Hearing Before the United States Senate
Committee on Homeland Security and Government Affairs
Permanent Subcommittee on Investigations

Testimony of Tiffany Scurry
Chief Compliance Officer
Advanced Micro Devices, Inc.

September 10, 2024

Chairman Blumenthal, Ranking Member Johnson, Members of the Subcommittee: My name is Tiffany Scurry, and I am the Chief Compliance Officer at Advanced Micro Devices, Inc., more commonly known as AMD. Thank you for the opportunity to testify today about the work we are doing to comply with export control and sanctions laws, and our extensive efforts as a company, alongside others, to help prevent our technology from being diverted for prohibited uses. AMD has cooperated extensively with your staff over the past year, and I also want to take a moment to thank them for their hard work.

AMD is a global semiconductor company, founded in 1969. Our strategy is to create and deliver the world's leading high-performance and adaptive computing products across a diverse set of end markets including data centers, client, gaming and a broad range of embedded applications including industrial, healthcare, automotive, aerospace, communications, and networking. We are honored that our products power many essential services and billions of people around the world rely on our technology every day.

As a trained engineer and attorney, I have spent much of my career monitoring and enforcing compliance programs. At AMD, I oversee a global team of highly trained experts responsible for managing and implementing our company-wide ethics and compliance programs. In this role, I also chair AMD's Corporate Compliance Committee.

Today's hearing calls attention to an important issue—namely, efforts to ensure that semiconductors do not find their way into the wrong hands where they may be used for illicit purposes. We appreciate Chairman Blumenthal's continued leadership on this particular issue. With respect to the ongoing conflict, I want to be very clear: We strongly condemn the invasion of Ukraine by Russia, and we stand with those who have been impacted by the war. We ceased all sales to Russia and Belarus soon after the invasion. This swift action was in keeping with our commitment, even pre-dating the invasion, against selling to military end users in Russia. AMD has also created a matching gift program to aid the Ukrainian victims of Russian aggression.

More broadly, we have redoubled our efforts to prevent diversion of our products to Russian weapon systems and are deeply committed to compliance with all export control and sanctions laws. I am especially proud of our collaboration with federal agencies, non-governmental organizations, and others to find new solutions to these challenges.

I. AMD's Comprehensive Compliance Programs

AMD maintains a rigorous export control compliance program, which was developed in accordance with guidance from the U.S. Bureau of Industry and Security ("BIS"). Every single order must pass an export compliance review. We have well-established management policies on global trade compliance, which we regularly review and update, and distribute to all our employees. Each element of our program addresses specific requirements associated with U.S. and international regulations to make sure we export our products consistent with our obligations. Our compliance system also leverages software controls to block prohibited sales, such as to government sanctions lists, as well as controls reflecting bans against exports to certain locations and for specified end-uses.

Additionally, we leverage the latest technology and take a risk-based approach to our compliance efforts. Our goal is to know our customers, and we also gather information on indirect customers with point-of-sale records. Before we consider doing business with any party, we screen them for sanctions issues. We have deployed leading third-party resources—including the same ones trusted by the U.S. government—to scrutinize potential customers. These platforms continually study open-source data to see if it yields new intelligence, and we refresh our systems with their up-to-date findings. If red flags arise, our team conducts enhanced due diligence before taking any further steps. Our checklists include tools to identify company ownership, location information, adverse media, legal actions, and more. When we see parties with whom business would be inconsistent with our standards, we do not complete that sale, even if it would otherwise be permitted under the law. In one instance, as our Global Trade Compliance ("GTC") team was vetting a possible new customer, it revealed that the company was newly formed and had no web presence. Our team recognized those flags as "common practice[s]" for "supplying western parts to Russia." They said no to the sale.

Our GTC team also checks with customers if our products are being sold down the line, and to whom and where. We have ended business relationships with companies that refused to cooperate with those types of questions. In one instance, a company would not, or could not, document how it used the semiconductors that we shipped to it. We stopped selling to that company.

While our Internal Audit team has always regularly tested distributors for appropriate export controls, this year they have amplified our anti-diversion efforts. When we audit a distributor, it has been our practice to have a team inspect the physical site and assess certain transaction data to validate onward sales. Practically, that translates into manual reviews of bills of lading and other paperwork. We inquire into the distributor's own export control team, their training, screening practices, as well diversion risk reviews. Also, for our distributors and foreign customers, we check their compliance with the Annual Letter of Assurance, in which they agree to not transfer our products to proscribed countries, companies or individuals, or military end-users. Our overall audit approach is strong and our metrics show that approach to be true. Additions to the Internal Audit program this year will further enhance our anti-diversion efforts. Based on feedback from the Subcommittee, we will also be conducting an audit of our export control processes in 2025.

At AMD, compliance is an enterprise-wide effort. All of our employees undertake mandatory compliance training on a yearly basis in order to stay current with their export control responsibilities. We also have a core GTC team of specialists around the world who report directly to me and are responsible for our export control policies, processes, and procedures. This team is located in six countries and collectively has decades of experience navigating export compliance regulations—and managing and executing export compliance policies—on a global scale. Since AMD's acquisition of Xilinx in 2022, we have doubled our core GTC team of export compliance specialists and we have plans to continue growing our core team capability to address a global regulatory trade environment that is expanding rapidly in both scope and complexity. GTC also facilitates AMD's compliance with U.S. and global export control regulations through technology controls, business contract requirements, record-keeping, and other measures.

II. Challenges in Stemming and Stopping Diversion

The anti-diversion effort requires many partners to succeed, and there are no easy solutions. We are facing criminal actors intent on subverting U.S. and other laws. Russia appears to be taking a volume approach and has sourced electronic components from numerous companies, with Ukraine listing over 60 manufacturers in its memo to this Subcommittee alone. Adding a layer of complexity, before Russia invaded Ukraine in 2022, there were fully legal sales of semiconductors, that bad actors are now helping Russia to use in its war effort. While AMD strictly adheres to export controls and has always done so, the reality is, there were substantial volumes of components already in the stream of commerce prior to the 2022 invasion. Indeed, when our teams are able to trace the provenance of components backward from the battlefield, the components are typically many years old, or even more than a decade old. The chips that are typically identified are field programmable gate arrays ("FPGAs"), which are sought because they have an unusually long lifespan and can be reconfigured to swap into an entirely different application. In addition to being older chips, many of the chips we have seen are mismarked or counterfeit, making it difficult, or in some cases impossible, to track and gather data.

We appreciate the Subcommittee identifying a number of countries about which it has specific concerns for diversion. We have reviewed our records and for 18 of the 27 figures reported on the Subcommittee's chart detailing sales to select countries, AMD products represent zero of the total number shown, and for two others, AMD products represent only one of the total number shown. For the remaining seven figures, AMD products represent less than 3% of the total number shown—totaling less than 1% in five of those instances.

Diversion also occurs because bad actors use illegal networks to circumvent sanctions. Multiple federal agencies have found these networks through their investigations, and we've reviewed those cases when the prosecutions become public. The federal government has a line of sight into such illegal behavior, illicit supply chains, and related intelligence that is much more comprehensive than our own. When we receive intelligence from the government that we can act on, we do. In addition to working in concert with U.S. authorities, we also coordinate with governments around the world to put a stop to the diversion of our products. This is a global marketplace and we will continue our cooperative efforts to stop and stem the flow of product to the Russian military.

III. AMD's Anti-Diversion Efforts

AMD has no tolerance for the diversion of our products into Russian weapon systems or any other malign use. We take strong steps to prevent it, both internally within AMD and in collaboration with government and non-governmental organization partners. We share the Subcommittee's goal when it comes to Russia: we do not want our products in the hands of the Russian military. To that end, we invest heavily in our diligence efforts to block sales to known bad actors, look for red flags, and share what we find with our regulators and enforcement agencies so they can take action. Additionally, we have hardened our supply chain. We are very focused on this issue across all our products, and we work closely with multiple agencies to continue to look for additional solutions.

In addition to these systemic changes, we have taken proactive steps to further enhance our anti-diversion capabilities:

- First, we have launched an Anti-Diversion Committee that will bring together multiple teams across the company to further strengthen our internal programs and amplify ongoing anti-diversion efforts. The Committee's role is three-fold. It facilitates and supports ongoing investigative work already being undertaken by its members and their staffs into potential unauthorized participants, transactions, product movement and other aspects of our supply chains. By supporting investigative work cross-functionally, our internal investigative efforts will become more coordinated and effective. The Committee also has cross-functional and holistic access to investigative results for collective consideration so that it can better determine potentially effective countermeasures to discourage, prevent or disrupt product diversion and harden our supply chain. Finally, the Committee maintains and fosters organizational awareness and readiness by ensuring the broader AMD workforce remains attuned to export control issues and equipped to recognize and report indications of potential diversion or malign use.

- Second, we are centralizing our intelligence related to anti-diversion findings. In addition to investigations we initiate, we receive information from different sources, such as the news media, law enforcement, and research organizations like Conflict Armament Research. Any time we receive information from an outside source, our procedure is to open an investigation that covers every part, entity, address and other piece of information we are provided. We appreciate the work these organizations are doing, and we make good use of the information they provide.

- Third, we have added to our tool kit. We have increased our investment in additional third-party resources to amplify our due diligence and Know-Your-Customer capabilities. New tools have come on the market in the past 24 months, with the ability to access and interpret global trade data. These are the same tools that the U.S. government uses to drive their investigative efforts, and we are also investing in these tools and bringing them online at AMD.

- Fourth, where regulators have identified actions they believe would be beneficial to slow bad actors, we have made it a priority to undertake those efforts. We have undertaken analyses of entities identified by the government, created blocks in our

system for certain entities and ensured that our distributors did the same, as well as engaged in regular collaboration to bolster efforts against diversion. We have a regular and ongoing dialogue with multiple federal agencies to find additional solutions, as we are always focused on opportunities to do more on this important and challenging issue.

- Fifth, AMD is tied in with and makes referrals to the Disruptive Technology Strike Force and FBI. By way of example, we have shared tips on suspected illegal brokers and while we are not privy to details, we do know that these tips have led to follow-up inquiries from federal law enforcement. Additionally, our Global Trade Compliance and Product Investigation team members routinely attend Strike Force events. Even when it requires travel to do so, we make an effort to attend and stay connected and engaged. AMD is a committed Strike Force partner.
- And finally, we are exploring tech solutions in the design of our products. AMD is investing in research and development to bolster anti-diversion efforts.

We believe our efforts are working, but the scope of the problem is greater than one company alone. The anti-diversion challenge requires many partners to succeed, and we are committed to continued cooperation to stem and stop the flow of products to Russia. We urge other governments around the world to do their part as well. Also, as we have increased our focus on preventing and shutting down potential diversion routes, distributors likewise need to do the same. And finally, we encourage the media and NGOs to continue their investigations, reporting and shining a light in dark corners to expose bad actors.

IV. Conclusion

Thank you again for the opportunity to share this information and I look forward to your questions.