Energy Reliability and Security Discussion Draft: Critical Electric Infrastructure Security

New Federal Authority to Address Grid Security Emergencies Would Be Most Effective by Focusing on Immediate Threats

Key Message

New federal authority is appropriate to address imminent grid security emergencies, but it is not necessary or appropriate for dealing with grid security *vulnerabilities* as those are addressed through the existing FERC/NERC process in coordination with owners and operators of the bulk-power system.

Background

Section 1204, Critical Electric Infrastructure Security, of Title I of the Committee's *Architecture of Abundance* discussion draft would give the Secretary of Energy new authority to address imminent grid security emergencies while facilitating the protection and voluntary sharing of critical electric infrastructure information.

It could be beneficial for a single federal agency – in this case the Department of Energy – to have authority to order specific emergency measures to protect the bulk-power system in the event of a real grid emergency. However, such emergency authority need not—and should not—be expanded further to include all types of grid vulnerabilities, which are already addressed under current law, industry standards and best practices.

Since 2005, Section 215 of the Federal Power Act has provided a statutory and regulatory framework for addressing bulk-power system reliability and cyber security. Under Section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities and government representatives, develops mandatory and enforceable reliability and security standards that apply across the international bulk power system. The Federal Energy Regulatory Commission (FERC) has authority to approve or remand those standards for modifications. Penalties for violating FERC-approved standards can reach $1 million per day per violation. The electric power industry is the only critical infrastructure sector with such standards.

Under Section 215, FERC, on its own initiative, can direct NERC to develop a standard to address a specific matter, which could include vulnerability issues. The Commission has exercised this authority in recent years with regard to geomagnetic disturbances and physical security, for example.

In response to concerns about the length of time it takes to develop standards, NERC has made continued improvements to shorten the time it takes develop its standards. Recently, the NERC standards development process proved successful in the development of physical security standards, which NERC and industry stakeholders crafted and approved for submission to FERC in 77 days.

Important Points

- Vulnerabilities are not the same as emergencies or threats, which involve a higher level of urgency and risk.
- Giving the Department of Energy emergency authority to address vulnerabilities would negatively impact the reliability regime established in section 215 of the Federal Power Act, which could result in duplicative, conflicting, or unworkable standards across the diverse North American grid and would undermine the effectiveness of NERC as an international standards-development body.
- Cybersecurity information sharing legislation that has already passed the House will provide government and the private sector important new tools and incentives to promptly share information about cyber threats and vulnerabilities. Sharing clear and actionable information about vulnerabilities and remediation strategies among affected stakeholders and public-private partnerships are the most effective ways to address all but the most urgent emergency situations.