HENRY A. WAXMAN, CALIFORNIA
CHAIRMAN

JOE BARTON, TEXAS
RANKING MEMBER

ONE HUNDRED ELEVENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

MEMORANDUM

March 22, 2010

To: **Members of the Subcommittee on Energy and Environment**

Fr: **Committee on Energy and Commerce Democratic Staff**

Re: **Subcommittee Markup of Committee Print on the Home Star Energy Retrofit Act of 2010, Committee Print on the Grid Reliability and Infrastructure Defense (GRID) Act, and H.R. 4451, the Collinsville Renewable Energy Promotion Act**

On Wednesday, March 24, 2010, at 9:30 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittee on Energy and Environment will meet in open markup session to consider a Committee print on the Home Star Energy Retrofit Act of 2010, a Committee print on the Grid Reliability and Infrastructure Defense (GRID) Act, and H.R. 4451, the Collinsville Renewable Energy Promotion Act. The text of these measures is attached.

I. COMMITTEE PRINT-THE HOME STAR ENERGY RETROFIT ACT OF 2010

A. Background

HomeStar is a proposal designed to increase economic opportunity in construction and related sectors while improving building energy efficiency in the United States. In December 2009, the President's Economic Recovery Advisory Board released a memorandum outlining a HomeStar program that would serve to quickly create construction-related jobs based on existing technology and labor skills. The proposal earned broad national support, including support from corporations such as Owens Corning, Dow, Home Depot, Lowes, Marvin Window and Doors, Fortune Brands, and MASCO, and home energy performance contractors in almost every state. Additional supporters include the Alliance to Save Energy, the Laborers' International Union of North America, and the 744 nationwide members of Efficiency First. The proposal has been endorsed by the National Association of Manufacturers, the U.S. Chamber of Commerce, the Natural Resources Defense Council, the American Council for an Energy Efficient Economy, and many other organizations.

A legislative hearing was held in the Subcommittee on Energy and Environment on Thursday, March 18, 2010. Witnesses testified representing the Department of Energy, WellHome Corporation, the National Association of Manufacturers, Owens-Corning Corporation, and the National Association of Homebuilders.

B. Summary of Committee Print

The HomeStar proposal offers two programmatic paths to incentivize energy efficient retrofitting: the Silver Star path and the Gold Star path. The Silver Star path offers rebates to homeowners for the purchase and installation of specified energy efficiency products including heating systems, insulation, and water heaters. Homeowners could receive rebates totaling up to half of their project costs, up to a maximum of $3,000 per home. The Gold Star path offers incentives to homeowners who undertake retrofits that demonstrate at least a 20% reduction in whole-home energy consumption. Under the Gold Star path, homeowners can be reimbursed $3,000 to cover half the cost of a project that reduces whole-home energy use by 20%, with additional rewards of $1,000 for each additional 5% improvement up to a maximum of $8,000, depending on the level of energy efficiency achieved.

The Silver Star and Gold Star paths will be primarily supervised at the state level, with the Secretary of Energy providing program management where states opt not to do so. All rebates will be processed and paid through a central system established and operated by the Department of Energy, and based on data provided by a network of rebate aggregators. The program provides financial support to states to perform quality assurance programs that will determine eligible contractors, verify compliance with Silver Star and Gold Star programs, target small businesses, and support workforce training.

As vendors and contractors complete Silver Star and Gold Star retrofit work, they pass the rebates to the homeowner, and submit rebate forms to rebate aggregators, who are supervised by the Secretary and subject to criteria developed by the quality assurance program. Vendors and contractors are reimbursed within 30 days after receipt of the rebate form. To prevent fraud, rebate aggregators check the validity of the rebate forms and consult with homeowners and quality assurance providers. A certain percentage of Silver Star and Gold Star retrofits are selected randomly and reviewed by quality assurance providers to ensure correct installation and performance.

HomeStar also offers an energy efficiency loan program to leverage private investment to create a strong market for home energy retrofits. The Department of Energy will offer financial support to states that allow qualified financing entities to make loans available for Silver Star and Gold Star projects.

II. COMMITTEE PRINT-GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT (GRID ACT)

A. Factual Background

The U.S. electric grid consists of interconnected transmission lines, local distribution systems to deliver electricity to end-users, generation facilities, and related communications systems. The components of the grid are highly interdependent, such that a line outage or system condition problems in one area can lead to reliability concerns in other areas. In addition, the operations controls over the transmission grid and generators are increasingly managed by computer systems (notably Supervisory Control and Data Acquisition, or SCADA systems) linked to the Internet or other communications systems and to each other. The grid's increasing reliance on automation and two-way communications increases its vulnerability to remote cyber attacks. The rise of advanced metering and other "smart grid" capabilities amplifies these concerns.

Public reports relating to cyber vulnerabilities of and threats to the grid have increased in recent years and have been the subject of several congressional hearings in this Congress and the prior Congress. Perhaps most notable are reports on what is known as the AURORA vulnerability. In 2006, the Department of Homeland Security's Control Systems Security Program conducted an analysis – performed by the Department of Energy's Idaho National Laboratory – that came to be known as AURORA. This analysis demonstrated that an attacker could hack into the control system of an electric generator or other rotating equipment connected to the grid and throw the equipment out of phase, causing severe physical damage to the equipment.

In addition, it has been reported that China, Russia, and other nations have conducted cyber "probes" of U.S. grid systems, and that cyber attacks have been conducted against critical infrastructure in other countries. Cyber attacks may create instant effects at very low cost, and are very difficult to positively attribute back to the source. These features could make such attacks attractive not only for criminal purposes, but also as a possible element of future national hostilities.

There also has been growing attention to physical vulnerabilities of the grid. For example, large transformers essential to the reliable operation of the grid are manufactured outside of the United States and replacement may require two years. A limited number of spare, large transformers are available within the United States, and industry has developed a voluntary program (the Spare Transformer Equipment Program, or "STEP") providing for sharing of such assets in the event of a terrorist attack.

A special subset of physical vulnerabilities and threats is associated with electromagnetic pulse (EMP), of which there are three general categories: (1) intentional electromagnetic interference (IEMI) from portable (vehicle-borne or even suitcase-sized) equipment that uses high-power radio frequency or microwave pulses to destroy or temporarily disable electronic equipment; (2) geomagnetic storms resulting from solar activity; and (3) EMP caused by a high-altitude detonation of a nuclear weapon.

Measures that protect against IEMI and geomagnetic storms also offer protection against an EMP from high-altitude nuclear detonation.

The vulnerabilities of the electric grid present substantial risks to military assets. A 2008 report by the Defense Science Board's Task Force on DoD Energy Strategy concluded that:

> critical missions … are almost entirely dependent on the national transmission grid. About 85% of the energy infrastructure upon which DoD depends is commercially owned, and 99% of the electric energy DoD installations consume originates outside the fence. ... In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.[1]

B. Regulatory Background

Section 215 of the Federal Power Act, enacted as part of the Energy Policy Act of 2005, provides for the establishment of mandatory reliability standards for the bulk-power system, including standards addressing cybersecurity threats. Under Section 215, the North American Electric Reliability Corporation (NERC) is responsible for proposing, for FERC review and approval, reliability standards to protect and enhance the reliability of the bulk-power system, including cybersecurity standards. NERC is a not-for-profit corporation, the principal members of which are electric utilities and other stakeholders in the electric sector. NERC develops standards on an open basis through its Standards Committee, which is composed of member representatives. NERC also operates the Electric Sector Information Sharing and Analysis Center (ES-ISAC), which works to communicate with electric sector stakeholders on cross-industry threats, vulnerabilities, and protective strategies. Canadian (and to a lesser extent Mexican) utilities participate in the bulk power system with U.S. entities, participate in NERC, and have agreed to be subject to NERC-adopted standards. They are not, however, subject to FERC jurisdiction.

Reliability standards developed by NERC and approved by FERC under section 215 apply to the users, owners, and operators of the bulk-power system and are mandatory and subject to enforcement by the Commission with respect to U.S. entities. FERC cannot prescribe standards under section 215, but it has authority to direct NERC to develop standards or to modify existing standards. Importantly, the scope of these standards is limited by section 215's definition of the "bulk-power system," which specifically excludes "facilities used in the local distribution of electric energy" and facilities in Alaska and Hawaii. Accordingly, these standards do not apply to lower-voltage distribution facilities that normally serve military installations and other end-users of electricity.

---

[1] Department of Defense, *Report of the Defense Science Board Task Force on DoD Energy Strategy, More Fight – Less Fuel*, at 18 (Feb. 2008).

To date, FERC has approved nine Critical Infrastructure Protection (CIP) Reliability Standards developed by NERC. With regard to cybersecurity, the CIP standards address critical cyber asset identification, security management controls, personnel and training, electronic security perimeters, physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. In approving these standards, FERC directed that NERC develop revised standards – including a first phase of high-priority modifications and a second phase. On September 30, 2009, FERC approved Phase I of the modifications to the standards. The second phase is currently under development. With regard to malicious physical attacks on the bulk power system, the sole NERC standard is one that requires reporting within industry and to government of disturbances or unusual occurrences, suspected or determined to be caused by sabotage.

C. Summary of Committee Print

H.R. 2165, the Bulk Power System Protection Act of 2009, was introduced by Mr. Barrow (with Mr. Waxman and Mr. Markey as co-sponsors) on April 29, 2009. On October 27, 2009, the Energy and Environment Subcommittee held a legislative hearing on this bill and related legislation. In preparation for that hearing, the Subcommittee convened a classified briefing on grid security vulnerabilities and threats for members of the full Energy and Commerce Committee and staff with appropriate clearances.

After the hearing, the majority and minority staffs of the Subcommittee and full Committee continued their joint effort to develop bipartisan grid security legislation. The Committee print reflects the results of these bipartisan staff discussions and may be subject to change based on input from and consultations with members.

The Committee print would amend the Federal Power Act to add a new Section 215A, giving FERC new authorities to protect the electric grid against cyber and other threats and vulnerabilities. Subsection (b) of the new Section 215A gives FERC authority to issue emergency orders if the President notifies the Commission that a "grid security threat" exists. A grid security threat is a substantial likelihood of a cyber attack, electromagnetic weapon attack, a geomagnetic storm, or a direct physical attack on the bulk power infrastructure that would have a significant adverse effect on the reliability of the bulk power system or defense critical electric infrastructure. An emergency order is discontinued when the President determines the grid security threat no longer exists, FERC determines the emergency measures are no longer needed to protect against the threat, or one year elapses from the date the order was issued, unless the President reaffirms that the threat continues to exist (which the President may do for an additional period of up to one year on a rolling basis).

Subsection (c) of the new Section 215A gives FERC, after notice and opportunity for comment, authority to require measures to protect against grid vulnerabilities to cyber and electromagnetic weapon attacks if FERC determines that NERC reliability standards do not adequately address such vulnerabilities. If NERC later submits an adequate

standard, the corresponding FERC standard must be rescinded. The Committee print also requires FERC to direct NERC to submit for FERC approval reliability standards under section 215 (1) to protect the bulk power infrastructure against geomagnetic storms and (2) to require adequate availability of large transformers to ensure the reliability of the bulk power system in the event of a physical or other attack or a geomagnetic storm. The large transformer standard must allow compliance entities to choose to comply either individually or jointly (e.g., through a spare transformer sharing program). Both standards must balance risks and the cost of protecting against those risks.

Subsection (d) of the new Section 215A directs the President to designate not more than 100 facilities located in the United States that are the most critical to the defense of the United States and most vulnerable to interruption of an external supply of electricity to the facility. If FERC identifies a vulnerability in infrastructure serving such facilities to a cyber or electromagnetic weapon attack that has not adequately been addressed, FERC has authority to require measures to protect such infrastructure. Infrastructure can be exempted from this authority, on a case-by-case basis, if FERC, in consultation with the owner or operator of the designated critical facility, determines that such infrastructure is adequately protected.

The Committee print also includes provisions to protect sensitive information and provide for Department of Energy assistance to industry in protecting the grid and obtaining information regarding grid security threats and vulnerabilities.

III. H.R. 4451, THE COLLINSVILLE RENEWABLE ENERGY PROMOTION ACT

A. Background

The Upper and Lower Collinsville Dams on the Farmington River were built to provide hydroelectric power to an ax factory, which was shut down in 1966. The dams have not produced power since that time, but continue to block upstream fish passage.

On February 23, 2001, FERC issued original licenses to Summit Hydropower to redevelop hydroelectric power capacity at these dams. The Upper Collinsville Dam project was to have a generation capacity of 373 kilowatts, while the Lower Dam was to have a capacity of 920 kilowatts. As part of this licensing process, an environmental assessment was completed. The licenses required Summit to commence project construction within two years from the issuance of the licenses.

Section 13 of the Federal Power Act requires licensees to commence construction of hydroelectric projects within the time fixed in the license, which shall be no more than two years from the issuance of the license, and authorizes the Commission to issue one extension of the deadline, for no more than two years.

On November 26, 2002, FERC granted Summit a two-year extension to commence project construction at both sites, moving the deadline to February 23, 2005.

Because construction did not commence by that date, the Commission terminated the licenses on December 4, 2007.

In November 2006, Congress added a segment of the Farmington River that contains the two dams to the list of rivers under study for eligibility for designation as a Partnership National Wild and Scenic River. The study is ongoing. However, the Farmington River Watershed Association does not expect the segment containing the dams to be included in the final request to Congress for designation. The Wild and Scenic Study Committee does not oppose the legislation.

The town of Canton, Connecticut intends to proceed with the two hydroelectric projects that were not completed by Summit. On January 9, 2009, FERC granted the town a preliminary permit to undertake the necessary feasibility studies. The town has said that it intends to pursue Low Impact Hydropower Institute certification for the projects and provide for fish passage.

B. Summary of H.R. 4451

Rep. Christopher Murphy introduced H.R. 4451, the Collinsville Renewable Energy Promotion Act, on January 13, 2010. The bill authorizes FERC to reinstate the terminated licenses for the Upper and Lower Collinsville Dams hydroelectric projects and to extend for two years the date by which the licensee is required to commence construction. If FERC exercises this authority for either of the two licenses, the bill requires FERC to transfer such license to the town of Canton. Before taking these actions, the bill requires FERC to complete an environmental assessment for the projects to update the environmental analysis that was previously performed.

After a 30-day public comment period, FERC is required to consider the public comments on the environmental assessment and incorporate terms and conditions in the reinstated licenses that the Commission determines are necessary based on the public comments. FERC is required to make a final decision regarding the reinstatement within 270 days of the date of enactment of the Act. If FERC reinstates the licenses and extends the deadline for commencing construction, the transfer of the licenses to the town of Canton must also take place within 270 days of the date of enactment of the Act.