

United States Senate

June 4, 2025

The Honorable Jeffrey Kessler
Under Secretary of Commerce for Industry and Security
Department of Commerce
1401 Constitution Avenue Northwest
Washington, D.C. 20230

Dear Under Secretary Kessler:

In his first term, President Trump issued a crucial warning through Executive Order 13873: foreign adversaries like Communist China were actively exploiting vulnerabilities in our information and communications technology and services (ICTS) infrastructure.¹ President Trump rightly outlined the threat Communist China and other enemies posed to our emergency services, the digital economy, and critical American infrastructure that our citizens and government rely on every day. The regime in Communist China openly spies on the United States and seeks to undermine our nation at every turn, and the threats posed to our national security and the American people have only increased after four years of President Biden's failures and appeasement that put American families, businesses, and security at risk.

In the Senate, we have worked for years to address these threats, get Communist China out of our networks, infrastructure, and government, and ensure the safety of our nation. We were alarmed by recent reports indicating that Communist China has already compromised the integrity of power inverters connecting to our power grid. These inverters contained unidentified communication equipment capable of transferring sensitive data outside the country.² We are concerned about recent reports indicating these CCP-manufactured parts and systems allow for remote access, unauthorized data exfiltration, and even operational disruption. This is the exact threat President Trump sought to address years ago, and that threat is clearly still dangerously real.

¹ <https://www.cisa.gov/eo-13873>

² <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>

In E.O. 13873, President Trump granted the Secretary of Commerce authority over ICTS transactions involving foreign adversaries. In service of this important initiative, we urge the Office of Information and Communications Technology and Services to initiate an investigation into the presence of any Chinese-manufactured components within the U.S. power grid – especially inverters, transformers, supervisory control and data acquisition devices, and their associated firmware and software. This investigation would be in full alignment with the president’s actions to ensure our nation’s supply chain resilience, critical infrastructure protection, and strategic decoupling from malign foreign influence. If we depend on Chinese technology for access to electricity and critical services, Congress must know to what extent and what action can be taken to secure our grid immediately.

Communist China has decided to be an adversary to the United States, and this would not be the first time Beijing has sought to infiltrate our systems and undermine our national security. We have warned for years that any item made in Communist China or sold by companies based in Communist China can be used against the United States. Every company based in Communist China reports to General Secretary Xi, who can and will use his power to disable, degrade, or manipulate U.S. infrastructure systems, thereby denying Americans access to electricity, communication, water, and transportation.

Communist China has already shown its willingness to use Chinese technology against the United States and control any components for their own gain:

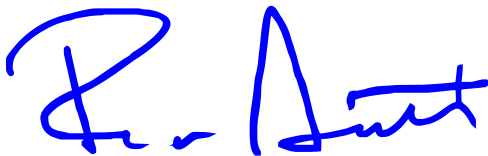
- Chinese-made drones surveilling and spying on American families;
- Telecommunications equipment and devices made by now-blacklisted Chinese companies Huawei, ZTE and others to spy on Americans;
- The collection of Americans’ data by CCP-controlled ByteDance and TikTok;
- The Volt Typhoon campaign, disclosed in 2023, targeted critical infrastructure entities across multiple sectors – including energy and communications – using “living-off-the-land” techniques to establish persistent access without deploying traditional malware;
- The Salt Typhoon breach, where a Chinese Communist Party-backed infiltration of Americans compromised the data of public officials like President Donald Trump; and
- Flax Typhoon, a cyber-espionage campaign by the Chinese Communist Party in Taiwan targeting power grid systems as strategic leverage.

The Honorable Jeffrey Kessler
June 4, 2025
Page Three

Communist China has shown time and again their willingness to defy international agreements and cheat the system to track, gain access to, and control sensitive data across the globe, putting Americans at risk. This regime cannot, under any circumstances, be allowed a 'kill switch' in our power grids.

We urge you once again to initiate an investigation on this urgent matter, and appreciate your continued leadership in securing our nation's ICTS ecosystem and the safety and security of the American people.

Sincerely,



Rick Scott
United States Senator



Marsha Blackburn
United States Senator