

# CRITICAL ELECTRIC INFRASTRUCTURE PROTECTION ACT

## Section by Section

### **Findings**

Congress finds: that the critical electrical infrastructure of the United States and Canada is valued at over \$1 trillion; that its functioning is highly dependent cyber control systems; that these control systems are increasingly connected to open networks, exposing them to cyber risks; that malicious actors pose a significant risk to this infrastructure; that intentional or naturally occurring electromagnetic pulse events also threaten this infrastructure; that according to news reports, this infrastructure has been penetrated by spies from China, Russia, and other countries; that utilities are underreporting their assets, potentially to avoid current cybersecurity compliance requirements; that a statutory mechanism is needed to protect this infrastructure; and that the former Chairman of the Federal Energy Regulatory Commission (FERC) testified to Congress that FERC needs additional legal authorities to protect this infrastructure.

- (a) **DEFINITIONS.**—Critical Electric Infrastructure, Critical Electric Infrastructure Information, Critical Infrastructure Information, Cyber Vulnerability, and Cyber Threat are defined.
- (b) **DETERMINATION OF THREAT TO CRITICAL ELECTRIC INFRASTRUCTURE.**—The Secretary of Homeland Security, working with other national security or intelligence agencies, may identify cyber vulnerabilities or threats that require immediate protective actions to be implemented by electric companies or authorities.
- (c) **ONGOING CYBER ASSESSMENT OF GRID.** —DHS shall perform ongoing cyber vulnerability and threat assessments to critical electric infrastructure, and produce reports with recommendations.
- (d) **COMMISSION AUTHORITY.**—FERC may issue rules or orders needed to protect critical electric infrastructure, and, if a cyber vulnerability or threat is imminent, may issue an emergency rule or order without prior notice or hearing.
- (e) **DURATION OF EMERGENCY RULES OR ORDERS.**—Emergency rules or orders shall remain effective for up to 90 days, unless the rule or order is opened to comment, and FERC subsequently affirms, amends, or repeals the rule or order.
- (f) **JURISDICTION.**—Any entity that owns, controls, or operates critical electric infrastructure shall be subject to FERC’s jurisdiction for purposes of this Act.
- (g) **PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.**—Information submitted to FERC pursuant to this act shall be protected in the same manner as Protected Critical Infrastructure Information, as defined under 6. U.S.C. 133 et seq.
- (h) **INVESTIGATION OF COMPROMISE OF CRITICAL ELECTRIC INFRASTRUCTURE.**— DHS shall conduct an investigation to determine if the security of Federally-owned critical electric infrastructure has been compromised. The investigation will focus on: extent of compromise; identification of attackers; method of penetration; ramifications of compromise; and recommended mitigation activities.
- (i) **EVALUATION OF EXISTING AUTHORITIES.**— The Secretary of Homeland Security shall evaluate the capacity and authority of DHS and other Federal agencies to protect critical infrastructure from cyber attack.