Before the
Federal Communications Commission
Washington, D.C.

In the Matter of	)	
	)	PS Docket No. 10-93
Cyber Security Certification Program	)	

COMMENTS OF
THE NATIONAL ASSOCIATION OF STATE UTILITY CONSUMER ADVOCATES
ON NOTICE OF INQUIRY

I. INTRODUCTION

On April 21, 2010, the Federal Communications Commission ("FCC" or "Commission") adopted a Notice of Inquiry ("NOI") seeking comment

> on whether the Commission should establish a voluntary program under which participating communications service providers would be certified by the FCC or a yet to be determined third party entity for their adherence to a set of cyber security objectives and/or practices.[1]

The FCC has established three goals for this proceeding

1. To increase the security of the nation's broadband infrastructure;
2. To promote a culture of more vigilant cyber security among participants in the market for communications services; and
3. To offer end users more complete information about their communications service providers cyber security practices. [2]

The National Association of State Utility Consumer Advocates ("NASUCA")[3] submits these initial comments on the NOI.

---

[1] FCC 10-63 (rel. April 21, 2010), ¶ 2.

[2] Id.

[3] NASUCA is a voluntary association of advocate offices in more than 40 states and the District of Columbia, incorporated in Florida as a non-profit corporation. NASUCA's members are designated by the laws of their respective jurisdictions to represent the interests of utility consumers before state and federal regulators and in the courts. Members operate independently from state utility commissions as advocates primarily for residential ratepayers. Some NASUCA member offices are separately established advocate organizations while others are divisions of larger state agencies (e.g., the state Attorney General's office). NASUCA's associate and affiliate members also serve utility consumers but are not created by state law or do not have statewide authority.

II. THE FEDERAL ADMINISTRATION HAS DEVELOPED THREE THEMES FOR A CYBERSECURITY STRATEGY

The National Broadband Plan ("NBP") recommended the FCC establish a voluntary cybersecurity certification regime that creates market incentives for communications service providers to upgrade the cyber security measures applied to networks.[4] The NBP further recommended the FCC examine additional voluntary incentives which could improve cybersecurity and education about cybersecurity issues, as well as inquire about the international aspects of a certification program.[5]

NASUCA notes the Administration has developed three themes undergirding its multi-billion dollar cybersecurity strategy: (1) tailored trustworthy spaces; (2) moving targets; and (3) economic incentives.[6]

The first theme, "tailored trustworthy spaces," entails the creation of differing levels of security for government and non-government Internet activities. These "spaces" would be designed to provide flexible and adaptive environments via a common framework to support functional and policy requirements as threats develop, evolve, and adapt.

The second, "moving targets," delineates a search for security systems that change constantly to increase uncertainty, cost, complexity and limit the exposure of vulnerabilities for hackers. Yet it also accepts and recognizes that all systems eventually become vulnerable. Ideally, a moving target system will dynamically alter itself in ways managed by the defender while appearing unpredictable to the would-be intruder.

The third and final theme, "economic incentives," involves seeking to find ways to

---

[4] NOI, ¶ 9, citing Federal Communications Commission, Connecting America: The National Broadband Plan (2010) at § 16.7.

[5] NOI, ¶ 9.

[6] See http://homelandsecuritynewswire.com/us-government-direct-more-cybersecurity.

motivate users to adopt cybersecurity defenses. Unfortunately, there are few, if any, good metrics that delineate how secure a specific system is, and costs are often based on anecdotal or un-quantified information to defend against a threat which may no longer be viable. These costs are then generally passed through to customers by the provider without any guarantee of actually securing the system against new evolving threats that will occur.

III. THE NATION'S BROADBAND INFRASTRUCTURE IS VULNERABLE

Because any type of attack – facility or cyber – against the nation's broadband infrastructure favors the attacker, the network is, by its very nature, vulnerable. That vulnerability is exacerbated by the multitude of entry points through which an attacker can access and maneuver through the network. Consequently, as the network is expanded to incorporate greater levels of data transfer, voice and video communication, and infrastructure command and control (Smart Grid, SCADA, etc.), the points of vulnerability and necessity for defending against attack increase exponentially.

Because, in addition to monitoring the system 24/7 for all conceivable types of attack, each provider or "defender" must also develop backup plans, systems, etc. to enable a continuity of operations during and post-attack, there is a corresponding exponential increase in system costs, improvements and investment, not to mention planning – costs that are either borne solely by the provider or passed through to the customer base.

IV. DEPLOYMENT OF SMART GRID TECHNOLOGY EXPOSES THE ELECTRIC GRID TO INCREASED VULNERABILITY THROUGH BROADBAND NETWORK INTEGRATION

As the nation moves forward integrating broadband networks and energy grids using Smart Grid technologies, security costs for the Smart Grid alone could represent up to 15 percent of total Smart Grid capital investment by 2015, while cumulative investment in the security sector could reach $21 billion between 2010 and 2015 with annual revenues reaching $3.7 billion

by 2015[7] – a cost that will be shared by the Smart Grid and national broadband networks alike. Because control networks and information technology networks become more integrated with the deployment of Smart Grid-compatible technologies, the networks themselves become increasingly vulnerable to cyber attacks. In fact, the constant reminder in the form of reports of attempts to infiltrate the energy grid adds tangible urgency to the need for cyber security in the emerging Smart Grid and associated broadband networks. One key element required to ensure stronger security for Smart Grid networks is the adoption of interoperable standards – the National Institute of Standards and Technology ("NIST") has been appointed by the Federal government to develop such standards between disparate systems and industry participants.

Interestingly enough, as the Smart Grid (and the associated broadband networking infrastructure) matures and grows, it will, through innovation and natural progression, venture into new avenues where the energy industry has traditionally rarely involved itself – transportation, integrated communications, entertainment, home security, and other non-energy markets. Home Energy Management Systems such as those produced by Control4 Technologies seek to combine functionalities to offer consumers "one-stop" shopping – managing home energy systems and communications networks.[8] That convenience can also be an Achilles Heel unless integrated cybersecurity systems are in place – preventing would-be intruders from access to various on-ramps into both the broadband and energy networks.

Because the standards being developed by NIST will directly and indirectly affect the security of broadband networks, Smart Grid networks, and other interconnected networks, they will, by default, affect all telecommunications networks in the U.S. Separating Smart Grid from

---

[7] *Smart Grid cybersecurity market to reach $3.7 billion by 2015*, Homeland Security Newswire, June 24, 2010, accessible at http://homelandsecuritynewswire.com/smart-grid-cybersecurity-market-reach-37-billion-2015

[8] See http://www.control4.com/.

the telecommunications and broadband networks that enable the host of other technologies to integrate with the Smart Grid is neither feasible nor practical as we move forward. Thus, the goal of increasing the security of the nation's broadband networks espoused by the FCC in this proceeding is a goal that effects consumers in both arenas – telecommunications and energy. And those consumers will likely be asked to bear the brunt of the cost for these integrated networks and the security which must be standardized, developed and employed to protect them, especially if we do not take the necessary steps to ensure the process is done right the first time.

V. CONCLUSION

NASUCA urges the Commission to investigate the increasing inter-relationships of broadband networks to other infrastructure industries as they develop cybersecurity programs – both voluntary and involuntary – to protect both consumers and the nation. NASUCA also urges the Commission to bear in mind the costs of these security programs and the impact that such costs will have on consumers – costs that will be neither short-term nor decreasing.

Respectfully submitted,

David C. Bergmann
Assistant Consumers' Counsel
Chair,
NASUCA Telecommunications Committee
Office of the Ohio Consumers' Counsel
10 West Broad Street, Suite 1800
Columbus, OH 43215-3485
Phone (614) 466-8574
Fax (614) 466-9475
bergmann@occ.state.oh.us

NASUCA
8380 Colesville Road, Suite 101
Silver Spring, MD 20910
Phone (301) 589-6313
Fax (301) 589-6380

July 12, 2010