

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C.**

In the Matter of )  
 )  
National Broadband Plan Recommendation to ) PS Docket No. 10-146  
Create a Cybersecurity Roadmap ) GN Docket No. 09-51  
 )

To: Chief, Public Safety and Homeland Security Bureau

**COMMENTS OF  
SOUTHERN COMPANY SERVICES, INC.**

Southern Company Services, Inc. ("Southern"), on behalf of itself and its operating affiliates, hereby submits its comments in response to the *Public Notice*, DA 10-1354, released August 9, 2010, on the creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users. This proceeding is responsive to Recommendation 16.5 of the Federal Communications Commission's ("FCC's" or "Commission's") National Broadband Plan ("NBP") that the FCC should "develop a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely."<sup>1</sup>

By way of background, Southern is a wholly-owned subsidiary service company of Southern Company, a super-regional energy company in the Southeast United States.

---

<sup>1</sup> Connecting America: The National Broadband Plan (March 2010), Recommendation 16.5.

Southern Company also owns four electric utility subsidiaries – Alabama Power Company, Georgia Power Company, Gulf Power Company, and Mississippi Power Company – which provide retail and wholesale electric service throughout a 120,000 square mile service territory in Georgia, most of Alabama, and parts of Florida and Mississippi. Members of the Southern Company family use a variety of communications technologies to support the safe and efficient delivery of energy services to their customers. Southern has significant interest in ensuring that broadband or other communications networks used to support “Smart Grid” and other utility-related communications requirements are secure and reliable.

Southern supports the Commission’s intent to identify and address cybersecurity threats to the communications infrastructure. Southern has a vested interest in protecting the critical *electric* infrastructure used to deliver energy to the public, and has a corresponding interest in ensuring that the communications facilities and services which Southern uses to support the generation, transmission and distribution of electric power are also reliable and secure.

## **I. Vulnerabilities**

There are inherent risks associated with communications technologies used to control the electric power grid. For this reason, Southern works hard to ensure that an associated security strategy is developed before putting into effect any new technology that could compromise the integrity of the grid itself or the systems that control the grid. Older grid control systems were physically isolated from the Internet and other public communications networks. However, newer control and “Smart Grid” systems may require interconnectivity via the Internet to work properly. Interconnection with public communications networks

inherently presents cyber vulnerabilities. A further complicating security risk is the growing use of public wireless services. Southern must be poised to address new risks as these technologies are introduced into the systems used to monitor and control the power grid.

From Southern's perspective as one of the nation's largest electric utilities, the most vital cybersecurity vulnerabilities for the nation's critical electric infrastructure are the following:

- Interruption of Control – Inability to remotely manage electric transmission and distribution assets, such as electric substations, line monitoring and control devices and generating plants.
- Malicious Control Actions – Third-party intrusions that take control of devices on the grid and thereby have the ability to damage key system components and create widespread power outages.
- Widespread, Extended Outages – Outages resulting from the interruption of communications systems and services.

## **II. Techniques to Address Vulnerabilities**

To address these vulnerabilities, Southern recommends using the following techniques:

- Virtual Private Networks (VPNs) – A VPN encompasses links across shared or public networks. VPN connections use the connectivity of the Internet plus a combination of tunneling and data encryption technologies to connect remote clients. It is essential that public wireless services utilize VPN tunnels to the Internet and not limit the tunnels to their systems only.

- Firewalls – These should be part of a security strategy to secure and isolate a network while still permitting authorized data communications to pass through. Firewalls with VPN capabilities also allow secure, encrypted communication from a remote location through the Internet.
- Encryption – Sensitive data on a device should be encrypted. Data sent across a wireless network should also be encrypted. The security strategy will determine the extent to which encryption is used.
- Strong Authentication – Especially for situations where security breaches could have large-scale ramifications (compromised customer data, loss of control, malicious control actions, etc.) strong authentication should be the outer layer of defense for a complete security strategy. Standard identity management services, biometrics, public key infrastructure (PKI) or automated authentication capabilities should be employed where appropriate.
- Intrusion Prevention Services – Using deep packet inspection, these systems can be deployed in front of a firewall to isolate suspicious traffic that appears to be in the nature of a virus, Trojan, or worm that could allow an intruder to take control of the system or exploit it with malicious intent.

### **III. The FCC's Role in Addressing Cybersecurity**

Within the electric industry, the Federal Energy Regulatory Commission (“FERC”) and the North American Electric Reliability Corporation (“NERC”) promulgate and enforce Critical Infrastructure Protection (“CIP”) standards that place a strong emphasis on cybersecurity protection, in addition to physical protection, of electric transmission system

assets. To the extent electric utilities use commercial broadband or wireless networks in support of their electric transmission operations, the utilities must have confidence that their communications are secure, cannot be compromised, and are verifiably compliant with the CIP standards. Indeed, in the the FCC noted in the National Broadband Plan that it is currently unclear whether or how services provided by a commercial carrier are covered by the CIP cybersecurity standards.<sup>2</sup> Moreover, the CIP standards only apply to the Bulk Electric System (*i.e.*, generation and transmission) and do not address communications used to support electric distribution, where much of the growth in Smart Grid devices and applications is expected to occur.

Southern therefore believes that public broadband networks should be subject to general standards on cybersecurity protection. As the primary agency with regulatory oversight of public communications networks and service providers, the FCC seems to be the most logical agency to assume responsibility for ensuring that commercial broadband networks, both wired and wireless, are made accountable for cybersecurity protection. Because it would be difficult to prescribe specific cybersecurity standards to which all providers would have to conform, Southern suggests that as a first step the Commission could amend its Part 4 Rules on disruptions to communications to require service providers to report third-party intrusions or other acts of a malicious or hostile nature that represent threats to critical infrastructure or public safety communications even if they do not cause a service “disruption” as currently defined in the Rules. Such reporting could help identify common

---

<sup>2</sup> NBP, Recommendation 12.3, and note 37 thereto.

cybersecurity vulnerabilities in public networks and encourage wider adoption of industry standards and best practices.

In addition, Southern encourages the FCC to coordinate on cybersecurity issues with other agencies and organizations having direct involvement in the protection of utility assets (*e.g.*, FERC, NERC, and the state public utility commissions). Such coordination will help the FCC to better understand the utility industry's need for secure and reliable communications and the expectations of these other agencies, and will help these other agencies to better understand the potential viability of commercial communications networks to meet these needs as a function of the FCC's statutory responsibility to make communications facilities available, so far as possible, "for the purpose of promoting safety of life and property through the use of wire and radio communications."<sup>3</sup>

#### **IV. Conclusion**

Southern supports the Commission's efforts to identify the most significant cybersecurity threats to the communications infrastructure and end users, and to develop a clear strategy for securing the vital communications networks upon which the nation's critical infrastructure and public safety communications rely. Southern believes that the Commission should have a role in ensuring that the providers of commercial communications services take all appropriate measures to protect their networks and end users from cyber threats, and suggests that a first step could be to expand outage reporting to include information on intrusions or other malicious acts that could represent threats to critical infrastructure such as

---

<sup>3</sup> 47 U.S.C. §151.

the electric power grid, or public safety communications. Southern also encourages the Commission to coordinate on cybersecurity issues with other agencies and organizations with a vested interest in the protection of critical utility assets.

Respectfully submitted,

**SOUTHERN COMPANY SERVICES, INC.**

By: /s/ Jimmy R. Williams  
Jimmy R. Williams  
Manager of Infrastructure Services Planning and  
Engineering  
Southern Company Services, Inc.  
600 North 18th Street  
Birmingham, AL 35203  
205.257.2303

Jeffrey L. Sheldon  
FISH & RICHARDSON P.C.  
1425 K Street, N.W.  
Washington, D.C. 20005  
202.626.7761

Counsel to Southern Company Services, Inc.

Dated: September 23, 2010