



Security Bulletin

TLP: WHITE

March 30, 2022

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

Strengthening American Cybersecurity Act of 2022

On March 15th, 2022, the White House signed into law a federal cyberattack reporting requirement aimed at protecting critical infrastructure in the United States. Key aspects of the law:

- The law impacts 16 industry sectors which include energy.
- CISA will also act as a central hub for receiving private sector incident response reports, sharing threat data, and tracking the evolution of ransomware.
- Imposes a 72 hour notification of a covered cyber security incident (SEC. 2242).
- CISA will have the authority to subpoena companies within the identified industry sectors that fail to report cybersecurity incidents or ransomware payments.

United States Congress: [Strengthening American Cybersecurity Act of 2022](#)

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.