Before the
Federal Communications Commission
Washington, D.C.

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

REPLY 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 comments

> 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[2]:

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.

The National Association of State Utility Consumer Advocates ("NASUCA") submitted initial comments concerning cybersecurity issues on July 12, 2010, and now submits these reply comments.

II. REASONABLE REGULATION IS NEEDED.

While NASUCA concurs with many of the comments submitted in this NOI, concern

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

[2] Id.

remains regarding the lack of inclusiveness a voluntary cybersecurity policy may have not only for the telecommunications industry, but also for other industries, which now and in the future will rely heavily on telecommunication infrastructure for everything from data transfer to command and control of critical infrastructure components. The deployment of Next Generation Networks (NGNs), mobile/distributed networking infrastructures, Peer-to-Peer (P2P) communications infrastructure, and a plethora of third-party-developed applications, combined with packet-based networking, advanced services, and increasingly intelligent consumer-owned devices, will support flexible, customized, multi-media services that are increasingly vulnerable to avenues of attack through traditional and non-traditional modes.

NASUCA agrees with commentors that stakeholders are in a good position to secure the cyber-space assets they own and control, but also believes that a basic underlying structure of cyber-security principles and guidelines are necessary to ensure inter-operability of communications infrastructure and the continued inter-communication of threats and vulnerabilities between stakeholders. It is imperative the FCC understand clearly these far-reaching implications as it continues to develop policy in this arena designed to increase cooperation between the public and private sector. Incorrect or poor policy decisions pertaining to cybersecurity of telecommunications infrastructure will have significant and long-term effects that cannot be easily negated, and which may actually provide additional opportunities for those attempting to exploit vulnerabilities.

NASUCA believes it is prudent for the FCC to establish a "baseline" of security requirements, in effect mandating a minimum set of national standards to ensure interoperability and establish a basic level of security. While preserving the telecommunication infrastructure, this also allows each company to do what is in its best interest to secure and protect the specific networks it operates. A provider may decide to provide a "super-secure" network, but should do

so at its own expense. Such a provider must recognize that the rest of the network may not be up to those standards. NASUCA understands the establishment of a baseline set of security standards will generate "mandated" costs, but when that cost is factored against the alternative, that is, a network with weak points vulnerable to attack, with limited ability to know where in the network the flaw(s) may be found, the reasonable and justified costs to secure our infrastructure are prudent and in consumers' interest.

It appears that the FCC may, however, be contemplating a more rigorous approach to the cyber-security issue – one which establishes layers of regulatory controls and mandates. The impact of this depends on the intensity of the "voluntary incentives-based certification program" that would provide participating communications service providers some type of accreditation for complying with "stringent FCC network security requirements," especially with government-approved auditors examining the provider's "adherence to stringent cyber security practices"[3]. An excessively intrusive approach could not only increase costs – costs borne by the consumer – but could unnecessarily impose operational and financial burdens on providers that may end up being counter-productive to ensuring a secure and viable telecommunications infrastructure. NASUCA urges moderation in this uncertain area.

III. CONCLUSION

NASUCA again strongly urges the Commission to investigate the increasing inter-relationships of broadband networks to other infrastructure industries as it develops cybersecurity programs – both voluntary and involuntary – to protect both consumers and the nation. But the Commission also must ensure that any baseline cyber security criteria have the breadth, depth, and flexibility to address rapidly evolving technological environments, while

[3] *Notice*, ¶12

having joint support from all government agencies with regulatory or other oversight in arenas not under FCC jurisdiction. And NASUCA continues to urge the Commission to bear in mind the costs of these security programs and the impact that cost will have on consumers as it examines this complex and far-reaching issue – remembering that these costs will not be short-term nor decreasing in their impact.

Respectfully submitted,

/s/ *David C. Bergmann*

David C. Bergmann
Assistant Consumers' Counsel
Chair, NASUCA Telecommunications Committee
Office of the Ohio Consumers' Counsel
10 West Broad Street, Suite 1800
Columbus, Ohio 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

September 8, 2010