U.S.-China Economic and Security Review Commission

Press Release

October 25, 2018

Contact: Leslie Tisdale
ltisdale@uscc.gov
202-624-1496

NEW REPORT: China's Internet of Things

Washington, DC— Today, the U.S.-China Economic and Security Review Commission released a report entitled *China's Internet of Things*, prepared for the Commission by SOS International LLC. The report examines the implications of China's development of the Internet of Things (IoT) for the U.S. economy, national security, and the privacy of U.S. citizen data. The IoT—the interconnection of physical and virtual things via information and communication technologies—is being applied to virtually every sector from smart thermostats in households to swarms of autonomous drones in the battlefield. The full report can be found here [link].

Key Findings:

- The Chinese government is driving development of the IoT—an industry it views as strategic—through the creation of IoT industrial and innovation centers, extensive financial support, and favorable regulations. Foreign firms, which are considered strategic rivals, face an uneven playing field and are subject to a number of policies that disadvantage them in favor of domestic firms, including restrictions on foreign investment, selective enforcement of Chinese laws to hinder the operation of foreign IoT firms in China, and forced technology transfer.
- China's large market size, production capacity, and government support offer it some significant advantages, but it is still behind U.S. and other foreign leaders in many IoT technologies. Therefore, there is still a window for U.S. companies and the U.S. government to maintain a technological edge and influence future IoT development, standards, and roll-out.
- The Chinese government is actively attempting to influence international technical standards for the IoT that would benefit Chinese companies at the expense of U.S. and other foreign counterparts. China pursues a more coordinated and comprehensive strategy than the United States' private-sector-led approach with U.S. entities often absent from key international standardization processes.
- China has laid a solid groundwork for a comprehensive roll-out of fifth-generation wireless technology (5G), which will make the IoT faster and more effective, relying on a whole-of-country approach that has created an entire ecosystem for domestically manufactured 5G technologies and furthered their inclusion in international technical standards. China is on track to roll-out the largest and most reliable 5G networks, gaining a head start in developing the technologies that 5G enables—first among them, the IoT.
- Chinese-manufactured IoT devices have already become common vehicles for unauthorized access due to their widespread usage and insecure device configurations that have resulted in surreptitious data collection and the exploitation for cyberattacks, unauthorized remote access, and data theft.
- China is actively researching IoT vulnerabilities, both for security purposes and almost certainly to collect intelligence, conduct network reconnaissance for cyberattacks, and enhance its

domestic surveillance powers. The combination of widespread adoption of IoT products and Chinese research into IoT exploits raises the threat of unauthorized access to U.S.-based IoT devices and networks.

- China's authorized access to the IoT data of U.S. consumers will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States.
- While authorized data access, collection, and processing are indispensable parts of the IoT's transformative potential, China poses a grave threat to U.S. privacy as its government and surveillance apparatuses are empowered to access this data well in excess of accepted international norms. In the short term, Chinese government and corporate access to U.S. data would be a huge opportunity for Chinese intelligence targeting operations. In the longer term, such access would provide a major edge to Chinese artificial intelligence (AI) development efforts, eventually culminating in a substantial Chinese economic advantage in another field that is expected to shape the economy of the future.
- Existing U.S. data protections appear insufficient to protect U.S. data against harmful but authorized data access. The patchwork nature of U.S. laws and authorities leaves loopholes that could facilitate Chinese access to U.S. IoT data in bulk, an especially risky proposition given known Chinese motivations for accessing big data.

The report was authored by John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray, and James Mulvenon.

###

The U.S.-China Economic and Security Review Commission was created by Congress to report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China. For more information, visit www.uscc.gov.