SHIELDS UP

FACT SHEET: CISA LEADS CALL FOR STRENGTHENING NATIONAL CYBERSECURITY

As the nation’s cyber defense agency, the Cybersecurity and Infrastructure Security Agency (CISA) helps organizations prepare for, respond to, and mitigate the impact of cyber incidents. In light of Russia’s ground war in Ukraine and potential for direct cyberattacks, as well as spillover from cyber incidents outside U.S. borders, CISA is actively providing federal, state, local tribal and territorial stakeholders, the private sector, media, and the general public with timely information to bolster national security preparedness. CISA has worked for months to share information, provide resources, and inform partners and stakeholders of the urgent, concrete actions they should take to heighten their cybersecurity posture. Every organization—large or small—must be prepared to respond to disruptive cyber activity.

SHIELDS UP

To help stakeholders protect their most critical assets ahead of Russia’s invasion of Ukraine, CISA launched the Shields Up campaign on CISA.gov with current and regularly updated guidance to help organizations of every size adopt a stronger cybersecurity posture. The webpage includes steps organizations can take, free cybersecurity resources available to critical infrastructure partners, and our guidance on how organizations can prepare themselves to mitigate the impact of potential foreign influence operations and mis-, dis-, and mal-information.

INFORMATION AND RESOURCES

Guidance for Organizations, CEOs, and Individuals

- Shields Up provides concrete actions for our broad range of stakeholders, to include guidance for all organizations, recommendations for corporate leaders and CEOs, steps you can take to protect yourself and your family, ransomware response, and additional resources. This information is intended to be a high-level roadmap to help stakeholders heighten their cybersecurity posture and prepare for disruptive cyber incidents.

Free Cybersecurity Services and Tools

- CISA hosts a living repository of free cybersecurity tools and services. This offering includes services created and provided by CISA, widely used open-source tools, as well as tools and services offered by trusted private and public sector organizations across the cybersecurity community.

Known Exploited Vulnerabilities (KEV) Catalog

- CISA launched its catalog of Known Exploited Vulnerabilities when outreach began in preparation for the war in November. The catalog fundamentally transforms how the federal government, and the nation as a whole, prioritize vulnerability mitigation. CISA’s highlights the specific vulnerabilities that are most actively being exploited by nation-states and criminal groups and pose significant risk to stakeholders and organizations of all sectors and sizes.

Technical Guidance for Network Defenders

- CISA’s work with our Joint Cyber Defense Collaborative partners has yielded critical technical guidance and information about Russian threat actors, ransomware threats, destructive malware, distributed denial of service (DDoS) attacks, and protective measures that we share with network defenders across the cybersecurity community and all sectors. CISA also has a comprehensive webpage on Russia-attributed advisories, as well as overviews of known tactics at Russia Cyber Threat Overview and Advisories.

Joint Cybersecurity Advisories

- In December and January, CISA began to urge critical infrastructure owners and operators to take immediate steps to strengthen their computer network defenses against malicious cyberattacks. Since then, CISA has worked with government partners to update and issue multiple Cybersecurity Advisories (CSAs) for network defenders, which are publicly accessible on the Shields Up Technical Guidance webpage. Available CSAs include Implement Cybersecurity Measures Now to Protect Against Critical Threats, Preparing For and Mitigating Potential Cyber Threats, Conti Ransomware, Strengthening Cybersecurity of SATCOM Network Providers and Customers, and Mitigating Attacks Against Uninterruptible Power Supply Devices, among others.

COLLABORATING ON CYBERSECURITY

Through its Joint Cyber Defense Collaborative (JCDC), CISA is engaged in ongoing operational collaboration with the nation's largest tech companies, banks, and energy firms, among others. Through this collaboration, we exchange, enrich, and amplify actionable information from the private sector and government partners, including the National Security Agency, the Federal Bureau of Investigation, and U.S. Cyber Command, in real-time. The JCDC allows us to quickly understand adversary activity and share actionable steps to reduce risk to U.S. networks.

Specific industry channels include:

- JCDC Alliance, which includes more than 25 of the nation's largest cybersecurity, technology, and infrastructure companies, including Internet Service Providers, Cloud Service Providers, and Cybersecurity Companies;
- Energy Sector, which includes 38 major energy companies and the Department of Energy; and
- Financial Sector, which includes 22 major financial services companies and the Department of the Treasury.

Coordination and Collaboration with Partners:

- Since November, CISA has convened U.S. Government and private sector stakeholders and conducted proactive outreach at both classified and unclassified levels. This outreach was provided to Federal Civilian Executive Branch Agencies, Sector Risk Management Agencies, private sector partners, SLTT governments, and international partners. To date, CISA had hosted or participated in more than 90 engagements reaching tens of thousands of partners.
- Following the President's designation of DHS as the lead federal agency for domestic preparedness and response related to the current crisis, DHS established a Unified Coordination Group (UCG) and designated interagency liaisons.

Leveraging International Partners:

- CISA is continuously exchanging cyber defense information with its counterparts around the world. Since the invasion of Ukraine, CISA has exchanged technical information with key partners including Ukraine, Lithuania, Latvia, Germany, and Poland. This information has been actively used to protect U.S. organizations and has issued joint cybersecurity alerts with our partners Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), National Cyber Security Centre New Zealand (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK).
- CISA continues to offer the government of Ukraine technical assistance including best practices for enhancing the cybersecurity and resilience of critical infrastructure, focused on industrial control systems.