

United States Senate

WASHINGTON, DC 20510

March 18, 2022

The Honorable Lloyd J. Austin III
Secretary of Defense
U.S. Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
U.S. Department of Homeland Security
245 Murray Lane S.W.
Washington, D.C. 20528

Secretary Austin & Secretary Mayorkas,

We write to you today regarding concerns over the vulnerability of our public and private infrastructure relating to potential cyber attacks by the Russian Federation and their proxies. The realm of cyber escalation remains largely unexplored. Presently, Russia is justly cornered by extreme sanctions measures and there are concerns it will lash out against the United States through non-kinetic attacks.

There have been Russian cyber attacks in the past, however, entanglements in Western markets have likely stymied the extent of these attacks—expulsion from these markets may have drastically changed this calculus. As Jason Healey of Columbia University recently stated, “If you are dealt out of the game, why not just flip the table?”¹

Moreover, it is understood that our nation’s cyber offensive capabilities are extraordinary, yet as we have seen with the Colonial Pipeline hack and the reported increase in cyber-attacks on our financial institutions, our defense—especially at private, state, and local levels—is wanting. Even beyond the current Russian-induced conflict, cyber threats are growing faster than our private, state, and local institutions can adapt to them. From banks, hospitals, liquified natural gas terminals, bridges and roads, our institutions need to be informed and supported by the federal government in order to be prepared to absorb and rebuff offensive cyber operations by foreign adversaries.

As such, we request a written response to the following questions:

1. What measures have your agencies taken to support reducing relevant cyber vulnerabilities to our:
 - a. State and local infrastructure;
 - b. Private institutions, such as banks, refineries and liquified natural gas terminals;
 - c. the U.S. electric grid;
 - d. And private citizens?
2. Are the institutions listed in the previous question adequately prepared for a major Russian retaliatory cyber offensive?

¹ Healey, Preventing Cyber Escalation in Ukraine and After, War on the Rocks, 2022

3. Has there been a coordinated effort to provide adequate information to non-federal entities about the risks of the increased cyber threat posed by Russia?
4. Has there been a coordinated effort to provide a centralized solution for non-federal entities?

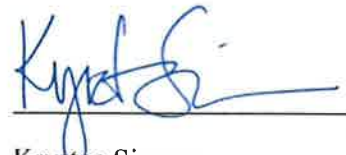
Additionally, please provide a written assessment of all recent significant malicious cumulative cyber activities against the U.S. or reported activities against U.S.-based private institutions by the Russian Federation or a suspected proxy. This written assessment should include an assessment of appropriate defensive measures taken in response to any malicious cyber activity.

We implore you to act without delay in providing the necessary resources and working with our private, state, and local institutions to prevent our critical infrastructure, systems, and institutions from being compromised by nefarious attempts to respond to justified sanctions. We must act now, with increased haste, before we find ourselves under a major retaliatory cyber offensive that causes extreme disruption in the lives of everyday Americans.


Sincerely,




John N. Kennedy
United States Senator



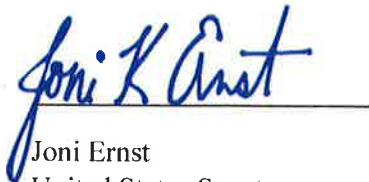
Krysten Sinema
United States Senator



Roger Wicker
United States Senator



Mark Kelly
United States Senator



Joni Ernst
United States Senator



Bill Cassidy, M.D.
United States Senator



Ted Cruz
United States Senator



Kevin Cramer
United States Senator



Steve Daines
United States Senator



Mike Braun
United States Senator



Bill Hagerty
United States Senator



John Boozman
United States Senator



Ron Johnson
United States Senator