The Grid Reliability and Infrastructure Defense (GRID) Act

Summary

The GRID Act provides the Federal Energy Regulatory Commission (FERC) with the authority to issue grid security orders and rules to address physical, cyber, electromagnetic pulse, and other threats to and vulnerabilities of the bulk-power system and defense critical electric infrastructure.

Under the GRID Act:

1. If an imminent grid security threat is identified, FERC can issue emergency orders to protect the reliability of the bulk-power system—the facilities and control systems necessary for operating the grid's generation and transmission assets—and defense critical electric infrastructure.

2. If a grid security vulnerability is identified and FERC determines that it has not been adequately addressed through a grid reliability standard developed by the North American Electric Reliability Corporation (NERC), FERC can promulgate a rule or issue an order to protect against the vulnerability. NERC is provided an opportunity to present recommendations regarding the rule or order.

3. If a grid reliability standard subsequently developed by NERC and approved by FERC adequately addresses a grid vulnerability, FERC shall rescind its applicable rule or order when the reliability standard goes into effect.

4. Within 180 days, FERC shall promulgate a rule or issue an order in order to protect against the Aurora vulnerability.

5. Within one year, FERC shall require NERC to develop a reliability standard to ensure the availability of sufficient numbers of spare large transformers to promptly replace any large transformers that are destroyed or disabled as a result of a reasonably foreseeable physical or other attack or a geomagnetic storm.

6. Within 180 days, the President shall designate a list of up to 100 facilities located in the United States that are critical to the defense of the United States and vulnerable to a disruption of the supply of electricity provided to the facility by an external provider. If FERC identifies a defense critical facility vulnerability that is not adequately addressed, FERC may promulgate a rule or order to ensure such facility is protected, provided that the incremental cost of compliance is paid by the defense facility.

7. Sensitive information related to grid security threats or vulnerabilities and measures to address them is protected from public disclosure. Provisions to facilitate sharing of information between authorized parties are included.

8. The Department of Energy shall share technical expertise with utilities and facilitate the acquisition of adequate security clearances for key personnel.