

STAFF DISCUSSION DRAFT

[This discussion draft highlights the remaining areas of disagreement. Language not highlighted has been tentatively agreed to by FERC representatives and the industry associations that have participated, pending full agreement.]

110TH CONGRESS

2D SESSION **H. R.** _____

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity [FERC: and other national security] threats to the reliability of the bulk-power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. _____ introduced the following bill; which was referred to the Committee on _____.

A BILL

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity [FERC: and other national security] threats to the reliability of the bulk-power system, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Bulk Power System Protection Act of 2008”.

SEC. 2. FINDINGS.

The Congress finds that:

(1) it is in the public interest to require the Federal Energy Regulatory Commission to promptly order measures to address known cybersecurity threats to the reliability of the electric bulk power system; and

(2) the Commission must have the necessary emergency authority to respond promptly to future cybersecurity [FERC: and other national security] threats that could compromise reliability of the bulk power system.

SEC. 3. PROTECTION OF BULK POWER SYSTEM FROM CYBERSECURITY [FERC: AND OTHER NATIONAL SECURITY] THREATS.

Part II of the Federal Power Act is amended by adding the following new section after section 215:

“SEC. 215A. EMERGENCY AUTHORITY TO ADDRESS CYBERSECURITY [FERC: AND OTHER NATIONAL SECURITY] THREATS TO THE BULK POWER SYSTEM.

“(a) DEFINITIONS.—For purposes of this section:

“(1) The terms ‘reliability standard’, ‘bulk power system’, ‘reliable operation’, ‘cybersecurity incident’, ‘Electric Reliability Organization’, ‘regional entity’, and ‘owners, users or operators’ shall have the same meaning as when used in section 215.

“(2) The term ‘cybersecurity threat’ [FERC: means that there is credible information or evidence of (1) the likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; or (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act.]

[Assns: means that there is credible information or evidence of: (1) the substantial likelihood of a malicious act that could disrupt the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system; and (2) a substantial possibility of disruption to the operation of such devices and networks in the event of such a malicious act].

“(3) The term ‘national security threat’ means a threat to the bulk power system identified by and Federal law enforcement, national security, or intelligence agency of the United States. [Assns would delete this definition]

(3) The term ‘security-sensitive information’ means information that, if revealed to the public, could reasonably be expected to have a significant adverse effect on the health or safety of the public or the common defense or national security. The Commission may designate information as ‘security sensitive information’ for purposes of this section in consultation with national security or national intelligence agencies, as appropriate, but may not designate as security-sensitive information any information that has been classified by another Federal agency.

“(b) INTERIM AUTHORITY TO ADDRESS EXISTING [Assns: CYBERSECURITY] THREATS.—

(1) After notice and opportunity for comment, and after consultation with appropriate governmental authorities in Canada and Mexico [FERC: (subject to adequate protections against inappropriate disclosure of security-sensitive information)] [Assns: (subject to adequate protections against public disclosure of security-sensitive information)], the Commission shall establish, by rule or order, within 120 days of enactment of this section, such measures or actions as are necessary to protect the reliability of the bulk power system against the cybersecurity threats resulting from: (i) the vulnerabilities identified in the June 21, 2007 communication to certain “Electricity Sector Owners and Operators” from the North American Electric Reliability Corporation, acting in its capacity as the Electricity Sector Information Sharing and Analysis Center, and (ii) related remote access issues. Such measures or actions may be required of any owner, user or operator of the bulk power system within the United States.

2) Until such time as the interim reliability measures or actions ordered under this subsection are replaced by cybersecurity reliability standards developed, approved and implemented pursuant to section 215, the Commission may issue additional orders to supplement the initial rule or order issued under this subsection only if, based on subsequent information or petition from an affected entity, the Commission determines that clarification or refinements to the originally ordered measures or actions are necessary to ensure that the threats are adequately and appropriately addressed. Any such additional orders shall be preceded by notice and opportunity for comment.

“(c) FUTURE EMERGENCIES INVOLVING IMMEDIATE CYBERSECURITY THREATS AND CERTAIN OTHER THREATS TO RELIABILITY. [Assns would delete “and certain other threats to reliability”]

“(1) AUTHORITY TO ADDRESS IMMEDIATE [Assns: CYBERSECURITY] THREAT.— Whenever the President issues and provides to the Commission (either directly or through the Secretary of Energy) a written directive or determination that an immediate cybersecurity, [Assns would delete the following: , or other national security,] threat to the reliability of the bulk power system exists, the Commission may on its own motion, with or without notice, hearing, or report issue such orders for emergency measures or actions as are necessary in its judgment to protect the reliability of the bulk power system against such threat

“(2) CONSULTATION.—Before acting under this subsection, to the extent feasible, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with appropriate governmental authorities in Canada and Mexico [FERC: (subject to adequate protections against inappropriate disclosure of security-sensitive information)] [Assns: (subject to adequate protections against public disclosure of security-sensitive information)], entities described in paragraph (3), and officials at other Federal agencies,

including the Secretary of Energy, as appropriate, regarding implementation of measures or actions that will effectively address the identified threat [Assns would delete the following: and protect national security.]

“(3) APPLICATION OF EMERGENCY MEASURES.—An order for emergency actions or measures under this subsection may apply to the Electric Reliability Organization referred to in section 215 or a regional entity with respect to the United States operations of the Electric Reliability Organization or the regional entity, or any owner, user or operator of the bulk power system within the United States.

“(d) DISCONTINUANCE.— The Commission shall issue an order discontinuing any measures or actions ordered under subsections (b) or (c) upon the earliest of:

“(1) when the President (either directly or through the Secretary of Energy) issues a written order or directive provided to the Commission to the effect that the threat to the bulk power system that requires such measures, or actions no longer exists;

“(2) when the Commission determines in writing that the ordered measures or actions are no longer needed to address the identified threat;

“(3) when a reliability standard developed and approved pursuant to section 215 is implemented to address the identified threat; or

“(4) [FERC: with respect to orders under subsection (c), one year after the issuance of an order unless the President (either directly or through the Secretary of Energy) issues a determination reaffirming the

continuing nature of the threat, provided that the determination issued under this paragraph shall expire upon the implementation of a standard under section 215 to address the identified threat.] [Assns: one year after the issuance of an order under subsections (b) or (c) unless the President (either directly or through the Secretary of Energy) issues a determination reaffirming the continuing nature of the threat, provided, however, that the determination issued under this paragraph (D) shall expire upon the implementation of a standard under section 215 to address the identified threat.]

The Commission shall issue such order to be effective within 30 days of the relevant triggering event set out in subsections (1) through (4).

“(e) PROTECTION OF SECURITY-SENSITIVE INFORMATION.—

“(1) NONDISCLOSURE OF SECURITY-SENSITIVE INFORMATION.—Notwithstanding any other provision of law, if a rule or order issued under subsection (b) or (c) contains security-sensitive information or if information in the record associated with such rule or order constitutes security-sensitive information, the Commission may make the rule, order or information non-public in whole or in part. The Commission may disclose such non-public rule, order or information to entities other than the recipient of the rule or order as the Commission deems necessary as needed to carry out the rule or order and protect the reliability of the bulk-power system or for purposes of judicial review.

“(2) CONFIDENTIALITY PROCEDURES.— The Commission shall develop procedures

(i) for maintaining confidentiality of security-sensitive information contained in any document or pleading filed with the Commission in response to a proceeding initiated under, or a rule or order issued under, subsection (b) or (c) and may make non-public, in whole or in part, any document or pleading containing security sensitive information. The Commission may disclose all or any part of such document or pleading as necessary to carry out a rule or order under this section and protect the reliability of the bulk-power system or for purposes of judicial review; and

(ii) governing the confidentiality of information deemed to be security-sensitive. The procedures developed by the Commission shall ensure, to the extent consistent with national security, that information may be shared by entities subject to Commission action under this section with their employees, contractors and third-party representatives (including trade associations), to the extent necessary to enable such entities to implement Commission orders or measures and to protect their rights, including the right to judicial review.

Such procedures shall be issued in an order of the Commission on an interim basis after consultation with affected entities and their representatives and shall subsequently be subject to a rulemaking initiated within 120 days of the date that the interim rules take effect.

“(f) REVIEW.— The Commission will act expeditiously to resolve all applications for rehearing of orders issued pursuant to this section which are filed under section 313(a). Any person or other entity seeking judicial review pursuant to section 313 may obtain such review only in the United States Court of Appeals for the District of

Columbia Circuit. In the case of any petition for review involving rules or orders containing or relating to security-sensitive information, the Commission and parties must develop with the court appropriate measures to ensure the confidentiality of such information, including, but not limited to, court filings under seal or otherwise in non-public form, or judicial review in camera.

(g) Enforcement Discretion. The Commission shall exercise its discretion in engaging in enforcement actions under this section to recognize good faith efforts to comply with directives of the Commission.

[Amend Section 201(b)(2) – add “section 215A” to the listing of applicable sections.]