DEFEND TODAY, SECURE TOMORROW
Critical Infrastructure Focused
Russia’s invasion of Ukraine is impacting organizations both within and beyond the region, to include malicious cyber activity against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners.

Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks.

Every organization—large and small—must be prepared to respond to disruptive cyber incidents.
CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

**Shields Up Guidance for All Organizations**
- Reduce the likelihood of a damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure that the organization is prepared to respond if an intrusion occurs
- Maximize the organization's resilience to a destructive cyber incident

[Visit Shields Up - cisa.gov/shields-up](https://cisa.gov/shields-up)
CISA No-Cost Cybersecurity Resources

• Preparedness Activities
  • Cybersecurity Assessments
  • Cybersecurity Training and Awareness
  • Cyber Exercises and “Playbooks”
  • Information / Threat Indicator Sharing
  • National Cyber Awareness System
  • Vulnerability Notes Database
  • Information Products and Recommended Practices
  • NEW Ransomware Readiness Assessment

• Response Assistance
  • Incident Coordination
  • Threat intelligence and information sharing
  • Malware Analysis

• Field-based Cybersecurity Advisors (CSAs)
  • Incident response coordination
  • Cyber assessments
  • Working group collaboration
  • Public-private advisory assistance
  • Public Private Partnership Development
For more information:
www.cisa.gov
www.cisa.gov/shields-up

Questions?