

LISA MURKOWSKI, Alaska, Chairman  
JOHN BARRASSO, Wyoming  
JAMES E. RISCH, Idaho  
MIKE LEE, Utah  
JEFF FLAKE, Arizona  
STEVE DAINES, Montana  
CORY GARDNER, Colorado  
LAMAR ALEXANDER, Tennessee  
JOHN HOEVEN, North Dakota  
BILL CASSIDY, Louisiana  
ROB PORTMAN, Ohio  
LUTHER STRANGE, Alabama  
MARIA CANTWELL, Washington  
RON WYDEN, Oregon  
BERNARD SANDERS, Vermont  
DEBBIE STABENOW, Michigan  
AL FRANKEN, Minnesota  
JOE MANCHIN III, West Virginia  
MARTIN HEINRICH, New Mexico  
MAZIE HIRONO, Hawaii  
ANGUS S. KING, JR., Maine  
TAMMY DUCKWORTH, Illinois  
CATHERINE CORTEZ MASTO, Nevada  
COLIN HAYES, STAFF DIRECTOR  
PATRICK J. MCCORMICK III, CHIEF COUNSEL  
ANGELA BECKER-DIPPMANN, DEMOCRATIC STAFF DIRECTOR  
SAM E. FOWLER, DEMOCRATIC CHIEF COUNSEL

## United States Senate

COMMITTEE ON  
ENERGY AND NATURAL RESOURCES

WASHINGTON, DC 20510-6150

[WWW.ENERGY.SENATE.GOV](http://WWW.ENERGY.SENATE.GOV)

March 14, 2017

President Trump  
The White House  
1600 Pennsylvania Avenue, NW  
Washington, DC 20500

Dear President Trump:

We write to ask you to ensure that, in any forthcoming executive order, the Department of Energy plays the leading role in U.S. government efforts to defend against--and respond to--cybersecurity incidents affecting our critical energy systems and networks. In addition, we urge you to direct the Department of Energy to begin a thorough analysis of Russian capabilities with respect to cyberattacks on our critical energy infrastructure.

While recent digitization of the nation's critical energy infrastructure has brought about many advances and efficiencies, it has also made it more susceptible to cyber intrusions. It is imperative that we are doing everything we can to harden and protect our infrastructure from very real and imminent threats.

This is particularly troubling as it becomes increasingly clear that the Russians and other foreign actors have the capability, and potentially the intent, to do significant damage to our economy by attacking our critical energy infrastructure, including our electric grid. As Admiral Rogers, the Director of the National Security Administration and the Commander of the U.S. Cyber Command during the Obama Administration, recently told Congress – Russia holds the cyber capability to cripple our infrastructure.

There are press accounts that indicate that the Russians most likely hacked into three Ukrainian distribution utilities, knocking power out to more than 225,000 customers for several hours. And it appears the Russians may have recently done it again. Two months ago a utility in northern Kiev reported that their grid was brought down as a result of a cyber-attack that was very similar to the alleged Russian attack in 2015. Fortunately, our grid in the United States has not yet been successfully attacked. But press reports suggest that there are frequent attempts to hack into our utility systems.

Recently, the Department of Homeland Security and the Federal Bureau of Investigation publicly issued a Joint Analysis Report documenting their findings of Russian malicious cyber activity in the United States known as Grizzly Steppe. They definitively state that “public attribution of these activities to RIS [Russian civilian and military intelligence Services] is supported by

technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities.”<sup>i</sup>

It has also come to our attention that your administration may be issuing an executive order on cybersecurity in the near future. While we agree that more action is urgently needed, it appears that the contemplated executive order may direct the Department of Homeland Security to carry out certain duties that have, by statute, been assigned to the Department of Energy, including a potential assessment of electricity disruption response capabilities. Such an executive order would be inconsistent with Public Law 114-94, the so-called FAST Act. Enacted last Congress, key bipartisan provisions expressly designate the Department of Energy as the lead Sector-Specific Agency for cybersecurity for the energy sector, given the Department’s technical expertise with respect to operations of the electric grid and other essential and interconnected elements of our nation’s energy systems, as well as its ongoing collaboration and information-sharing with U.S. industry.

As a result of the increased threat that Russia and other foreign state actors potentially pose to the cybersecurity of the nation’s grid and critical energy systems, we respectfully request that:

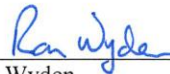
1. Your administration directs the Department of Energy, in consultation with other relevant agencies, to conduct a thorough analysis of: a) the scope of Russian capabilities to use cyber-warfare to threaten our energy infrastructure; and b) the extent to which the Russians have already attempted cyber-intrusions into our electric grid, pipeline, and other important energy facilities; and
2. Your administration seeks to ensure any forthcoming executive order on cybersecurity is consistent with provisions of federal law that designate the Department of Energy as the lead Sector-Specific Agency for cybersecurity of the energy sector and its networks.

If there was ever a time that proves the pressing need for the work of the Department of Energy’s cybersecurity efforts, it is now. We thank you for your attention to these matters.

Sincerely,



Maria Cantwell  
United States Senator



Ron Wyden  
United States Senator

<sup>i</sup> [https://www.us-cert.gov/sites/default/files/publications/JAR\\_16-20296A\\_GRIZZLY%20STEPPE-2016-1229.pdf](https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf)