TESTIMONY OF MICHELLE STOUT,
Vice President of Global Trade Compliance and Government Affairs
Analog Devices, Inc.
Before the United States Senate Homeland Security & Government Affairs Committee,
Permanent Subcommittee on Investigations

September 10, 2024

Chairman Blumenthal, Ranking Member Johnson, and members of the Subcommittee, thank you for the opportunity to speak with you today.

My name is Michelle Stout. I am Vice President of Global Trade Compliance and Government Affairs at Analog Devices, Inc. ("ADI"). We appreciate the Subcommittee's focus on the illicit diversion of semiconductors, which we are also focused on and working very hard to prevent.

Let me say at the outset: we are horrified by Russia's invasion of Ukraine. We have Ukrainian employees, including our Chief People Officer and a legal team member whose father rejoined the military after 25 years and came out of retirement to work in a civil service position. At the highest levels of ADI, ensuring that our products are used as intended is not just a legal or commercial matter—it's personal.

We have reviewed our own operations carefully and have found no instance of ADI or our distribution partners diverting products. Let me be clear: if we were to discover instances of diversion, we would immediately take appropriate action. However, all diversion brought to our attention appears to have happened further down the distribution chain.

When we identify conditions that may give rise to diversion, we do what we can to put a stop to them immediately, as detailed below. We hope that this hearing and the Subcommittee's efforts will spark fresh ideas about how we can build upon that work to advance our common goal of stopping bad actors from gaining access to our products.

I. Analog Devices, Inc.

ADI is headquartered in Wilmington, Massachusetts, with sizeable footprints in California, Oregon, Washington, Texas, and North Carolina. We operate across 31 countries, employing approximately 26,000 people worldwide. We sell 75,000 different products to about 125,000 customers.

ADI combines analog, digital, and software technologies into solutions that drive advancements in numerous fields, ranging from automotive and industrial automation systems and consumer electronics to advanced digital healthcare items and digitized factories. Our products are intended to drive solutions needed to create a better society and healthier planet. They are found in airbags, electric vehicles, wind turbines, noise-cancelling headphones, hearing aids, chronic disease

monitoring systems, and smart phones. They help our customers reduce overall operating emissions, increase energy efficiency, and access more real-time insights to monitor environmental impacts. Our products also help connect people around the world. Although most of our business is centered on civilian technology, ADI is a proud partner of the U.S. Department of Defense in its efforts to protect the United States and our allies.

II. ADI's Above-and-Beyond Culture

ADI does not condone product diversion and we are taking industry-leading steps to prevent it. We go above and beyond what the law requires to prevent ADI products from falling into the wrong hands. Going above and beyond what is required is part of our culture. Our approach to compliance is no different. We are committed to compliance with export control laws in the United States and all other countries in which we operate, but we see the laws as a floor, not a ceiling. For example, when Russia invaded Ukraine, we immediately stopped all transactions in Russia, even those still allowed under the law.

As another example, some semiconductor parts are not subject to the U.S. Export Administration Regulations ("EAR") because they are deemed low-tech and do not touch U.S. soil. U.S. companies can legally sell those products to entities on the entity list, and several do, which could be one way semiconductor products make their way to Russia. On my fifth day at ADI, I consulted our Chief Legal Officer, and with full support from our top leadership, including our CEO, we again went beyond what the law requires and did the right thing. We updated our policy and, with just one exception, for which we determined there to be no risk of diversion, instructed our distribution channels to immediately stop selling products not subject to the EAR to companies on the entity list.

ADI was not legally required to change its policy, but we knew that it was the right thing to do, and we didn't hesitate to do it. Following our instructions, our distribution channel partners adjusted their processes and informed us that they had not received similar instructions from other companies. In other words, our instructions were unique.

III. ADI's Export Law Compliance Program

Prior to the Russian invasion of Ukraine, our baseline level of compliance with sanctions and exports controls was already high. We have always been committed to following the law and working to prevent the illicit diversion of our goods. ADI has robust processes, internal policies, controls, and practices to ensure that sales of ADI products comply with export control laws and sanctions in the United States and in other countries in which ADI operates. ADI employees and entities are and always have been strictly prohibited from engaging in transactions that would involve the export, re-export, sale, or transfer of commodities, software, or technology under U.S. jurisdiction to sanctioned or embargoed jurisdictions, individuals, or entities.

To confirm that these controls are working, ADI regularly reviews its own export control compliance program. ADI's Global Trade Compliance Team conducts quarterly functional reviews of its internal trade compliance program with the goal of reviewing the entire program each year. This team also has reviewed the trade compliance programs of several of our distributors and offered suggestions for enhancements. Additionally, given the increased risk of diversion, our Grey Market Mitigation Team regularly reviews distributors' point-of-sale reports for accuracy and red flags. Further, our Internal Audit function, as part of its corporate-wide audit process, audits ADI's distributors across four main areas: (1) revenue recognition, (2) pricing, (3) contract compliance, including compliance with export controls, and (4) inventory management.

If any of these reviews and audits indicate deficiencies in a distributor's export control programs, ADI works with them to enhance their export control programs to meet ADI's high standards.

IV. ADI's Increased Anti-Diversion Efforts

When Russia invaded Ukraine, we recognized the threat of diversion and redoubled our efforts to prevent misuse of ADI products. We have taken the following steps since Russia's invasion to strengthen our anti-diversion efforts:

***First*, ADI fortified its already-robust internal policies, controls, and practices to ensure that sales of ADI products comply with export control laws.** Following Russia's invasion of Ukraine, we enhanced customer screening and our proactive grey market monitoring.

We implemented a "red-flag process" based on guidance from the Departments of Commerce, Treasury, and Justice so our teams can identify and further evaluate transactions that bear indicia of potential diversion. We also prohibit our distributors from selling to resellers, brokers, and freight-forwarders. Although many of those entities are likely not bad actors and it is legal to sell to them, we decided that selling to them was not worth the increased risk of diversion posed by their business models.

Since implementation of our red flag process and restricting sales to resellers, brokers, and freight forwarders, we have denied sales to approximately 5,000 actual and potential customers. Again, not all of these purchasers were confirmed bad actors, and none of them were on the Entity List when we blocked them (some have subsequently been added to the Entity List). In line with our company values, however, we chose to block these lawful transactions.

***Second*, we built our Grey Market Mitigation Team, which is dedicated to enforcing enhanced controls and ensuring that we identify and prevent grey market activities to the best of our ability.** Among other things, the team reviews data sets in conjunction with our data science team to flag impermissible or questionable activity. The team actively monitors the Ukrainian National Agency on Corruption Prevention's War and Sanctions website and database and other resources to identify red flags that raise concerns of potential diversion.

***Third*, we required every employee in the company to take mandatory trainings** that helps them identify potential compliance transgressions and report red flags to the appropriate departments.

***Fourth*, we strengthened our relationship with the Bureau of Industry and Security, Federal Bureau of Investigation, Intelligence Community, and Department of Homeland Security to identify and prevent diversion.** The information exchange between semiconductor companies and our government partners is crucial to our efforts to prevent diversion.

And we are not done. We are always looking for ways to improve our compliance programs. Next year, we will be commissioning an independent audit of our export control compliance programs and will also be expanding our internal audit team to allow us to audit 100 percent of our distribution channel each year.

There is evidence that our efforts and U.S. export controls are working. Non-governmental organizations and think tanks have reported that Russia is having to use extreme measure to get access to U.S. technology and is paying much higher prices to import technology through China and other countries that are facilitating diversion.

V. Recommendations for Improvement

Unfortunately, stopping diversion completely is nearly impossible because of the ubiquity of chips in modern economies, the sprawling global nature of chip markets, and determined efforts by bad actors to circumvent regulations. Semiconductors are the sixth largest U.S. export. In 2023 alone, approximately 900 million units of chips were shipped globally, worth a total of $526 billion. The United States represented $264 billion of that total. In the two prior years, more than 1 billion units were sold. It is crucial that the United States—in close concert with our allies—work to prevent diversion with thoughtful regulations. At the same time, we need to be careful not to overregulate the semiconductor industry, which risks blocking legitimate business, undermining industry, stifling innovation, and working counter to our national security goals and the CHIPS Act.

That said, we know what the stakes are, which is why ADI is a leader in preventing illegal diversion. We are committed to doubling down on our efforts by continuously improving our compliance programs, increasing information sharing, and strengthening our cooperation with the U.S. government and with our European and Asian allies.

We offer five steps the federal government can take right now to help further curtail diversion of restricted technologies to Russia:

1. Increase information sharing between government and industry, focusing on accurate, actionable information that will help industry partners locate and halt sales to bad actors early. ADI is willing to take action, but that's difficult to do when the data we receive is

incomplete, anonymized, or in foreign languages like Russian or Chinese. It would be helpful for the government to provide actionable, translated, and complete information. We know this is a two-way street, and ADI remains committed to sharing information with government agencies like BIS when we identify red flags. Our experience tells us that the Department of Commerce—particularly a sub-agency like BIS or the new Office of Information and Communications Technology and Services—would be an appropriate entity to aggregate information from multiple companies when aggregated information would be useful to help identify trends.

2. Provide early notification about entities of concern. Currently, we only receive notification of entities BIS has placed on the Entity List once it is published. Early notification of entities of concern, even before they are put on the Entity List, would enable companies to engage in early assessment and monitoring of potential red flags.

3. Increase education of online marketplaces so they can automate blocking the sales of products. Online marketplaces play a part in facilitating the grey market when they allow bad actors to post products on their sites for sale. These marketplaces should be held accountable. The current situation of companies having to ask online marketplaces to take down postings on a case-by-case basis is not scalable or efficient (and, often, they push back). Online marketplaces are better positioned than individual companies to solve this problem by automating the removal of problematic postings from their websites in real time. We have had success with addressing diversion through online marketplaces, and we think this solution shows promise on a broader scale, especially when the government gets involved.

4. Provide BIS with additional resources to conduct more oversight in intermediary countries which will allow them to take advantage of cutting-edge tools and conduct more inspections. Additionally, they should conduct more inspections on a surprise basis rather than giving significant advance notice.

5. Work with our allies to implement multilateral export controls, ensuring there are no sales to restricted entities and sanctioned countries from anywhere, not just the United States. Our nation's national security objectives and economic power are undermined when our allies sell to sanctioned countries.

***

This is just the start of our ongoing conversation. As a leader in the effort to prevent illegal diversion of semiconductors, ADI welcomes continued collaboration with our federal government partners, including the Subcommittee, to advance that goal.

I thank the Subcommittee for holding today's hearing, and I look forward to your questions.