The Secretary of Energy
Washington, DC 20585

February 23, 2022

Dear Energy Sector Executives,

I am reaching out to you as leaders in the U.S. energy sector because you play a critical role in ensuring the reliable and secure flow of electricity, oil, and natural gas across the country. Your organization is particularly important during times of heightened geopolitical tensions like those we are seeing in Eastern Europe. The White House continues to work to reach a diplomatic solution to de-escalate the crisis, but a more expansive invasion remains a distinct possibility that we must prepare for in partnership with you and with Allies across the world.

The Department of Energy (DOE) is proactively recommending the energy sector prepare to the highest possible level for potential Russia-linked cyber and disinformation activity or cybercriminal activity from actors seeking to exploit the ongoing geopolitical situation. While there remains no specific credible threat to the homeland from Russia, that I am aware of, the U.S. Government has been working with energy sector owners and operators to prepare for all geopolitical contingencies.

Historically over the last decade, Russia has used cyber capabilities as a major part of its military and intelligence activity beyond its borders, not only to undermine, coerce, and destabilize Ukraine, but to weaken U.S. institutions and interests. For that reason, and at President Biden's direction, we have been working to prepare for potential cyber-attacks both in Ukraine and here in our homeland. I would like to focus here on the latter.

Over the last several weeks, DOE hosted threat briefings for the energy sector, shared guidance such as the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency's (CISA) "Shields Up" recommendations, released the DOE Analysis of Risks in the Energy Sector (ARES) Report to help energy sector entities evaluate the risk to their systems from identified threat vectors, and held regular conversations with the three energy sector information sharing and analysis centers (ISACs) – the Electricity ISAC, Downstream Natural Gas ISAC, and the Oil and Natural Gas ISAC – to ensure that we are distributing timely, relevant, and actionable information.

As leaders of the energy sector, I am calling upon each of you to do your part to ensure our national preparedness and security. Please engage with your information and operational technology (IT/OT) and cybersecurity teams and confirm they take the following actions now:

1. Review the CISA "Shields Up" guidance (https://www.cisa.gov/shields-up) and DOE ARES report (the DOE ARES Report can be found on the ISAC portals) and confirm whether relevant and necessary measures have been fully

implemented. If they have not been fully implemented, ask about timelines to expeditiously implement the measures appropriate to your systems.

2. Ensure that your cybersecurity team is a member of one of the three energy ISACs and that your organization is both reviewing alerts and guidance documents that the ISACs distribute through their portals and other information sharing tools. Please also lower the thresholds for information sharing and report unusual cyber activity to the ISACs. The ISACs are a key resource for shared sector-wide situational awareness. If one energy sector entity is seeing anomalous cyber activity, it is critical that we share that information with other energy entities and expect them to do the same in return.

3. Discuss your organization's cyber response procedures with your staff and have a clear understanding of roles and responsibilities within your organization. This should include representatives from cybersecurity, information technology, operations (e.g., transmission and distribution, pipeline operators), legal, business continuity, public relations, and others.

4. In the event of an attempted or confirmed cyber intrusion, immediately report to points of contact at the ISACs and in the government through DOE, CISA, or the Federal Bureau of Investigation (FBI). DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) can be reached, at EnergyResponseCenter@hq.doe.gov or through the DOE Watch Office by phone, at (202) 586-8100 or by email, at doehqeoc@hq.doe.gov. Alternatively, your organizations can reach out to CISA (https://www.cisa.gov/uscert/report) or the FBI via your local FBI field office (https://www.fbi.gov/contact-us/field-offices) (https://www.fbi.gov/contact-us/field-offices).

DOE will remain closely engaged with the energy sector, to share information, provide threat briefings, and support any response efforts. Please feel free to reach out to DOE CESER's Principal Deputy Assistant Secretary Puesh Kumar (puesh.kumar@hq.doe.gov) or Acting Deputy Assistant Secretary Kate Marks (kate.marks@hq.doe.gov), if you would like to follow-up on any of the items mentioned above. We stand ready to support you and your efforts.

Thank you all again for your continued collaboration and vigilance on this issue as we continue to work towards securing our nation's critical energy infrastructure.

Sincerely,

Jennifer Granholm