Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Electric Grid Physical Security: Recent Developments

Updated February 7, 2023

On February 6, 2023, the Justice Department announced the arrest of two individuals for planning to attack five electric power transmission substations around Baltimore, MD, allegedly as part of a "racially or ethnically motivated violent extremist" conspiracy. On December 25, 2022, four electric distribution substations in the Tacoma, WA, area were physically attacked, allegedly by two malicious individuals in a burglary scheme, causing millions of dollars in damage and cutting power to some 30,000 utility customers. Three weeks earlier, unknown perpetrators attacked two substations in Moore County, NC, causing an extended blackout for 45,000 area customers. According to press analysis of Department of Energy (DOE) incident reports, such attacks are becoming more frequent. The Baltimore, Tacoma, and Moore County incidents are just the latest examples of physical threats against U.S. electric power infrastructure that have drawn attention among policymakers and prompted calls for more extensive grid security standards.

Federal Regulation of Grid Security

The Energy Policy Act of 2005 (P.L. 109-58) mandated the implementation of electric transmission reliability standards under new authority granted to the Federal Energy Regulatory Commission (FERC), the independent federal regulator of the interstate electric transmission system. The commission subsequently designated the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization certified to establish and enforce reliability standards—including security standards—for the U.S. electric transmission grid, subject to commission review. In 2008, FERC's Order 706 approved NERC's initial security standards for critical electric infrastructure; however, these standards primarily addressed cybersecurity, not physical security.

A 2013 rifle attack by unknown perpetrators on a high-voltage electric power substation in Metcalf, CA, revealed the need for physical security standards in addition to cybersecurity standards for electric power. In response to the Metcalf attack, as well as other grid incidents and findings from utility security exercises, Congress enacted provisions in the FAST Act (P.L. 114-94) to protect or restore the reliability of critical electric infrastructure during a grid security emergency. Congress also sought stronger physical security standards from FERC under the commission's existing statutory authority. Accordingly, on

Congressional Research Service
https://crsreports.congress.gov
IN12074

March 7, 2014, FERC issued Order 802 requiring NERC to promulgate new mandatory standards for the physical security of transmission critical infrastructure.

After consultation within the utility industry, NERC proposed a new Physical Reliability Security Standard in May 2014. FERC approved the initial standard the following November, as well as two subsequent revisions, the most recent (CIP-014-3) in 2022. The standard applies to electric transmission owners with assets operating at 500 kilovolts (kV) or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain criteria. It consists of six principal requirements, including risk assessments; threat and vulnerability assessments for critical facilities; implementation of physical security plans for critical facilities; and a process for compliance monitoring and assessment. (For more background and details about the development of the CIP-014 standard, see CRS Report R45135, *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?*)

Revisiting the NERC Standards

The targeted facilities in the Baltimore incident appear to be subject to NERC's physical security standards, with mandated physical security measures (e.g., protective walls) reportedly present in at least one of them. However, over the course of the emergency response to both the Moore County and Tacoma substation attacks, it became apparent that there was little physical security at those affected sites, which made it relatively easy for the perpetrators to disable them. Because the Moore County and Tacoma substations are part of local electric distribution systems rather than transmission systems, they are not under FERC's jurisdiction and not subject to NERC's standards. Rather, physical security at these substations is under the jurisdiction of state utility regulators.

Although the distribution substation attacks did not affect the regional transmission system, they nonetheless caused significant service outages and negatively impacted local communities. Consequently, some officials and Members of Congress have questioned whether states or the federal government should do more to prevent grid infrastructure attacks in the future. Likewise, on December 15, 2022, FERC issued an order directing NERC to submit a report within 120 days evaluating the adequacy of the applicability criteria and risk assessment provisions of CIP-014-3. The report must also examine whether a minimum level of physical security should be required for all electric transmission stations, substations, and primary control centers.

Congressional Initiatives

Even before the Tacoma and Moore County incidents, initiatives in the 117th Congress sought to bolster the physical security of the electric grid, including electric distribution. The Infrastructure Investment and Jobs Act (IIJA, P.L. 117-58) includes provisions to provide financial assistance to states for developing and implementing state energy security plans to secure energy infrastructure "against all physical and cybersecurity threats" (§366). The act also requires DOE and the Department of Homeland Security to submit a report to Congress assessing "priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems," among other provisions (§40121). The Grid Security Research and Development Act (H.R. 4939) would have directed DOE and other agencies to conduct a research, development, and demonstration program to protect the electric grid, "including assets connected to the distribution grid," from physical attacks by increasing the security capabilities of the sector and accelerating relevant technology development.

The 118th Congress may continue to examine the state of electric grid physical security, including the security of grid infrastructure not currently subject to NERC's existing security standards. Among many specific issues of potential interest, Congress may consider the evolving physical threat environment,

oversight of physical security implementation, the relationship between federal and state grid security initiatives, and the cost-effectiveness of security requirements. Congress may also examine tradeoffs between investments to "harden" grid infrastructure (e.g., physical barriers) and investments to make the grid more resilient to physical attacks (e.g., additional transmission lines). As CIP-014 implementation and other physical security initiatives proceed, Congress also may examine the power sector's overall progress in securing its infrastructure, including organizational and structural changes supporting physical security as a corporate priority.

Author Information

Paul W. Parfomak
Specialist in Energy Policy

Disclaimer