Good morning. Thank you, Chairman Garbarino, Ranking Member Swalwell, and the members of the subcommittee for inviting me here today.

My name is Tim O'Neill and I am the Vice President, Chief Information Security Officer & Product Security, at Hitachi Vantara. Hitachi Vantara is a subsidiary of Hitachi, Limited, a global technology firm founded in 1910 and focused on creating a sustainable society via data and technology. We co-create with our customers to leverage information technology (IT), operational technology (OT), and our products and services to drive digital, green, and innovation solutions for their growth. Our regional subsidiary was established in the U.S. in 1959 and for over 30 years we have heavily invested in U.S. research & development through our 24 major R&D centers that are supporting high-skilled jobs in manufacturing and technology. Our commitment to the U.S. is demonstrated by the establishment of our digital business unit's global headquarters in Santa Clara, California, and we now employ over 16,000 in the U.S. in 30 states and across 60 group companies. North America is our second largest market, representing 17% of our global revenue.

Because of our heavy focus on the intersection of IT and OT technology, one of our major areas of business development and research has been in the industrial Artificial Intelligence (AI) area. This use of AI is often overlooked in favor of conversations about generative AI and ChatGPT; however, industrial AI has the potential to significantly enhance the productivity of U.S. manufacturing and create working environments that benefit employees assembling products. Our co-created AI solutions can address challenges in factories, from the quality of products to the productivity of workers, and respect and address worker concerns on health, safety, discrimination and bias, privacy, and security.

Today's AI systems are tools that workers can use to enhance their job performance. Programs are predicting possible outcomes based on the data being given to them and what the program has been trained to understand as the most likely scenario. That is true of a predictive maintenance solution Hitachi may create for a client to help them more quickly ascertain the likely cause of a breakdown, or of a generative AI system that is predicting what the next sentence could be for a maintenance manual. The system cannot think for itself, and thus humans are necessary to confirm the AI's outcomes or make the ultimate decision. It is like a piece of software that we would use in our jobs to perform a calculation, but just as in the case of an Excel document that is running a formula on a group of cells, it is important for the user to ensure the formula is correct.

The U.S. government has taken a number of positive steps over the last 5 years to promote and further the development of AI. The previous administration laid the foundation with their request to the stakeholder community asking how AI could be used in the federal government. This set the course for the AI standards work that we have seen from the National Institute of Standards and Technology (NIST). The Biden Administration has continued that work with their Blueprint for an AI Bill of Rights, and now this AI Executive Order. We encourage the U.S. to further the development of AI via engagement with international standards setting bodies as well as by reaffirming the U.S.'s commitment to digital trade standards, digital trade titles in treaties like the ones found in the United States-Mexico-Canada Agreement (USMCA), and promotion of digital trade policies in international trade settings.

The AI EO speaks frequently to the necessity of secure AI systems. CISA's core mission focuses on cyber treaties and cybersecurity, making them the obvious agency to take the lead in implementing this part of the EO. As an example, CISA's work on ransomware and the on-going updates and alerts of ransomware attacks has been vital to informing businesses and stakeholders and helping them identify,

defend, and recover from attacks. This same type of threat assessment can be provided for AI. CISA is integral to supporting and providing resources for other agencies on cyber threats and security as those agencies focus on their roles in implementing the EO; this mission is vital to the federal government and where CISA is by far the expert. Other agencies should turn to CISA for this threat identification and cyberthreat detection support.

We applaud the CISA team for their excellent outreach to stakeholders and private industry to understand the implications of security threats and help carry out solutions in the marketplace. Their outreach to the stakeholder community is a model for other agencies to follow. As CISA's expertise lies in assessing the cyber landscape, they are best positioned to support the AI Executive Order and help further development of AI innovation in the U.S. It is also important that CISA recognize the potential benefits AI could pose to critical infrastructure systems to help them identify possible attacks or defend against cyber or physical attacks, and not just on the ways AI could make them vulnerable to failure.

There is great potential for CISA to work across agencies to support or augment their AI work and provide insight into cybersecurity guidance and/or threat identification. CISA is also discouraged against creating separate frameworks, processes, or testbeds and instead should work collaboratively across the federal government to utilize the resources other agencies have, have already, or are currently creating. Manufacturers, especially those who are making products for critical infrastructure industries, have been engaged with their respective agencies and are assisting in the development of AI systems. While some manufacturers may not have engaged with CISA as they implement technology solutions in their operations, as CISA coordinates across agencies to implement the EO, it can broaden its reach to educate all on the crucial role cybersecurity plays in core IT and AI processes.

As an example, the Department of Energy's Cybersecurity, Energy Security, and Emergency Response office (CESER) is charged with overseeing cybersecurity in the electric grid, and thus manufacturers of components for the grid have worked with and continue to engage with CESER. CISA is best served by working with CESER on electric grid AI security issues versus creating a new regime that may duplicate existing work. We envision that CISA would continuously update CESER of threats or security concerns—ongoing or new—that could be used to attack the energy grid, and work with the office to develop guidance to direct manufacturers on how to mitigate potential threats in the manufacturing process.

The Department of Energy (DOE) and the National Science Foundation (NSF) are tasked with creating testing environments for AI systems, including testbeds. CISA, therefore, should avoid creating testbeds and instead work with the DOE and NSF on securing testing environments, including how they are accessed and used, to support their integrity and mitigate potential data manipulation which could compromise the subsequent testing or training of AI systems. CISA should also guide DOE and NSF on specific needs within those testbeds or testing environments to challenge the cyber resiliency of AI systems. This requires CISA's unique expertise, which agencies can lean on versus creating redundant processes or procedures for developers. Continuous evaluation of AI models for CISA should only be focused on the evolving cybersecurity threat landscape.

NIST is tasked with creating and promoting guidelines, standards, and best practice development. To date, it already has a well-established Cybersecurity Framework, the Secure Software Development Framework, and now the AI Risk Management Framework. CISA should encourage use of those existing documents and focus on additional frameworks to address gaps specific to their cybersecurity mandate. There is no need for CISA to create its own risk management or analytical framework for assessing AI

systems. Rather, the agency must work with NIST to promote awareness of emerging threats and ensure that frameworks and testing environments are regularly updated to address them.

Some manufactured products, including Hitachi-produced railcars and energy grid equipment, have been, and will be, in the market for decades. As new technology is incorporated into new products —for example, to assist in creating predictive maintenance schedules to anticipate failures before they happen, or create guided repair solutions to fix equipment issues faster—the future cybersecurity landscape needs to be better understood. CISA can, for instance, facilitate understanding around protecting assets when there are multiple versions of a technology in use at the same time. We believe that CISA's intention to create SBOM toolchains, and the desire to provide information on how AI fits into the Secure by Design program, are valuable avenues to pursue. Manufacturers of AI-enabled equipment, developers of AI programs, and deployers of AI systems must determine mitigation measures to keep the security of their equipment intact throughout its lifecycle. CISA can thus help develop threat assessment guidelines, and the necessary mitigation efforts, to guard against legacy technology becoming a possible gateway for bad actors.

Hitachi certainly supports CISA's ongoing cybersecurity work. CISA's Roadmap for AI has very meaningful areas that can help promote the security aspects of AI usage. We strongly recommend that CISA avoid duplicating the current or tasked work of other agencies as that could create multiple layers that manufacturers would then have to navigate. Such a multi-layered approach would create more harm than good and divert from CISA's well-established and much appreciated position as a cybersecurity leader. It could also create impediments for manufacturers, especially small and medium sized enterprises, from adopting AI systems that would enhance their workers' experience and productivity, improve factory safety mechanisms, and improve the quality of products for customers.

Thank you for your time today. I am happy to answer your questions.