

**Testimony of Assistant Secretary C.S. Eliot Kang
Bureau of International Security and Nonproliferation
U.S. Department of State
Hearing on Emerging Technologies in the Indo-Pacific
House Foreign Affairs Committee
Subcommittee on the Indo-Pacific
January 17, 2024**

Chairwoman Kim, Ranking Member Bera, distinguished members of the subcommittee, thank you for inviting me and my colleagues to testify today.

The mission of the Bureau of International Security and Nonproliferation (ISN) at the Department of State is to prevent, disrupt, and reverse the proliferation of weapons of mass destruction (WMD), associated delivery systems, destabilizing advanced conventional weapons, and related dual-use technologies. The protection of critical and emerging technology is a vital national security issue. These technologies can be used to develop or improve WMD, and other weapons programs and, in the hands of our adversaries, can be used against us; their protection is a national security issue, not a trade one. The promotion of peaceful civil nuclear cooperation is another key component of our mission; it is important that civil nuclear programs are conducted under the highest standards of safety, security, and nonproliferation to ensure that nuclear material is not diverted to weapons programs.

ISN plays an important role in leading the Department's efforts to shape and maintain a secure international landscape, fostering stability, mitigating proliferation threats, and supporting America's national security interests by working to protect critical and emerging technologies and their supply chains. ISN leverages strategic partnerships, negotiates and implements nonproliferation agreements and treaties, conducts export control diplomacy -- including leading interagency U.S. delegations to the multilateral export control regimes -- imposes sanctions, leads interdiction

and other efforts to stop proliferation-related activities, and provides a broad array of capacity-building programs worldwide.

ISN plays a vital role in maintaining a free and open Indo-Pacific by promoting regional stability and cooperation in collaboration with our allies and partners while protecting U.S. interests in the region where authoritarian and revisionist countries like the People's Republic of China (PRC), Russia, and the Democratic People's Republic of Korea (DPRK) seek to undermine regional stability and actively threaten their neighbors. In collaboration with the Office of the Special Envoy for Critical and Emerging Technology, the Bureau of Cyberspace and Digital Policy, and regional bureaus, we work vigorously within the interagency, including a deep and longstanding partnership with the intelligence community, to limit the capabilities of the PRC, Russia, the DPRK, and others that threaten America's partners, allies, and our shared national security interests.

ISN uses its full suite of interdiction and disruption tools throughout the Indo-Pacific to help counter advances in threat capabilities, whether with respect to the PRC, Russia, the DPRK, or other countries of concern. The region is a tremendously important global center of trade and technological development, with a nexus of high-tech suppliers, commercial and financial hubs, and transit and transshipment lines that proliferators of sensitive technologies both within and outside the region seek to exploit to procure sensitive items. Sharing timely information with partners to stop transfers or shut down proliferation-linked firms, sanctioning entities and individuals who engage in illicit activities, and taking other steps to press for action are all central to our ongoing mission. We work very closely with our likeminded foreign partners on these efforts whether in bilateral channels or through multilateral efforts.

The PRC in particular is pursuing efforts to acquire, develop, and dominate critical and emerging technologies such as artificial intelligence, advanced materials, biotechnologies, leading-edge semiconductors, and quantum information systems. Although these technologies have legitimate commercial applications, the PRC believes that mastery of these

technologies can also be used to safeguard the authoritarian rule of the Chinese Communist Party and provide the People's Liberation Army military advantages. The PRC increasingly deploys these technologies to oppress its population, threaten its neighbors, and expand its influence globally in a manner that undermines regional stability and the international rules-based order.

We are especially concerned about PRC efforts to implement its Military-Civil Fusion (MCF) strategy, which merges the PRC's military and commercial innovation ecosystems to facilitate mutually reinforcing efficiencies in both domains. This MCF strategy decreases our confidence in our ability to ensure that U.S. technologies exported to the PRC will be used only for legitimate civilian purposes and remain free from government interference. ISN therefore works closely with Department colleagues, the interagency, and the intelligence community to counter MCF and related PRC activities, leveraging our entire existing counterproliferation tool kit and developing new capabilities to protect against PRC exploitation.

We have been working closely with our colleagues in the Department of Commerce's Bureau of Industry and Security and the interagency to tighten export controls to protect key sensitive U.S. technologies from misuse. This includes developing export restrictions on advanced computer chips and semiconductor manufacturing equipment to the PRC, which were announced in October 2022 and further strengthened in October last year.

The Department of State led diplomatic outreach on these rules and continues to lead plurilateral and multilateral efforts with allies and partners on export controls. This includes sharing information on indications of evasion or circumvention that can inform enforcement efforts or coordination on additional regulatory considerations.

ISN also implements programs to engage with countries developing critical and emerging technologies in the Indo-Pacific and elsewhere. Our programs build awareness of the PRC's predatory and exploitative tactics for acquisition of critical and emerging technologies and help strengthen

national safeguards such as intangible technology controls, military end-use and catch-all controls, and foreign direct investment screening measures.

A central focus is our collaboration with allies and partners to further protect semiconductor and other emerging technologies. Thanks to the work of this subcommittee and strong bipartisan support in Congress, the CHIPS and Science Act of 2022 and its International Technology Security and Innovation (ITSI) fund are making profound contributions to this effort.

With ITSI funding, we are developing another nonproliferation tool called the Semiconductor Protect Fusion Cell to counter MCF. The Fusion Cell gives front-line Department of State personnel access to worldwide open-source semiconductor industry data and business registries, military procurement, research funding, and investment data. By combining and analyzing these data sources, we will increase our ability to recognize and raise awareness of problematic PRC end-users and disrupt any illicit activities in which they attempt to engage.

In collaboration with Bureau of Economic and Business Affairs, ISN programs engage Indo-Pacific countries, as well as their relevant industrial and academic sectors, to strengthen their respective regulatory environments, implementation, and enforcement measures, and research, physical, and cybersecurity protection practices to bring them up to international standards and plug potential loopholes our competitors could exploit to access leading-edge semiconductor technology. Key partners in this area include Indonesia, Malaysia, the Philippines, and Vietnam.

ISN's capacity-building programs also strengthen the ability of researchers, the private sector, and government officials from the Indo-Pacific region and elsewhere to recognize and prevent the forced transfer or theft of critical and sensitive intellectual property and related technical knowledge via research collaborations, predatory talent acquisition programs, or cyberattacks. These programs provide technology protection measures that can be applied to secure advancements in biotechnology, artificial intelligence, and other critical and emerging technology fields from being

used against the United States and our allies and partners, such as India and Singapore.

We are clearly concerned by the PRC's self-described "no-limits" partnership with Russia and the evasion by PRC entities of sanctions and export controls on Russia and Belarus imposed by nearly 40 partner countries. To date, the Department of State and the Department of the Treasury have imposed sanctions on some 40 PRC-based targets involved in supporting Russia's war against Ukraine.

Russia, which is both a European and Indo-Pacific country, relies on imports of components, including microelectronics, to build the weapons it uses to wage its brutal war against Ukraine and for the strategic modernization of its military and defense industrial base. Since February 2022, ISN has coordinated with our partners and allies to use sanctions and export controls to restrict Russia's access to advanced technologies and interdict shipments to Russia's defense sector. During this period, ISN has imposed sanctions under its own authorities on more than 430 Russia-associated targets and continues to expand efforts in this area.

ISN is also continuing to vigorously implement our global campaign to implement the Countering America's Adversaries through Sanctions Act (CAATSA) Section 231 and related sanctions by deterring exports by Russia's defense sector that bring Moscow revenue, access, and influence it could use, among other things, to sustain or expand its own military modernization programs. Public data suggests the value of annual Russian arms export deliveries has dropped by almost two-thirds between 2018 and 2022. Several key Indo-Pacific states have notably abandoned potential major Russian arms purchases during that period.

We are particularly troubled by Russia's increasing reliance on the DPRK to support its illegal war against Ukraine. In response to the DPRK's deliveries of military equipment and munitions to Russia last year, ISN has used its sanctions authorities to block the proliferation networks facilitating these transfers, including by targeting individual Russians and North Koreans

involved to the shipping companies and vessels transporting such munitions. We remain concerned and vigilant about what Russia may be providing to the DPRK in exchange. We will continue to try to impede, delay, or curtail this trade using all the tools in our toolkit.

ISN's international capacity-building programs also help other countries with implementation of sanctions imposed by the U.S. and its allies and partners against Russia. These programs assist partners to identify Russian sanctions evasion networks, build awareness in the national authorities of key transshipment hubs of Russia's sanctions evasion techniques, and work with industry associations to strengthen compliance practices. We further conduct training to bolster our partners' ability to enforce relevant sanctions, combat corruption, and counter illicit flows of money and sanctioned goods to Russia.

For example, within the Indo-Pacific, we are engaging government and private sector stakeholders on how to develop the capacities to identify and disrupt Russian attempts to access global financial markets, procure microelectronics, airframe components, and other materials needed to manufacture unmanned aerial systems and other weapons Russia is using on the battlefield in Ukraine.

Critical and emerging technologies have global supply chains dependent on geographically diverse suppliers and innovators. ISN takes a global approach to protecting these technologies, including engaging likeminded partners in plurilateral efforts and expanding bilateral cooperation. Our efforts seek to bolster multilateral export control regimes to address the challenges posed by critical and emerging technologies.

To further address threats – as well as opportunities - posed by artificial intelligence (AI), we have established cooperative programming with key partners around the world. Building on these efforts, we are launching an AI Safety and Security project that will bring together allies and partners, including those in the Indo-Pacific, in a series of workshops designed to empower the AI community to develop robust safeguards against the

proliferation of WMD-enabling and weaponizable AI. These workshops and other ISN efforts will convene technical AI experts, lab security officials, counterproliferation experts, policy makers, and governance researchers to identify AI challenges and promote AI development best practices. This effort directly supports the Secretary's initiative to promote responsible technology development and AI application across the globe.

In addition to continuing its work of helping partners improve their legislation and laboratory safety, ISN is expanding efforts and developing new projects to address the potential for AI to be used to facilitate the creation of novel chemical and biological weapons. And we are making engagement with key partners and supplier countries a priority to ensure emerging biotechnology is protected from proliferators.

We are also investing in our own capacity to effectively engage international partners on protecting critical and emerging technology. In 2022, ISN stood up the Office of Critical Technology Protection (CTP) to serve as the focal point for developing and implementing policies to impede foreign development or acquisition of advanced technological capabilities that would be used by autocratic competitive powers. CTP supports efforts to counter the PRC's destructive influence and destabilizing behavior by engaging with allies and partners, including a core group of likeminded countries, to increase awareness, exchange information and best practices, and coordinate efforts to protect sensitive technologies and critical infrastructure.

And we have several other key initiatives to promote a secure and stable Indo-Pacific region and protect critical and emerging technology:

- The trilateral security partnership with Australia and the United Kingdom known as AUKUS supports Australia's acquisition of conventionally armed, nuclear-powered submarines. ISN is leading efforts to ensure Australia's proposed naval nuclear propulsion program will set the highest nonproliferation standard for others seeking a naval nuclear propulsion capability.

- Technology Safeguard Agreements (TSAs) with Australia and New Zealand protect and safeguard U.S.-licensed space launch vehicle (SLV) technology which is virtually identical and essentially interchangeable with ballistic missile technology. TSAs also provide the legal and technical framework for new U.S. commercial space launch opportunities consistent with U.S. nonproliferation policy and commitments to the Missile Technology Control Regime.

ISN will continue to work with the interagency and our allies and partners to ensure critical and emerging technology is protected and proliferation networks are disrupted, and we continue to expand our engagement and cooperation in the Indo-Pacific region with likeminded partners.

Thank you again for inviting me to testify today. I look forward to taking your questions.