensitivity behind revealing exact audit frequency, neither AMD nor Analog Devices audited all of their distributors' export controls yearly prior to the Subcommittee's inquiry—last week, Analog Devices informed the Subcommittee that it intends to do so beginning in fiscal year 2025.[141] An AMD audit official who briefed PSI acknowledged that distributor audits are "not difficult" and are "scripted," suggesting AMD could conduct more distributor audits every year and accordingly audit

[134] The Subcommittee reviewed representations made, and documents produced by Intel regarding export controls.

[135] Letter and Attachment from Intel to Chairman Blumenthal at Appendix 5 (May 31, 2024).

[136] Call between Intel and the Subcommittee (May 7, 2024).

[137] Briefing from Intel to the Subcommittee, (Feb. 20, 2024); Intel, *Distribution Flow of Product: Ecosystem, Reporting, Audit Rights* (Feb. 20, 2024); Letter from Intel to Chairman Blumenthal the Subcommittee, at Appendix 1 (Apr. 1, 2024); Letter from Intel to Chairman Blumenthal, at Appendix 3 and Appendix 5 (May 31, 2024).

[138] Briefing from Intel to the Subcommittee, (Feb. 20, 2024). Intel, *Distribution Flow of Product: Ecosystem, Reporting, Audit Rights* (Feb. 20, 2024); Letter from Intel to the Subcommittee, at Appendix 1 (Apr. 1, 2024); Letter from Intel to the Subcommittee, at Appendix 3 and Appendix 5 (May 31, 2024).

[139] Letter from Counsel for Analog Devices to the Subcommittee (Jun. 4, 2024).

[140] Briefing from AMD to the Subcommittee (June 21, 2024); Letter from AMD to Chairman Blumenthal (April 26, 2024).

[141] Briefing from AMD to the Subcommittee (June 21, 2024); Briefing from Analog Devices to the Subcommittee (May 6, 2024); Email from Counsel for Analog Devices to the Subcommittee (Sept. 4, 2024).

its distributors more frequently.[142]

In addition to its standard distributor audits, AMD, unlike the other three companies, has informed the Subcommittee that it intends to undertake an audit looking at a specific export compliance issue across all distributors. AMD intends to audit end-user assessments (i.e. who its distributors sell to and the policies and procedures in place to check those entities) across all its distributors at some point in 2024.[143] AMD made the decision to add this audit in November 2023.[144] AMD presently intends that this will be a stand-alone audit rather than an audit conducted on a routine schedule, although it has not yet finalized its audit plans for 2025.[145]

D. Semiconductor manufacturers have not sufficiently increased their export control compliance efforts since Russia's invasion of Ukraine.

In addition to the specific issues identified in the Four Companies' compliance programs, the Subcommittee's inquiry found that semiconductor manufacturers have not sufficiently increased their compliance efforts fast enough or substantively enough to combat increased diversion risks following Russia's invasion of Ukraine.

i. Semiconductor companies remain less diligent at targeting illicit transactions than the financial sector.

As noted above, Ms. Ribakova of KSE Institute testified at the Subcommittee's February 27, 2024 hearing that, when her organization released its first report in June 2023 detailing semiconductor companies (including the Four Companies) whose products had ended up in Russia, no semiconductor companies reached out to find out more about the data her organization utilized or ask for any further information about the diversion of their products.[146] By contrast, multiple financial institutions proactively reached out to find out if KSE Institute's data might help them discover suspicious financial transactions.[147]

Ms. Ribakova emphasized her opinion that semiconductor manufacturers must catch up to the financial sector, and a comparison shows where the semiconductor industry still

[142] Briefing from AMD to the Subcommittee (June 21, 2024).
[143] Letter from Counsel for AMD to Chairman Blumenthal (April 26, 2024).
[144] Briefing from AMD to the Subcommittee (June 21, 2024).
[145] *Id.*
[146] PSI February 2024 Hearing, *supra* note 16.
[147] *Id.*

falls short.[148] Bank Secrecy Act/Anti-money (BSA/AML) laundering requirements mandate corporate monitoring of transactions that go through many hands—and, similar to semiconductors, are highly fungible.[149] Under BSA/AML requirements, financial institutions are required, for example, to implement appropriate risk-based customer due diligence procedures; and "maintain written, board approved compliance programs designed to provide reasonable assurance and monitor compliance with regulatory requirements".[150] Financial institutions subject to BSA/AML are also required to file Suspicious Activity Reports for known or suspected violations of law or suspicious activity observed.[151] Penalties for violations by financial institutions can be substantial: in 2013 The Financial Crimes Enforcement Network (FinCen) and the Office of the Comptroller of the Currency each assessed a $37.5 million penalty against TD Bank for failing to detect and report suspicious activities in a timely manner.[152]

Elements of such a regulatory framework are in place for semiconductor companies to take similar steps. For example, in June 2022, BIS and FinCEN issued a joint notice to financial institutions urging increased vigilance for potential Russian export control evasion attempts.[153] The notice included multiple "behavioral red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion."[154]

---

[148] *Id.*

[149] The Anti-Money Laundering Act of 2020 amends and builds upon the existing anti-money Laundering statutory framework that was established under the Bank Secrecy Act in 1970. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2022, Pub. L. No.116-283 Bank Secrecy Act, Pub. L. No. 91-508.

[150] U.S. Gov't Accountability Off., GAO-20-574, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks' Costs to Comply with the Act Varied* (2020) https://www.gao.gov/assets/d20574.pdf.

[151] FinCEN, *Guidance on Preparing a Complete & Sufficient Suspicious Activity Narrative*, U.S. DEP'T OF THE TREASURY (Nov. 2003), https://www.fincen.gov/sites/default/files/shared/sarnarrcompletguidfinal_112003.pdf.

[152] Alma Calcano, *History Repeats Itself, Especially When You Ignore It: A 10-Year Look Back At BSA Enforcement Actions*, NAT'L ASS'N OF FEDERALLY INSURED CREDIT UNIONS (July 19, 2019), https://www.nafcu.org/compliance-blog/history-repeats-itself-especially-when-you-ignore-it-10-year-look-back-bsa-enforcement-actions.

[153] FinCEN & BIS, *FinCen & BIS Joint Alert: FIN-2022-Alert003*, U.S. DEP'T OF THE TREASURY and U.S. DEP'T OF COMMERCE (June 28, 2022), https://www.fincen.gov/sites/default/files/202206/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf.

[154] *Id.*

ii. Policy changes at certain companies show that semiconductor manufacturers can do more.

The Subcommittee also found that certain companies have more proactive anti-diversion policies which others could adopt but have not. As noted above, Analog Devices added a Grey Market Mitigation Team and made the decision to limit certain sales following its post-invasion review of its compliance program. Analog Devices informed the Subcommittee that the Grey Market Mitigation Team blocked $66 million of sales in Fiscal Year 2023 as a result of screening customers.[155] Analog Devices has also halted sales to brokers and resellers, as well as sales through third-party websites—entities which Analog Devices determined pose a higher risk for diversion.[156]

Actions taken in the year since the Subcommittee launched its inquiry also point to the finding that each of the Four Companies can be doing more to proactively combat Russian diversion. In the last year:

- Officials from BIS officials and the Departments of State and Treasury met with the CEOs of the Four Companies in early 2024 and asked them to take specific, concrete steps to stem Russian diversion efforts, such as providing the Four Companies with certain customs data and asking them to compare it to the entities in their respective systems.[157] As noted above, this effort led to the halting of sales to entities at all Four Companies. BIS officials informed Subcommittee staff that all Four Companies have begun taking action on this and the other steps requested.[158]

- Texas Instruments began engaging with CAR on tracing efforts shortly after the Subcommittee's February 27, 2024 hearing, after having been unresponsive to those efforts for over a year.[159]

- Intel stated to the Subcommittee that new export control policies are under review that will become company policy.[160]

- AMD decided in the late summer and fall of 2023 to add expanded export

[155] Letter from Analog Devices to Chairman Blumenthal (April 22, 2024).
[156] Briefing from Analog Devices to the Subcommittee (May 6, 2024).
[157] Briefing from BIS to the Subcommittee (July 18, 2024).
[158] *Id.*
[159] Letter and Attachments from Counsel for Texas Instruments to the Subcommittee (July 22, 2024), TSI_PSI_00002244; *Id.* TI_PSI_00002248-00002249.
[160] Call between Intel and the Subcommittee (Jun. 20, 2024).

control compliance questions to all of its distributor audits.[161] AMD also decided in November 2023 that it would conduct a stand-alone, focused audit to closely analyze whether its distributors are sending its products to the resale customers they represent to AMD.[162]

- Last week, Analog Devices informed the Subcommittee that it plans to invest in a further expansion of its team for fiscal year 2025 to enable it to audit all of its distributors' export controls annually.[163] Analog Devices is also seeking an independent third-party assessment of its export compliance program in fiscal year 2025.[164]

[161] Letter from AMD to Chairman Blumenthal (April 26, 2024); Briefing from AMD to the Subcommittee (June 21, 2024).

[162] *Id.*

[163] Email from Counsel for Analog Devices to the Subcommittee (Sept. 4, 2024).

[164] *Id.*

PART III: RECOMMENDATIONS

The four companies reviewed by the Subcommittee are some of the largest and most profitable semiconductor companies in the United States, with un-tapped and underutilized resources that could improve their export compliance. The findings about these companies are unlikely to be unique in the industry. Rather, they were selected to demonstrate problems faced by other semiconductor manufacturers in an ever-changing industry with an ever-evolving landscape of export controls. The Subcommittee's findings show that it is critical that the semiconductor industry, writ large, take concrete steps to improve their export compliance. The national security threats posed by Russia's invasion of Ukraine do not exist in a vacuum. They are just one example of how other adversaries can, and do, exploit gaps in our export controls to use U.S. technology for their gain.

The Subcommittee makes the following recommendations.

A. Semiconductor manufacturers should respond to external tracing efforts thoroughly and in a timely manner.

External tracing assists governments across the globe with finding and preventing the ongoing diversion of needed components for weapons. Despite the importance of this work, of the Four Companies, only AMD had provided responses of any utility based on records provided to the Subcommittee.[165] Since the Subcommittee's February 27, 2024 hearing, the engagement and utility of the Four Companies' responses shows some improvement, however, more is needed.[166]

Nongovernmental organizations have a critical role in the effort to combat Russian diversion given their access to unique data and/or firsthand evidence of the appearance of U.S.-manufactured semiconductors in Russian weapons. Successful efforts to find and combat Russian diversion require substantive and timely engagement from semiconductor manufacturers whose products are found in Russian weapons. Increased engagement by companies should continue to help identify and block off new paths for U.S.-manufactured semiconductors to make it to Russia.

[165] *See supra* Section II.C.i.
[166] *Id.*

B. Semiconductor manufacturers should annually audit their entire export controls compliance programs, and audit targeted processes more frequently—particularly when problems arise or regulations change.

As noted above, BIS's *Export Control Guidelines* recommended that companies annually audit their entire export control programs, with smaller, more frequent audits focused on discrete pieces of the export control program.[167] None of the Four Companies provided the Subcommittee with records or information showing that it has such an audit program in place.[168] The issues identified and corrected by the stand-alone audits conducted by Analog Devices and Texas Instruments show the utility of auditing, but the changing nature of export controls means stand-alone audits like these are insufficient.[169] Regular auditing is needed to address new issues in this rapidly evolving space. Semiconductor manufacturers should implement robust audit programs of the type recommended in BIS's *Export Control Guidelines*.

C. Semiconductor manufacturers should implement policies to increase visibility into export controls in their distribution chain, including yearly audits of all of their distributors' export controls compliance.

The Subcommittee's findings demonstrate that the Four Companies lack visibility into the path of their products throughout the whole distribution chain. There is again no reason to believe this problem is limited to these companies. One prominent example of this problem is each company's review and discovery of sales to questionable entities based on certain customs data provided to the companies by BIS in early 2024—data which was otherwise commercially available or that the companies could have readily obtained from, for example, non-governmental organizations.[170]

Modern analytics and data analysis programs that can quickly assess shipping data could and should allow semiconductor manufacturers to more quickly prevent sales to entities of potential concern. Each of the Four Companies (other than Texas Instruments) integrates such software into its standard new customer screening processes, but the discovery of sales to entities of concern earlier this year suggests the semiconductor manufacturers need to work to integrate these systems to review

[167] BIS, *Export Control Guidelines*, *supra* note 43.
[168] *See supra* Section II.C.ii.
[169] *Id.*
[170] *See supra* Section II.B.

records of their existing customers, including the customers of their distributors, as well. Texas Instruments should also adopt modern analytics and data analysis into its standard customer screening.

Cost can no longer be an excuse for failing to integrate at least some of this data. In July of this year, BIS announced that companies should, as a best practice, screen all transaction parties against the Trade Integrity Project (TIP), a new, free resource that identifies third-country suppliers with a history of exporting high-priority items (such as semiconductors) to Russia since its invasion of Ukraine based on public and whistleblower data.[171] The TIP screening tool enables companies to identify possible red flags prior to proceeding with an export transaction that risks diversion to Russia.[172] There is no reason every semiconductor company should not immediately utilize the TIP to screen its entire distribution chain.

Export controls that look at the entire distribution chain also include routine audits of distributors that, in every audit, include an analysis of the distributors export controls utilizing point-of-sale data. None of the Four Companies presently has a distributor audit program which does this frequently enough. Such a program should aim to audit all distributors export controls yearly and include review of point-of-sale data, checking of customers against lists of sanctioned parties or other do-not-sell type lists, and review of compliance agreements and documentation from distributors to evidence due diligence performed on their customers.

D. Semiconductor manufacturers should routinely submit export control plans for review and comment by BIS.

BIS offers to assist companies by having a specialist evaluate their export control plans and suggest areas for improvement, but very few semiconductor companies (and none of the Four Companies) have requested this service since the onset of Russia's war in Ukraine.[173] Specifically, information provided to the Subcommittee shows that for fiscal years 2022 and 2023 BIS only reviewed 4 export control plans for semiconductor-related companies, and that none of the Four Companies sought such a review.[174]

---

[171] BIS, *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*, U.S. DEP'T OF COMMERCE (July 10, 2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf; *Monitoring Military and Dual-Use Trade with Russia*, Trade Integrity Project, https//:trade-integrity.org (last accessed Sept. 5, 2024).

[172] BIS, *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*, U.S. DEP'T OF COMMERCE (July 10, 2024), https://www.bis.gov/sites/default/files/files/Guidance-for-Complying-with-BIS-Letters-Identifying-Transaction-Parties-of-Diversion-Risk_v8.pdf.

[173] Letter from BIS to Chairman Blumenthal (July 3, 2024).

[174] *Id.*

Given the rapidly changing nature of export controls and the fact that semiconductors are among the items at highest risk for diversion, this statistic shows an industry that is not yet focused on proactive improvement of export control compliance.

The Subcommittee's findings show why more semiconductor manufacturers proactively seeking such review would be useful. Many of the flaws identified in the Subcommittee's inquiry are due to policies and practices at the Four Companies which are contrary to BIS's *Export Control Guidelines* or other best practices offered by BIS. 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.[175] The Subcommittee's findings make clear that large semiconductor companies could also benefit from such review.[176] There is no reason to believe this is not true for U.S. semiconductor manufacturers more broadly, and yet only 4 have taken advantage of this free service. Given the significant diversion risks semiconductor manufacturers face from Russia and China, manufacturers should submit their export control plans for BIS review regularly as a check to make sure they are complying with the latest regulations and implementing the most up-to-date best practices.

[175] *Id.*

[176] *See supra* Section II.

CONCLUSION

Semiconductor export controls provide a targeted economic tool allowing U.S. policymakers to exploit U.S. manufacturing dominance to prevent adversaries across the globe from gaining critical military technology. Over the past decade and a half, the increasing recognition of the potential of export controls as a tool of national security has led to their deployment in new and novel ways. DOJ and BIS have repeatedly emphasized that U.S. companies need to enhance their export control compliance programs to keep up with these new regulations.

The Subcommittee's inquiry makes clear that semiconductor manufacturers have not acted quickly and substantively enough despite these warnings. The need for these improvements is critical both in the context of the Russia-Ukraine war, but also given the increasing importance of export controls in constraining China's advances in artificial intelligence. Semiconductor manufacturers need to take further action if the potential of export controls as a national security tool is to be fully realized.