HEADLINES

Staff Presentation | Notice of Proposed Rulemaking (NOPR) Regarding Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems

January 20, 2022

Docket No. RM22-3

Item E-1 | News Release

Item E-1 is a draft Notice of Proposed Rulemaking (NOPR) that proposes, pursuant to section 215(d)(5) of the Federal Power Act, to direct the North American Electric Reliability Corporation (NERC) to develop and submit for Commission approval new or modified Critical Infrastructure Protection (CIP) Reliability Standards that require internal network security monitoring for high and medium impact Bulk Electric System (BES) Cyber Systems.

The draft NOPR explains that the currently effective CIP Reliability Standards do not address internal network security monitoring, and this omission constitutes a gap in the CIP Reliability Standards. Currently, network security monitoring in the CIP Reliability Standards focuses on preventing unauthorized access to BES Cyber Systems at the network perimeter. Including internal network security monitoring requirements in the CIP Reliability Standards, as the draft NOPR proposes, would complement existing perimeter requirements for high and medium impact BES Cyber Systems by improving the visibility of communications inside the network.

The 2020 SolarWinds attack demonstrated how an attacker can bypass all network perimeter-based security controls traditionally used to identify the early phases of an attack. This supply chain attack leveraged a trusted vendor to compromise the networks of public and private organizations, and SolarWinds customers had no reason to suspect the installation of compromised updates because the attacker used an authenticated SolarWinds certificate.

In the event of a compromised Electronic Security Perimeter, early detection of an attack through internal network security monitoring reduces the time that an attacker has to gain a strong foothold and potential command and control of protected systems, including operational control over equipment like circuit breakers. Internal network security monitoring

increases the chance of early detection of malicious activity, which in turn allows for quicker mitigation and recovery from an attack. In addition to improved incident response capabilities and situational awareness, internal network security monitoring also contributes to better vulnerability assessments within an Electronic Security Perimeter, all of which support an entity's cybersecurity defenses and could reduce the impact of cyberattacks.

To address the current reliability gap and improve cybersecurity, the draft NOPR proposes to direct that NERC develop new or modified CIP Reliability Standards requiring that applicable responsible entities implement internal network security monitoring for their high and medium impact BES Cyber Systems.

While centered on high and medium impact BES Cyber Systems, the draft NOPR also seeks comments on the potential usefulness and practicality of implementing internal network security monitoring to detect malicious activity in networks with low impact BES Cyber Systems, including any potential benefits, technical barriers and associated costs. Among other specific questions, the draft NOPR seeks comment on possible criteria or methodologies for identifying an appropriate subset of low impact BES Cyber Systems that could benefit from internal network security monitoring.

Comments in response to the draft NOPR would be due 60 days following publication in the Federal Register.

This concludes our presentation. We are happy to take any questions you may have.

This page was last updated on January 20, 2022