Congressional Testimony

Cyber Threats to Our Nation's Critical Infrastructure

Thomas A. Fanning
Chairman, President, and Chief Executive Officer
Southern Company

Testimony before the
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

August 21, 2018

Chairman Graham, Ranking Member Whitehouse, and Members of the Subcommittee, thank you for inviting me to testify today. My name is Tom Fanning, and I am the chairman, president, and chief executive officer of Southern Company.

Southern Company is one of America's largest energy companies, with 46,000 megawatts of generating capacity and 1,500 billion cubic feet of combined natural gas consumption and throughput volume serving 9 million customers through its subsidiaries, as of December 31, 2017. We operate nearly 200,000 miles of electric transmission and distribution lines and more than 80,000 miles of natural gas pipeline as of December 31, 2017. The company provides clean, safe, reliable and affordable energy through electric operating companies in four states, natural gas distribution companies in four states, a competitive generation company serving wholesale customers in 11 states across America and a nationally recognized provider of customized energy solutions, as well as fiber optics and wireless communications.

I am pleased to address the Subcommittee today to share what steps Southern Company and the electric power industry are taking to make energy infrastructure more secure and resilient so that we may continue to deliver the safe, affordable, reliable, and clean energy that Americans count on and need.

This is an important hearing on an important topic. The cybersecurity of critical infrastructure is one of the most pressing issues facing our nation. That this hearing includes witnesses from both the public and private sectors is fitting; energy grid security, especially against cyber threats, requires a holistic and national response. None of us can secure critical infrastructure alone.

The electric sector faces constantly evolving threats to the energy grid. The industry's risk mitigation strategy relies on a "defense-in-depth" approach that focuses on preparation, prevention, response, and recovery, with an emphasis on prioritizing and isolating the most critical assets. While this hearing is focused on cybersecurity, it is important to note that our companies do not build the energy grid or our security responses to meet only one type of threat. Whether manmade or natural, malicious or unintentional, relating to cyber or physical security, or a combination, we must prepare and plan for all types of threats.

Thankfully, grid security is a top priority for the entire electric power sector. It is notable that our industry—unlike most other critical infrastructure sectors—is subject to mandatory and enforceable cyber and physical security standards. These Critical Infrastructure Protection (CIP) regulatory standards are developed and enforced through a process created by Congress through the Energy Policy Act of 2005. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day. These standards are important, and they give baseline security across the bulk power system. But, standards alone cannot guarantee security. That is why we are focused on growing partnerships across the industry and with government and on preparing to respond and to recover from impacts to our systems through the industry's culture of mutual assistance.

The Electricity Subsector Coordinating Council

The electric power industry—which includes investor-owned electric companies like Southern Company, public power utilities, and electric cooperatives—supports more than 7 million

American jobs and contributes $880 billion annually to U.S. gross domestic product, about 5 percent of the total. The three segments of our industry jointly have formed the Electricity Subsector Coordinating Council or ESCC.

In October 2010, the National Infrastructure Advisory Council (NIAC) issued a report, “A Framework for Establishing Critical Infrastructure Resilience Goals,” that included nine recommendations. The first recommendation was for the White House to “initiate an executive-level dialogue with electric and nuclear sector CEOs on the respective roles and responsibilities of the private sector in addressing high-impact infrastructure risks and potential threats…” That recommendation eventually led to the creation of the ESCC.

I serve as one of three co-chairs of the ESCC. My fellow co-chairs are Duane Highley, President and CEO for Arkansas Electric Cooperative Corp. and Arkansas Electric Cooperatives, Inc., and Kevin Wailes, CEO of Lincoln Electric System in Nebraska.

The ESCC is comprised of the CEOs of 22 electric companies and 10 major industry trade associations. This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the electric sector and the federal government for coordinating efforts to prepare for, and respond to, cybersecurity threats, physical terrorism, and natural disasters that imperil critical infrastructure.

Through the ESCC, our industry works in close coordination with our government counterparts, including senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations. The ESCC is where these senior leaders from industry and government come together to set strategy and priorities on the security, resiliency, and responsiveness of the industry and, by extension, the nation.

Each year, the ESCC convenes three coordination meetings with our government partners to identify emerging security issues and to develop approaches to mitigate risk, including cyber and physical security. However, the ESCC is much more engaged than three formal meetings a year with the government. Those “blue sky” meetings help prepare the industry and government for response efforts. In between, we work together constantly to leverage industry and government executives and subject matter experts to develop numerous initiatives with the goal of improving the industry's preparedness and resilience. During incidents, the ESCC helps to coordinate efforts across industry and government in response to all hazards.

Over the past several years, this partnership has resulted in several important changes in how both government and industry work together to protect critical infrastructure. I would like to highlight a few:

- The ESCC Playbook is a framework for senior industry and government executives to coordinate response and recovery efforts and communications to the American public. The playbook has been tested in a series of exercises, and it informs our response and recovery efforts today.

- We test this Playbook during industry-only and industry-government exercises to ensure that our processes are ready to be put into action. There are many exercises throughout the year, but the largest is the biennial GridEx, run by the North American Electric Reliability Corporation (NERC). GridEx IV, held in November 2017, brought together more than 6,000 participants representing more than 400 organizations from across the electric power industry and federal and state governments. These drills sharpen not just the unity of effort between electric companies and government agencies, but also practice unity of message to ensure that we speak with one voice to our customers and your constituents during incidents. Not only has the Playbook been exercised repeatedly in recent years, but it also has been utilized during several incidents, including last year's historic storms, and in response to other major outages.

- A key focus of the ESCC is to enhance our tools and technology. One key example is the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership that includes industry, the Department of Energy (DOE), Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing & Analysis Center (E-ISAC), which manages the program. More than 75 percent of U.S. electricity customers are served by an electric company that has deployed CRISP, and this program will continue to grow as the information gleaned from its sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

- We have supplemented our industry's traditional mutual assistance—usually seen as bucket trucks and lineworkers travelling to restore power following natural disasters—with a new group to meet digital challenges: cyber mutual assistance. The same surge capacity that rushes to companies in need during hurricanes, winter storms, and wildfires stands ready to assist and to share resources in the face of a potential cyber incident. So far, more than 140 entities, including investor-owned electric and natural gas companies, electric cooperatives, public power utilities, Canadian electric companies, and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs), are participating in the program. These entities cover more than 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and 74 percent of natural gas distribution pipelines.

- Along with DOE, we have developed a threat landscape initiative. No company can protect every asset from every threat all the time. Accordingly, we must prioritize based on the likelihood and severity of a threat. This matrix allows electric companies and the government to consider how to invest, coordinate, and deploy assets to cover the wide range of potential threats faced by some of the nation's most critical infrastructure.

That is what we have done in the past. But, as threats evolve, so must our defenses. This year, the ESCC set three broad strategic priorities that will drive our work going forward:

1. **Collective Defense:** Our industry will work with government to improve the collective defense of the nation's most critical infrastructure to better prepare for, and respond to, an existential threat to the United States.

2. **Preparedness & Resilience:** We will identify areas and opportunities for government support to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

3. **Collective Response:** We will develop response and recovery architectures and frameworks to coordinate with government on mitigating systemic threats and/or responding to significant multi-sector, multi-regional physical and cyber events.

Conclusion

Securing critical infrastructure from all threats—but particularly from new and evolving cyber threats—is a defining challenge for our nation. The threat to critical infrastructure and to our way of life is growing, but so is the work that is underway to prepare our systems, to prevent attacks in the first place, to detect intrusions, to respond to issues, and to recover quickly. That work is enhanced through our work within industries and across sectors and with the strong support from government partners at all levels.

The Subcommittee is showing great leadership in tackling this important issue. Thank you for your interest in our work, and I look forward to your questions.