NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Security Bulletin

TLP: WHITE

July 7, 2021

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

CISA's Ransomware Tool and NIST Ransomware Risk Management Framework

CISA's Ransomware Readiness Assessment (RRA) Tool

On June 30, 2021, CISA released a new module in its Cyber Security Evaluation Tool (CSET), RRA. This desktop software tool provides a step-by-step process to evaluate cybersecurity practices on IT and ICS networks.

- CISA CSET Tool Sets Sights on Ransomware Threat Announcement
- CISA Github Ransomware Readiness Assessment CSET v10.3

NIST Preliminary Draft Cybersecurity Framework Profile for Ransomware Risk Management

On June 9, 2021, NIST published a Preliminary Draft of NISTIR 8374 Cybersecurity Framework Profile for Ransomware Risk Management. The paper discusses ransomware challenges, cybersecurity resources, and provides a ransomware profile. The ransomware profile aligns organizations' ransomware prevention and mitigation objectives, risk appetite, and cybersecurity resources with the elements of the Cybersecurity Framework. The ransomware profile is broken down into the cybersecurity framework categories of identify, protect, detect, respond, and recover.

- NIST Cybersecurity Framework Profile for Ransomware Risk Management Announcement
- Preliminary Draft NISTIR 8374 Cybersecurity Framework Profile for Ransomware Risk Management

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.