



2. **CYBERSECURITY: Lawmakers taking on cyber attacks, nuclear threats (06/01/2011)**

Hannah Northey, E&E reporter

Security gaps that hackers or terrorists could use to manipulate energy infrastructure, the electric grid, nuclear reactors and even the U.S. military have triggered a rare bipartisan legislative push from Congress and the White House.

The cooperative effort arrives amid repeated messaging on Capitol Hill from lawmakers, top federal energy regulators and industry groups: The electric grid is vulnerable and so is the United States' energy infrastructure.

Under continued grilling from Rep. Ed Markey (D-Mass.), federal officials conceded before the House Energy and Commerce's energy and power subcommittee yesterday that the country's 104 nuclear reactors are in many cases less secure than in the past and that "smart grid" technology is making the electric grid increasingly vulnerable to hackers.

"When it comes to national security, the process ... is too slow, it's too open, and it's too unpredictable," said Joseph McClelland, director of the Federal Energy Regulatory Commission's Office of Electric Reliability.

McClelland has repeatedly said FERC needs broader authority to take evasive action and deal with emergencies, although industry groups are pushing back somewhat on federal intervention in the electric sector. Gerry Cauley, president of the North American Electric Reliability Corporation, said the current system is sufficient to deal with the threats and that FERC already has the ability to order NERC to address vulnerabilities.

But Rep. Ed Whitfield (R-Ky.), the panel's chairman, pointed to a cyber attack in February that has been dubbed the "Night Dragon" and believed to have emanated from China. Although it was not overly sophisticated, the hackers succeeded in using Chinese Internet services to steal proprietary data from six U.S. and European energy companies, including Exxon Mobil Corp., Royal Dutch Shell PLC, BP PLC, Marathon Oil Corp., ConocoPhillips and Baker Hughes Inc. ([Greenwire](#), Feb. 24).

Whitfield called the attack the "tip of the iceberg" and the committee said that intelligence officials have revealed that countries like China and Russia are engaged in cyber espionage to probe the electric grid, posing a threat to the country's power, water supply and telecommunication systems -- all of which the U.S. military depends on.

Markey said the vulnerabilities could also provide an advantage to terrorist groups like al-Qaida. "We know there are many, many Ph.D.s inside of al-Qaida, whether we like it or not," he said.

Legislative push

House and Senate committees are firming up discussion drafts and some panels have introduced legislation to combat threats to the electric grid, including physical attacks, electromagnetic pulses from solar activity or nuclear weapons, and the destruction of large numbers of transformers, to name a few.

The House Energy and Commerce subcommittee is circulating its draft legislation, dubbed the "GRID Act," which mirrors legislation that House Energy and Commerce Chairman Fred Upton (R-Mich.) and Markey co-sponsored last Congress. The measure passed the House but stalled in the Senate.

The draft bill grants FERC cyber and physical authority over the bulk power system if the president declares an imminent threat to the grid and enables the agency to conduct rulemakings to address those vulnerabilities.

FERC would also have authority over distribution-level facilities that are currently outside its regulatory scope and could direct NERC to develop reliability standards to ensure the United States has a sufficient stockpile of transformers available if the equipment is damaged.

Earlier this month, the Obama administration sent Congress a long-awaited set of proposals to safeguard the grid, as requested by Senate Majority Leader Harry Reid (D-Nev.) and six Senate committee leaders who had asked the president for input.

The White House is calling for operators of transmission lines and other critical energy infrastructure to hire third-party commercial auditors to assess their cybersecurity risk mitigation plans ([E&ENews PM](#), May 12).

At a Senate hearing last week, administration officials agreed that Obama's proposals are reflected in cybersecurity legislation before the Senate Homeland Security and Governmental Affairs Committee introduced by Sen. Joe Lieberman (I-Conn.), chairman of the committee, ranking member Susan Collins (R-Maine) and Sen. Tom Carper (D-Del.).

Both the administration and the Senate bill would direct the Department of Homeland Security to protect critical infrastructure such as the electric grid.

Separately, the Senate Energy and Natural Resources Committee approved a cybersecurity measure that would broaden FERC's authority over critical distribution networks, including generation, transmission or distribution equipment affecting interstate commerce that regulators consider vital to U.S. security and safety ([E&E Daily](#), May 31).

Advertisement



The advertisement features a circular logo on the left with a scale of justice and the text 'NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS'. The main text reads 'NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS SUMMER COMMITTEE MEETINGS' in large, bold letters. Below this, it says 'JULY 17 - JULY 20, 2011 • LA LIVE JW MARRIOTT • LOS ANGELES, CALIFORNIA' and 'www.naruc.org/summer'. The background is a light green and blue gradient with two white sailboats on the right.



ClimateWire

ENVIRONMENT
& ENERGY DAILY

Greenwire

Land Letter

E&ENEWS PM

EETV

The Premier Information Source for Professionals Who Track Environmental and Energy Policy.

© 1996-2011 E&E Publishing, LLC [Privacy Policy](#) [Site Map](#)
