

**OPENING STATEMENT, AS PREPARED
CHAIRWOMAN YVETTE D. CLARKE (D-NY)
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
COMMITTEE ON HOMELAND SECURITY**

“SECURING THE MODERN ELECTRIC GRID FROM PHYSICAL AND CYBER ATTACKS”

**TUESDAY, JULY 21, 2009
2:00 P.M. IN 311 CANNON HOUSE OFFICE BUILDING**

The electric grid is fundamental to our lives and our country’s existence. Without electricity, banks shut down. Food goes bad. Sewage and water plants don’t function. Medicines expire. Chaos ensues and crime explodes. We simply cannot afford to lose broad sections of the grid for days, weeks, months, or years.

It is our very reliance on this infrastructure that makes it an obvious target for attack. We know that many of our adversaries – from terrorist groups to nation states – have or continue to develop capabilities that would allow them to attack and destroy our grid at a time of their choosing.

There are two significant threats that will be discussed at today’s hearing. One is the threat of cyber attack. Many nation states, like Russia, China, North Korea, and Iran, have offensive cyber attack capabilities, while terrorist groups like Hezbollah and al Qaeda continue to work to develop capabilities to attack and destroy critical infrastructure like the electric grid through cyber means.

If you believe intelligence sources, our grid is already compromised. An April 2009 article in the Wall Street Journal cited intelligence sources who claim that the grid has already been penetrated by cyber intruders from Russia and China who are positioned to activate malicious code that could destroy portions of the grid at their command.

The other significant threat to the grid is the threat of a physical event that could come in the form of a natural or manmade Electromagnetic Pulse, known as EMP. The potentially devastating effects of an EMP to the grid are well documented. During the Cold War, the U.S. government simulated the effects of EMP on our infrastructure, because of the threat of nuclear weapons, which emit an EMP after detonation. Though we may no longer fear a nuclear attack from Soviet Russia, rogue adversaries (including North Korea and Iran) possess and test high altitude missiles that could potentially cause a catastrophic pulse across the grid.

These are but two of the significant emerging threats we face in the 21st century. Our adversaries openly discuss using these capabilities against the United States. According to its “Cyber Warfare Doctrine,” China’s military strategy is designed to achieve global “electronic dominance” by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of traditional military operations.

Cyber and physical attacks against the grid could both be catastrophic and incredibly destructive events, but they are not inevitable. Protections can – and must – be put in place ahead of time to mitigate the impact of these attacks.

My colleagues on the Homeland Security Committee and I have spent nearly three years identifying and reviewing the security protections that are in place to mitigate the effects of any intentional or unintentional attack on the electric system. Our goal is to determine whether appropriate protections are in place that would mitigate catastrophic incidents on the grid. Our review has required

extensive discussions and review with the private sector, which owns, operates, and secures the grid. The private sector develops its own security standards. The private sector also oversees compliance with these standards. In short, the private sector has the responsibility for securing the grid from electromagnetic events and cyber attacks.

In the course of our review, we have questioned hundreds of experts and reviewed thousands of pages of research and analysis. Many have submitted statements for the record today. They have all reached one conclusion: the electric industry has failed to appropriately protect against the threats we face in the 21st century.

In the past, this Committee has been deeply critical of the standards that the industry has written. They are, in the words of GAO, NIST, and other independent analysts, “inadequate for protecting critical national infrastructure.” The Committee has suggested that the industry adopt NIST standards for control systems if it hopes to achieve greater security. My understanding is that the industry has not embraced this suggestion.

The Committee has also been critical of the industry’s effort to timely mitigate the Aurora vulnerability. What should have been an urgent action issue has taken some utilities years to fix. Many have not even hardened their assets at all. This is especially troubling, given the catastrophic damage that could be caused by an Aurora-style attack.

Today there’s a new problem. Many in industry are apparently trying to avoid compliance with their own inadequate standards. I am deeply concerned about this irresponsible behavior. A letter dated April 9, 2009, which is attached for the record, sent to industry by NERC, suggests that industry is choosing not to identify critical assets in order to avoid securing them. According to NERC, only 29% of Generation Owners and Generation Operators reported identifying at least one critical asset. 63% of Transmission Owners identified at least one critical asset. This effort seems to epitomize the head-in-the-sand mentality that seems to permeate broad sections of the electric industry. The Committee will be following up with NERC to learn which utilities have not appropriately identified assets, and seek to make this information public.

It is amazing that many within the industry would gamble with our national and economic security than implement precautionary security measures. This calculus amazes me even more when you realize that utilities can be reimbursed for these security expenditures in their rate cases.

I’m at a loss to explain why the industry isn’t appropriately securing its assets. But clearly, the time has come for change. I am pleased to join Chairman Thompson, Ranking Member King, and my other colleagues in co-sponsoring HR 2195. Given the industry’s lackluster approach towards securing its own assets, I believe this measure will provide the Federal Energy Regulatory Commission with the appropriate authorities to ensure that our grid is secure and resilient against the threats we face in the 21st century.

This Subcommittee will continue to perform vigorous oversight until we are satisfied that progress is being made.