BEFORE THE
U.S. SENATE APPROPRIATIONS COMMITTEE

SUBCOMMITTEE ON HOMELAND SECURITY

HEARING ON "INVESTING IN CYBER SECURITY: UNDERSTANDING RISKS AND BUILDING CAPABILITIES FOR THE FUTURE"

TESTIMONY OF CHRISTOPHER PETERS
VICE PRESIDENT, NERC/CRITICAL INFRASTRUCTURE PROTECTION COMPLIANCE
ENTERGY CORPORATION

MAY 7, 2014

Good afternoon, Chairwoman Landrieu, Ranking Member Coats, and distinguished Members of the Subcommittee. Let me begin by thanking you for convening this panel and for inviting Entergy to participate. My name is Chris Peters and I am Entergy's Vice-President for NERC and Critical Infrastructure Protection compliance, reporting to Entergy's Executive Vice President and Chief Operating Officer.

I am pleased to appear here today to discuss Entergy's point of view on cyber and physical security threats to our system, the benefits of the public-private partnership process, and our experiences to date interfacing with the Electricity Sector-Information Sharing and Analysis Center (ES-ISAC).

By way of background, Entergy Corporation is an integrated energy company engaged primarily in electric power production and retail distribution. Entergy owns and operates power plants with approximately 30,000 megawatts of electric generating capacity, including more than 10,000 megawatts of nuclear power. We deliver electricity to 2.8 million customers in Arkansas, Louisiana, Mississippi and Texas. We have approximately 14,000 employees.

For some time now, Entergy has recognized the uptick in cyber and physical threats that have the potential to impact the reliability, safety and security of our operations and the nation's

power grid. We accord such threats the same attention as we have always given to forces of nature, including ice storms, tornadoes, hurricanes, floods and extreme heat - all of which can threaten the delivery of safe, reliable power.

Entergy supports a comprehensive strategy to managing our cyber and physical security defenses. This strategy leverages our corporate resources to minimize impacts from intentional and unintentional cyber or physical threats to our energy portfolio. Importantly, these efforts have strong support at the Board and CEO level, which we believe is essential to implementing an enterprise-wide security program with the right amount of people for a security workforce and sufficient funding of the technologies required to deal with threats and breaches.

The threat landscape is inherently unpredictable and evolving, which is mastering the fundamentals of cyber and physical security is the best defense: In most cases successful attacks exploit lapses in basic operations that have been either ignored or which were not fully deployed. One priority for Entergy is threat management. When a new threat emerges, Entergy conducts an internal review of our defense-in-depth plans to validate the existing security control framework and make changes as necessary. Accordingly, increasing physical security threats to energy delivery infrastructures have triggered reviews and updates to our security plans and posture, including the implementation of additional physical security controls at key facilities.

Public-private partnership participation is a key element in our cyber and physical security program and can be a significant force multiplier when leveraged. To strengthen our posture, over the past several years we have participated in a number of public-private programs.

- The Government Forum of Incident Response and Security Team Conference
- The FBI's Classified Cybersecurity Threat Briefings
- NERC's GridEx and GridEx II sector-wide exercises

- DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the Control Systems Cybersecurity Training delivered by Idaho National Labs
- More than a few DHS' initiatives, including: Monthly Unclassified Nuclear Sector Threat Teleconferences, the Control Systems Cybersecurity Program, the Cyber Security Evaluation Tool (CSET), Classified Nuclear Cybersecurity Threat Briefings at the National Security Agency, the Enhanced Critical Infrastructure Protection Initiative, and the Cyber Storm III exercise
- Lastly, Entergy worked closely with NIST and participated in several workshops during the drafting of the Cybersecurity Framework in relation to Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity.*

Allow me to highlight one program we feel is particularly helpful. Since 2008, Entergy has received and responded to over 40 NERC Alerts related to grid security threats from the ES-ISAC. Based on the content of each alert, we quickly assemble cross-functional teams of Subject Matter Experts (SMEs) to evaluate the highlighted vulnerabilities, assess potential impacts, and carry out appropriate mitigation steps. Entergy considers the ES-ISAC to be a vital partner in achieving electric sector-wide situational awareness, improving national-level response and coordination, and fostering collaboration among key electric sector stakeholders.

The public-private partnership model is not perfect and will continue to evolve over time to ensure that the private sector can realize maximum value from federally-funded programs and technologies. Every utility must drive the daily transformation of their own cyber and physical security programs to defend against constantly-changing threat landscapes.

Before concluding, I would like to add that Entergy is a strong advocate of regulations and legislation that would bolster information sharing between public and private entities about

cybersecurity risks and events. Allowing that protections are built in for confidentiality and non-recourse, we believe access to information of this kind will help enhance the security posture of utilities.

Thank you for giving Entergy the opportunity to share its views and I hope you've found these comments helpful. We look forward to continuing to work with you in the coming year to ensure strong public-private relationships aimed at better securing the energy sectors' critical infrastructure. I am happy to answer any questions you may have.