

United States Senate

WASHINGTON, DC 20510

March 26, 2019

Mr. James Robb
President and Chief Executive Officer
North American Electric Reliability Corporation
1325 G Street NW, Suite 600
Washington, DC 20005

Dear Mr. Robb:

We write to request information regarding the North American Electricity Reliability Corporation's (NERC) efforts to protect the reliability of the nation's bulk power system from supply chain vulnerabilities, particularly those posed by vendors from Russia and China. The Energy Policy Act of 2005 (PL 109-58) and subsequent Federal Energy Regulatory Commission certification in 2006 require NERC to establish and enforce reliability standards for the bulk power system.

We are deeply concerned about companies from Russia and China in light of recent statements by the Director of National Intelligence, Daniel Coats. Director Coats noted that "China and Russia are more aligned than at any point since the mid-1950s, and the relationship is likely to strengthen in the coming year."¹ China, according to Director Coats, has the potential to take down a natural gas pipeline, and Russia has the ability to disrupt an electrical distribution network. Unfortunately, China and Russia "have significantly expanded their cooperation, especially in the energy, military and technology spheres, since 2014."²

The federal government has taken some action. On September 13, 2017, the Department of Homeland Security (DHS) issued a Binding Operational Directive³ which barred products from the Russia-based Kaspersky cybersecurity firm from being used across all federal government information systems. DHS explained its actions by noting that the "Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks."⁴ We understand NERC alerted its members immediately after DHS issued its release of the risks posed by using Kaspersky products.

With respect to specific Chinese companies, the statement of an ally is telling. The Director-General of the Australian Signal's Directorate, Mr. Michael Burgess, noted that Australia banned

¹ <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>

² *Ibid.*

³ <https://cyber.dhs.gov/bod/17-01/>

⁴ <https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01>

Chinese companies Huawei and ZTE from being able to participate in Australia's new 5G mobile network because such participation would prevent the electricity grid and other infrastructure from being protected.⁵ The Federal Communications Commission has proposed action that would discourage Huawei and ZTE's participation in our nation's new 5G network.⁶ Finally, Congress acted in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (PL 115-232), effectively banning Huawei and ZTE from all federal contracts for telecommunications equipment or services, and effectively prohibiting Huawei and ZTE from doing business with U.S. government contractors.

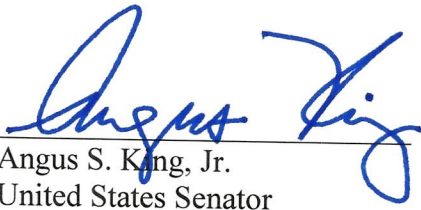
We fear the same risks posed to the country's federal agencies and departments, telecommunications networks, and military assets also threaten to impair the reliability of our nation's energy infrastructure. As a result, we request answers to the following questions:

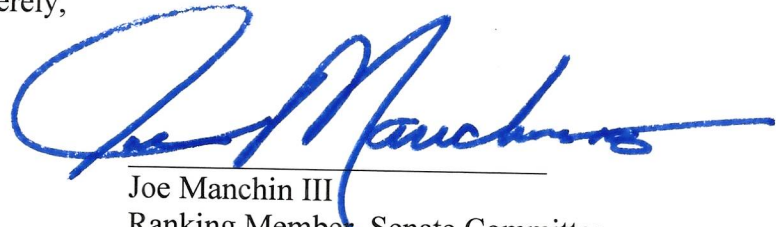
1. Since August 2017, has NERC undertaken efforts to determine whether the bulk power system includes any components or software provided by Kaspersky, ZTE, or Huawei? If so, what were the results? If not, why not?
2. Has NERC issued guidance or recommendations to the users, owners, and operators of the bulk power system for mitigating the potential risks posed by components or software provided by Kaspersky, ZTE or Huawei?
3. What are NERC's next steps to mitigate the potential risks posed by components or software from Kaspersky, ZTE or Huawei?

Your assistance in this matter will continue to ensure the reliability of our nation's energy assets, which are critical to the safety, security, and economic well-being of the country. Please provide your response to this letter within 30 days. We would be pleased to receive your response in either a letter or a private briefing.

Thank you for your consideration.

Sincerely,


Angus S. King, Jr.
United States Senator


Joe Manchin III
Ranking Member, Senate Committee
on Energy and Natural Resources

⁵ <https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says>

⁶ <https://docs.fcc.gov/public/attachments/FCC-18-42A1.pdf>