Subject: Geopolitical Tension and Increasing Critical Infrastructure Cybersecurity Awareness

---

As a nation, we are watching with increasing concern the heightened tensions between Russia and Ukraine. While there are not currently any specific credible threats to the U.S. homeland, we are mindful of the potential for the Russian government to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine. Specifically, we are watchful for any malign activity targeting America's critical infrastructure.

CISA continues to lean forward to inform our industry partners of potential threats—part of a paradigm shift from being reactive to being proactive. On January 11, 2022, we released a joint cybersecurity advisory with the FBI and NSA about the Russian threat to U.S. critical infrastructure, including specific tactics, techniques, and procedures associated with Russian actors. We followed this advisory with an executive-level product urging every organization to take urgent, near-term steps to reduce the likelihood and impact of a potentially damaging compromise. We maintain a dedicated public webpage providing an overview of the Russian government's malicious cyber activities as well as all our advisories and products on Russian state-sponsored cyber threats, to include the recent advisory on known tactics, techniques, and procedures used by Russian state-sponsored cyber actors.

We strongly encourage all organizations to review and take advantage of the following resources:

- **Shields Up** – CISA launched a new Shields Up webpage that provides actionable information on urgent steps to harden systems given the heightened threat environment.
- **Pro Bono Services** – CISA recently launched a new catalog of free cybersecurity services from CISA, the open-source community, and our private sector partners in the Joint Cyber Defense Collaborative. The catalog is designed to help under-resourced organizations improve their security posture.
- **Mis-, dis-, Malinformation (MDM) –** CISA released a *CISA Insights* titled, Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure, which provides critical infrastructure owners and operators with guidance on how to identify and mitigate the risks of influence operations using MDM narratives from steering public opinion and impacting National Critical Functions and critical infrastructure.

By utilizing the services above, all organizations can make near-term progress toward improving cybersecurity and resilience. As the nation's cyber defense agency, CISA is available to help organizations improve cybersecurity and resilience, including through cybersecurity experts assigned across the country. In the event of a cyber incident, CISA is able to offer assistance to victim organizations and use information from incident reports to protect other possible victims.

We also encourage organizations to remain vigilant and lower the threshold for reporting. If you believe that your jurisdiction, or a critical infrastructure partner, has experienced a cyber intrusion, please report incidents and anomalous activity to CISA (Central@cisa.gov; 1-888-282-0870) and/or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Connect with us at CISA, Facebook, Twitter, LinkedIn, and YouTube

Subscribe to receive CISA alerts and updates

Subscribe to receive DHS information, alerts, & updates