



Security Bulletin

TLP: WHITE

February 16, 2022

NPCC is publishing this security bulletin to engage and inform NPCC entities on aspects of Bulk Power System security and reliability.

CISA Alert: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

In early January, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) have issued and updated their Alert on Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. This alert provides the following information:

- Technical Details: common tactics and vulnerabilities used by Russian state-sponsored advanced persistent threat (APT)
- Detection: recommended methods
- Preparation: procedural actions, suggested cyber posture enhancements and cyber incident response plan recommendations
- Resources for nation-state threat overviews and advisories

CISA Link: [Alert \(AA22-011A\) Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure](#)

CISA SHIELDS UP: <https://www.cisa.gov/shields-up>

TLP: WHITE

NPCC assumes no responsibility for any material, e.g., information, data, text, software, graphics et cetera, of computer "links" to sites hosted by third parties that are outside of NPCC's control. NPCC does not endorse products, services, or information provided by third parties and shall not be responsible or liable, directly, or indirectly, for any damage or loss caused or alleged to be caused by or in connection with, use or reliance on any content available on or through any third-party site. Further, the inclusion of links to third party websites within this Security Bulletin does not imply that the owners of such third party websites have given permission for inclusion of these links, or otherwise sponsored or endorsed NPCC's Security Bulletin.

NPCC is not responsible for the accessibility of third party websites via the Security Bulletin. Should you discover that a third party link on a Security Bulletin is broken, no longer pointing to the content so indicated on the Security Bulletin, or points to a third party website containing infringing content, malicious code, or any offensive, libelous, or otherwise illegal or inappropriate content, email: support@npcc.org. To ensure NPCC can quickly respond to the issue, your email should include the originating Security Bulletin, the linked page URL and a description of the content in question.