

Sponsors: Nebraska Public Power District; NMPP Energy, American Municipal Power; Ohio  
Municipal Electric Association

**Cybersecurity Incident Reporting for Electric Utilities**

1 Information sharing is a key pillar of cybersecurity. Industry and the federal government have mutual  
2 responsibilities to share cyber threat information with each other as a means to protect, prepare for, and  
3 respond to cybersecurity incidents. The electric sector is unique in that it has long been subject to cyber  
4 incident reporting mandates to the Department of Energy (DOE) via an Electricity Emergency Incident  
5 and Disturbance Report (OE-417) and the North American Electric Reliability Corporation (NERC) and  
6 the Federal Energy Regulatory Commission (FERC). Moreover, there is robust electric utility industry  
7 participation in information sharing organizations known as the Electricity Information Sharing and  
8 Analysis Center and the Multi-State Information Sharing and Analysis Center.

9  
10 Another layer of mandatory cyber incident sharing requirements will be added through the Cyber Incident  
11 Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Signed into law in March 2022, CIRCIA will  
12 require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware  
13 payments within 24 hours to the Department of Homeland Security’s Cybersecurity and Infrastructure  
14 Security Agency (CISA). This law is currently in the rulemaking stage of implementation at CISA.

15  
16 There have been numerous attempts in recent years to mandate additional layers of information sharing  
17 for electric utilities. While information sharing should be timely, excessively tight reporting windows  
18 would likely result in utilities overreporting, making it difficult if not impossible to get a meaningful  
19 signal through the noise. Information sharing mandates should be tightly focused on utilities and assets  
20 that, if targeted, could pose a high risk to national security. The federal government must recognize the  
21 administrative burden information sharing places on electric utilities of all sizes. Therefore, the federal  
22 government should prioritize sharing information internally across departments and agencies rather than  
23 asking electric utilities to report to multiple federal entities. Finally, the federal government must more  
24 openly share threat information it has with industry – far too often information sharing has been a one-  
25 way street, with the federal government demanding ever more information from industry without sharing  
26 any substantive or meaningful information itself.

27  
28 **NOW, THEREFORE, LET IT BE RESOLVED:** That the American Public Power Association (APPA)  
29 opposes consideration of additional statutory or regulatory cybersecurity incident reporting mandates until  
30 the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is fully implemented; and  
31

32 **BE IT FURTHER RESOLVED:** That APPA supports maintaining the Department of Energy (DOE) as  
33 the sector risk management agency for the electricity sector and for DOE to play an active role in  
34 implementing CIRCIA in a manner that is harmonized with existing reporting requirements (at DOE, the  
35 North American Electric Reliability Corporation, Federal Energy Regulatory Commission, Nuclear  
36 Regulatory Commission, and any other relevant agencies or departments); and

37

38 **BE IT FURTHER RESOLVED:** That APPA strongly encourages the Cybersecurity and Infrastructure  
39 Security Agency and DOE to take a careful and deliberative approach to implementation of CIRCIA,  
40 taking into account existing reporting mandates and organizations, and to appropriately tailor reporting  
41 mandates commensurate with risk to national security.

**Adopted at the Legislative & Resolutions Committee Meeting**

**February 27, 2024**

**Sunsets in March 2032**