crowell moring

CLIENT ALERT

Delayed Self-Report and Poor Internal Controls Lead to Greater Penalties

May.07.2019

The North American Electric Reliability Corporation (NERC) proposes to assess an unidentified entity a $356,000 penalty for violations of the CIP-006-3c NERC reliability standard which governs physical security of cyber assets. The violation lasted 13 months and was determined to pose a serious risk to reliability. The case highlights the importance of following up promptly with NERC when violations are identified. Although the violations were self-reported, the entity received no credit for self-reporting because it waited too long to do so. The case also highlights the importance of having effective internal controls to ensure compliance.

According to NERC's Notice of Penalty (NOP), the entity did not deploy security patches to systems that controlled physical access to several substations thereby allowing the potential for unauthorized access to vulnerable systems. There were multiple process failures. First, an incorrect setting in the system that deploys patches led to the failure to identify available patches upon release. Second, when those patches were identified a year later, the push package to deploy them failed due to unspecified operability issues. Finally, when manual installation was identified as a necessary step, the entity chose not to install the patches because it was concerned that rebooting the system that controlled physical access—which was at its end-of-life—would result in the system failing and there was no backup.

A key benefit of self-reporting a violation is to potentially obtain a reduced penalty. According to NERC, the entity waited 210 days before self-reporting, which made it ineligible for any self-report credit. NERC has stated that self-reports should be submitted "as soon as practical but typically within three months of discovery." NERC-registered entities should keep this window in mind when they are considering whether and when to self-report a potential violation.

Additionally, this NOP reaffirms the importance of NERC-registered entities having effective internal controls—an ongoing compliance theme as discussed here. According to the NOP, the entity's patch management program initially failed to identify necessary patches until one year after their release, and should have, but did not, identify the missing patches throughout that one-year period. Together, these infirmities called the entire patch process into question. These inadequate procedures led to the violations, which were deemed to have posed a serious risk to reliability due to the potential for unauthorized access to vulnerable systems. NERC-registered entities should periodically reassess their internal controls to confirm that they remain effective to ensure compliance.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Deborah A. Carpentier
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2857
Email: dcarpentier@crowell.com