**U.S. Department of Homeland Security**
Cybersecurity & Infrastructure Security Agency
*Office of the Director*
Washington, DC 20528

February 22, 2022

Members of the Business Roundtable,

As a Nation, we are watching with increasing concern the activities in Ukraine, including the recent deployment of Russian troops to the eastern part of the country. While there are currently no specific or credible threats to the U.S. homeland, we are mindful of the potential for the Russian government to escalate its destabilizing actions in ways that may impact businesses both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. As Chief Executives of America's leading companies, I urge you to ensure you are taking the necessary steps to protect your businesses from the impact of potential cyber-attacks.

The Cybersecurity and Infrastructure Security Agency (CISA), along with our partners in the U.S. Intelligence Community, law enforcement, the military, and sector risk management agencies, is monitoring the threat environment on a 24/7 basis, and as those threats manifest themselves in potential risks to your business, we will be in continuous contact with the private sector. But we cannot see or deal with these threats alone. As a matter of national and economic security, we need your collaboration, both in taking the necessary steps to protect yourselves, and second, in working with us to see and understand the threat.

To the first point, we recently launched a "Shields Up" at (www.cisa.gov/shields-up) with actionable information to help ensure the security and resilience of your businesses from cyber threats. In particular, I strongly encourage you to take the following steps if you've not already done so:

**Urgent Focus Areas for Every CEO:**

- **Empower Chief Information Security Officers (CISO):** In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:** Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.

- **Participate in a Test of Response Plans:** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.
- **Focus on Continuity:** Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.
- **Plan for the Worst:** While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

In today's highly connected and highly complex technology environment, with dependencies on supply chains where there is inherently imperfect control, it has become increasingly challenging to completely prevent incidents that may disrupt business operations. Such an environment necessitates a laser-focus on resilience, to include dedicated efforts to ensuring preparedness and a rapid, coordinated response to mitigate the impact of such disruptions to your business or the wider economy.

As the first signs of a major cyber-attack on U.S. infrastructure may be detected by one of your companies, I want to reemphasize the importance of continuous collaboration and information sharing in working together to see and understand the threat. At CISA, we lead the national effort to understand, manage, and reduce risk to America's critical infrastructure and serve as your close partner, along with the rest of the Federal government, in ensuring the security and resilience of your operations. Please do not hesitate to reach out directly if we can support you in any way.

Sincerely,

Jen Easterly
Director
Cybersecurity & Infrastructure Security Agency (CISA)
Department of Homeland Security
jen.easterly@cisa.dhs.gov
202.763.5405