

October 2026

Priority Level: High

Threat Overview: Cyber Risks to the Bulk-Power System

The White House has declared a national emergency over threats to the security and reliability of the U.S. bulk-power system. President Trump's recent Executive Order highlights risks from foreign-sourced equipment, software, firmware, remote access, and other technologies that could enable unauthorized access or disruption. A compromise of power-system technology could have cascading impacts across critical infrastructure and essential services. While the Order focuses on the bulk-power system, the risks it identifies around supply-chain compromise, remote access, and operational technology (OT) security are relevant to organizations across the State, Local, Tribal, and Territorial (SLTT) community.

Threat Vectors to Watch:

- **Supply-Chain Compromise:** Foreign-sourced hardware, software, and components can introduce vulnerabilities or hidden access into critical systems.
- **Remote Access:** Poorly secured vendor or administrative remote access can provide attackers a pathway into critical systems and operational technology.
- **Compromised Software & Firmware:** Malicious or compromised updates can introduce threats directly into trusted systems and devices.
- **OT & ICS Exploitation:** Attacks against industrial control systems and other operational technology can disrupt physical processes, not just data or information.
- **Power Disruption & Cascading Impacts:** A disruption to the bulk-power system could affect other critical infrastructure and essential services that depend on reliable electricity.

GOAL: The goal of this bulletin is to give business leaders, IT teams, and operational staff simple, actionable guidance to strengthen defenses against modern cyber threats. While attackers use complex and evolving methods, many successful intrusions still exploit basic weaknesses. The foundational controls show that doing the simple things, such as patching, authentication, access control, visibility, and backup, can make a biggest difference. More awareness materials will follow through October's Cybersecurity Awareness Month.

Remember: Security is a Shared Responsibility

- ✓ When in doubt, verify through official internal channels before interacting with unexpected requests.
- ✓ If you click on a suspicious link or enter credentials on a suspicious website, notify your security operations center or responsible IT support immediately.



For more information, scan the QR code or visit
ransomwareinfo.oregon.gov



CYBER READINESS TIPS

Best Practices For Organizations

- **Know Your Critical Technology:** Maintain an inventory of critical hardware, software, firmware, systems, and third-party services that support essential operations.
- **Understand Your Supply Chain:** Know your critical vendors and suppliers, where technology originates, and who has access to your systems.
- **Secure Remote Access:** Limit remote access to critical systems and require MFA, least privilege, and monitoring for authorized connections.
- **Separate IT and OT:** Segment operational technology from IT networks where possible, and closely monitor connections between environments.

Best Practices For Individuals

- **Use strong, unique passwords** by using a different password for every account, and consider using a reputable password manager to securely store them.
- **Turn on multi-factor authentication (MFA)** which adds an extra layer of protection to important accounts.
- **Think before you click.** Be cautious with unexpected and urgent emails, texts, links, and attachments.
- **Keep devices and apps updated** with security updates and patches for your operating system, apps, browsers, and other devices as soon as practical.

Questions For Organizations

- Do we have **visibility into our critical technology and vendors**?
- Do we know **who has remote access** to critical systems?
- Are our **IT and OT environments properly segmented**?
- Do we verify the **source and integrity of software and firmware updates**?
- Could a **vendor or supply-chain compromise** disrupt essential operations?
- Do we have **tested continuity plans** for an extended power or technology outage?

Questions For Individuals

- **What am I sharing online?** Could information I post publicly help someone guess my passwords, answer security questions, impersonate me, or target me with a scam?
- **Who has access to my accounts?** Have I reviewed old accounts, connected apps, browser sessions, and devices that may still have access?
- **What happens if I lose my phone or laptop?** Are my devices protected with a strong passcode, encryption, and the ability to locate or remotely wipe them?

Additional Resources:

Oregon Emergency Response System
(OERS) 1-800-452-0311

Cybersecurity & Infrastructure Security Agency (CISA)
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
Portland Office 503-224-4181
<https://www.ic3.gov/fbi.gov/contact-us/field>

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

State of Oregon Security Operations Center
503-378-5930 | css.soc@eis.oregon.gov

National Institute of Standards and Technology (NIST)
<https://www.nist.gov/cybersecurity-and-privacy>



For more information on strengthening your cybersecurity posture, refer to the FBI's Operation Winter SHIELD guidance.

<https://www.fbi.gov/investigate/cyber/wintershield>

