

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. IC08-725C-000]

Proposed Information Collection and Request for Comments

(December 7, 2007)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Request for Office of Management and Budget Emergency Processing of proposed information collection and request for comments.

SUMMARY: The Federal Energy Regulatory Commission (Commission) is providing notice of its request to the Office of Management and Budget (OMB) for emergency processing of a proposed collection of information in connection with steps being taken by the electric industry to address potential cyber vulnerabilities, and is soliciting public comment on that information collection.

DATES: The Commission and OMB must receive comments on or before [**30 days after publication in Federal Register**].

ADDRESSES: Send comments to:

(1) Nathan Frey, FERC Desk Officer, Office of Information and Regulatory Affairs, Office of Management and Budget. Mr. Frey may be reached by telephone at (202) 395-7345.

(2) Michael Miller, Office of the Executive Director, ED-30, Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426. Mr. Miller may be reached by telephone at (202) 502-8415 and by e-mail at

michael.miller@ferc.gov.

FOR FURTHER INFORMATION CONTACT: Jonathan First, Office of the General Counsel, Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426. Mr. First may be reached by telephone at (202) 502-8529 and by e-mail at jonathan.first@ferc.gov.

SUPPLEMENTARY INFORMATION: A recent experiment conducted for the Department of Homeland Security by the Idaho National Laboratory demonstrated that under certain conditions energy infrastructure could be intentionally damaged through cyber attack. In that experiment, researchers caused a generator to malfunction through an experimental cyber attack. This potential cyber vulnerability, which was recently broadcast on CNN, was the subject of an October 17, 2007 hearing before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House of Representatives.

The Commission intends to immediately issue a directive that requires all generator owners, generator operators, transmission owners, and transmission operators that are registered by the North American Electric Reliability Corporation (NERC) and located in the United States to provide to NERC certain information related to actions they have taken or intend to take to protect against the potential cyber vulnerability discussed above. The Commission will also require NERC to make this information available for Commission review.

Section 215 of the Federal Power Act, 16 U.S.C. 824o, vests the

Commission with authority over the Electric Reliability Organization (ERO) and over the users, owners and operators of the Bulk-Power System for purposes of approving and enforcing mandatory Reliability Standards. Under section 215, the term “Reliability Standard” includes requirements for the cyber security protection of the Bulk-Power System. Moreover, the Commission is charged not merely with approving (or remanding) Reliability Standards filed by the ERO, but also with ordering the ERO to submit a proposed standard or a modification to an existing standard that “addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.”

A number of efforts are underway to secure the Nation’s electric infrastructure against potential cyber vulnerabilities. One such effort is an advisory issued by NERC, acting through the Electric Sector-Information Sharing and Analysis Center (ES-ISAC), to generator owners, generator operators, transmission owners, and transmission operators. This advisory identified a number of short-term measures, mid-term measures and long-term measures designed to mitigate the potential cyber vulnerability discussed above.

It has been represented that a number of entities are already either secured against the potential cyber vulnerability referred to above or have taken steps to mitigate this vulnerability, and NERC has since sent a data request to industry members. That data request is limited in scope. It is essentially a request that industry members indicate if their mitigation plans are “complete,” “in progress,” or “not performing.” This information is not sufficient for the Commission to

discharge its duties under section 215 of the Federal Power Act because it does not provide information on what facilities are the subject of the mitigation plans, what steps to mitigate the potential cyber vulnerability are being taken, when those steps are planned to be taken, and, if certain actions are not being taken, why not.

In sum, given the seriousness of this potential vulnerability and given that the NERC data request does not provide information that the Commission needs to discharge its statutory responsibilities, the Commission believes further action is necessary in order to ensure that the owners and operators of the Bulk-Power System have taken or are taking appropriate steps to protect the Bulk-Power System.

Section 307 of the Federal Power Act, 16 U.S.C. 825f, authorizes the Commission to “investigate any facts, conditions, practices, or matters which it may find necessary or proper . . . to aid in . . . prescribing rules or regulations [under the Federal Power Act], or in obtaining information to serve as a basis for recommending further legislation.” Section 39.2(d) of the Commission’s regulations, 18 CFR 39.2(d), requires owners and operators to “provide the Commission . . . such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission.”

The Commission believes that the information that will be requested is critical to ensuring that appropriate mitigation of this potential cyber vulnerability is put in place and that it is put in place as quickly as possible. The Commission believes that an accurate overview of the actions taken and expected to be taken in

the industry is a necessary first step to determine whether any further measures need to be taken by the Commission to ensure the safety and reliability of the Bulk-Power System. The Commission is very sensitive to the need to preserve confidentiality of the information requested and the need to minimize the burden on industry. Accordingly, the information will be examined on-site at NERC headquarters, and disclosure by NERC will be on a need-to-know basis to NERC personnel and the Commission and its staff.

Respondents will provide the information listed below to NERC, which will secure the information and treat the responses as nonpublic information available, as noted above, on a need-to-know basis to NERC personnel and to the Commission and its staff. Following Commission review, the information will be returned to the submitters.

Each respondent will be required to provide the following information to NERC:

1. a copy of the owner or operator's plan for responding to the cyber vulnerability outlined in the ES-ISAC advisory, along with a general description of the facility for each plan,
2. a description of the measures – short-term, mid-term, and long-term – taken or planned to be taken (and the timeframe for implementing such measures) as recommended by the ES-ISAC advisory to mitigate the risks associated with this cyber vulnerability including projected completion dates if they fall outside the ES-ISAC advisory deadlines,
3. an explanation of how the plan and measures described above secure the owners or operators' facilities against this cyber vulnerability, and

4. if an owner or operator believes no actions are necessary regarding a measure, an explanation why it believes that to be so, along with a general description of the facility that the respondent proposes to exempt from actions under the advisory.

The Commission estimates that it would take each respondent no more than 12 hours to generate the requested information. The Commission estimates that the number of respondents will be approximately 1,150. Therefore, the total number of hours it would take to comply with the reporting requirement would be 13,800. The Commission estimates a total cost of \$1,214,400 to respondents @ \$88 per hour, based on salaries for professional and clerical staff, as well as direct and indirect overhead costs.

The Commission has submitted this reporting requirement to OMB for approval. OMB's regulations describe the process that federal agencies must follow in order to obtain OMB approval of reporting requirement. See 5 CFR Part 1320. The standards for emergency processing of information collections appear at 5 CFR 1320.13. If OMB approves a reporting requirement, then it will assign an information collection control number to that requirement. If a request for information subject to OMB review has not been given a valid control number, then the recipient is not required to respond.

OMB requires federal agencies seeking approval of reporting requirements to allow the public an opportunity to comment on the proposed reporting requirement. 5 CFR 1320.5(a) (1) (iv). Therefore, the Commission is soliciting comment on:

(1) Whether the collection of the information is necessary for the proper performance of the Commission's functions, including whether the information will have practical utility;

(2) The accuracy of the Commission's estimate of the burden of the collection of this information, including the validity of the methodology and assumptions used;

(3) The quality, utility, and clarity of the information to be collected; and

(4) How to minimize the burden of the collection of this information on respondents, including the use of appropriate automated electronic, mechanical, or other forms of information technology.

Kimberly D. Bose,
Secretary.