Before the
National Institute of Standards and Technology
National Telecommunications and Information Administration
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Incentives to Adopt Improved Cybersecurity Practices	)	Docket No. 130206115-3115-01
	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Howard J. Symons
Christopher J. Harvie
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Rick Chessen
Loretta Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

April 29, 2013

TABLE OF CONTENTS

Before the
National Institute of Standards and Technology
National Telecommunications and Information Administration
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Incentives to Adopt Improved Cybersecurity Practices	)	Docket No. 130206115-3115-01
	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association (NCTA)[1] hereby submits its comments in response to the Notice of Inquiry[2] issued by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) at the U.S. Department of Commerce in the above-captioned proceeding.

INTRODUCTION AND SUMMARY

The Notice of Inquiry (NOI) requests input to assist the Secretary of Commerce in evaluating a set of incentives designed to promote private sector participation in the Critical Infrastructure Cybersecurity Program (Cybersecurity Program) and the voluntary adoption of the Cybersecurity Framework by the owners and operators of critical infrastructure.[3]

---

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of broadband service after investing $200 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 26 million customers.

[2] Dep't of Commerce, Nat'l Inst. of Standards & Tech., Nat'l Telecomm.& Info. Admin., Dkt. No. 130206115-3115-01, *Incentives to Adopt Improved Cybersecurity Practices*, 78 Fed. Reg. 18954 (Mar. 28, 2013) ("NOI").

[3] NOI at 18594.

In our recent comments in response to NIST's Request for Information on the Cybersecurity Framework, NCTA explained that its members have strong market-based incentives to address cyber threats and vulnerabilities, and incorporate cybersecurity practices and protocols into their business operations.[4] Our companies' business success depends on customers using their networks and consuming their network-based offerings, so ensuring a safe and secure network environment is a top business priority.

As the Cybersecurity Executive Order[5] recognizes, however, further incentives may be necessary to encourage sufficient private sector participation in the Cybersecurity Program.[6] NCTA urges the Department to consider several such incentives. First, the Department should recommend federal legislation to remove uncertainty regarding potential legal liability arising from the adoption or deployment of cybersecurity countermeasures and the sharing of cyber threat information. Second, federal law should preempt state and local laws to the extent they are inconsistent with this legislation, in order to ensure a uniform national framework for cyber defense activities. Finally, the Department should recommend that the government provide grants and tax abatements, such as accelerated depreciation for cybersecurity related assets, to owners and operators of critical infrastructure to help defray the high fixed costs associated with development, investment, and deployment of the most up-to-date cybersecurity assets and tools. Providing these incentives will greatly facilitate the ability of critical infrastructure owners and

---

4 Dep't of Commerce, Nat'l Inst. of Standards & Tech., Dkt. No. 130208119-3119-01, *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 13024 (Feb. 26, 2013), Comments of the National Cable & Telecommunications Association at 6 (filed Apr. 8, 2013) ("NCTA Cybersecurity Framework Comments").

5 Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013) ("Cybersecurity EO").

6 *See id.* at 11742; NOI at 18594.

operators to develop and implement the full range of cyber defenses necessary to deter and respond to cyber attacks.

Equally important to these affirmative incentives is the need for the government to refrain from erecting regulatory burdens that constrain the flexibility and business judgment that network providers require in order to effectively confront and respond to the constantly-changing cyber threat landscape. The adoption of incentives that merely reward participants for rote compliance with a checklist of minimum security standards that may quickly become obsolete does not improve the nation's cyber defense posture. Because of the dynamic and continually-evolving nature of cyber threats, compliance with a particular set of restrictive standards is not tantamount to actual security. Indeed, by conditioning the benefits of participation on adherence to government-specified practices, the government risks creating *reverse* incentives that would *discourage* innovation and foster complacency.

Finally, the government should ensure that all sectors are engaged in cybersecurity measures. Categorically excluding the information technology (IT) sector will weaken our nation's overall cybersecurity readiness, and disproportionately burden network operators and others who will, by default, be unduly expected to ensure that the IT products and services utilize on their networks do not present cyber vulnerabilities. Placing this responsibility on network operators is inefficient and inappropriately shifts the responsibility from the IT sector, which is best suited to address and respond to potential security risks.

I. THE ELIMINATION OF LEGAL UNCERTAINTIES AND THE AVAILABILITY OF REASONABLE FINANCIAL ASSISTANCE ARE ESSENTIAL COMPONENTS TO THE ADOPTION OF THE FRAMEWORK.

NCTA urges the Commerce Department to recommend a four-part incentives program to promote the adoption of the most effective cybersecurity practices:

- Liability protections to insulate companies against the threat of civil actions for employing defensive countermeasures to deter and mitigate real-time cyber threats;
- Clear authority, and protection against liability, for sharing cyber threat information with private entities;
- Preemption of state and local laws that are inconsistent with federal cybersecurity policy; and
- Financial incentives to help alleviate the costs of cybersecurity investments.

A. Liability Protection is Necessary to Eliminate Legal Uncertainties Regarding Cybersecurity Activities.

Legal uncertainty and the potential for litigation are significant impediments to utilization of the most effective and robust countermeasures and threat mitigation practices. The cable industry is subject to various federal laws related to privacy and data access and security on our networks. These laws create legal uncertainty regarding the extent to which companies may employ countermeasures in response to cyber threats and incidents and share information related to threats and attack signatures.[7]

For example, certain provisions in the Electronic Communications Privacy Act (ECPA) may raise civil liability concerns if cyber threat information sought and/or collected is embedded within an attachment to or the body of an otherwise content-free email.[8] The deployment of

[7] *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*; Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

[8] 18 U.S.C. § 2511(1).

certain defensive countermeasures may cause a temporary disruption or degradation of service, which in some cases may constitute a breach of the company's contractual quality of service obligations or create potential tort liability. Uniquely for cable operators, uncertainty regarding the applicability of the privacy provisions of the Communications Act[9] could potentially inhibit monitoring for threats or the implementation of countermeasures. As an industry built upon a trusted service relationship with our customers, cable operators and programmers have long been leaders in protecting the privacy of personal data. Under the exigent circumstances of a cyber emergency, however, it may not be possible to scrub all personal data from information shared with the government or with other providers grappling with the emergency, despite reasonable efforts to do so. In these circumstances, clear liability protection could make the difference in the timely sharing of actionable information.

Antitrust laws could also be implicated where competitors may share real-time, cyber-related information about their systems, services and customers. While those laws may not serve as a bar to some data sharing that may be required, uncertainty could arise in real-time crisis situations, particularly where circumstances may make it difficult to identify or share timely information with all potentially affected competitors/network providers. The goal should be to remove impediments to timely information sharing, by eliminating the need for a legal assessment each time that could delay or deter such sharing altogether.

To be truly effective, liability protections must be clearly defined and broad in scope. It is impossible to identify every potential source of liability that may be implicated by the adoption of cybersecurity practices, so affirmative protection should be provided "notwithstanding any other provision of law." Protection that is limited to a subset of statutes or

[9] Cable operators are subject to two different sections of the Communications Act regarding the collection and use of customer data obtained in the course of providing product and services over their networks. *See* 47 U.S.C. §§ 222, 551.

that relies solely on a "good faith" defense would simply invite litigation over whether a particular law continues to apply in some way or whether an action had been taken in good faith, even if the action was otherwise consistent with the Cybersecurity Framework or other recognized cyber measure.

When responding to a real-time threat or incident, companies should not be confronted with a Hobson's choice between incurring liability risks in connection with taking the most effective countermeasures and mitigation steps, versus effectuating a sub-standard response that does not raise liability concerns but may not effectively address the threat. Indeed, in a real-time threat situation, the very process of weighing the benefits associated with a set of countermeasures and mitigation steps against the liability risks each presents could deprive companies of precious time needed to expeditiously contain or eradicate an incident or threat. Without general liability protection against the wide variety of potential claims – both known and unknown – the risk of becoming embroiled in unnecessary legal battles remains a significant barrier to attaining the most optimal cyber defense posture and implementation of the most effective response measures and mitigation steps.

Removing the specter of litigation will not only encourage the adoption of the Cybersecurity Framework, it will significantly streamline the cost-benefit analysis by eliminating the delays associated with legal risk assessments and attorney review. In the event of a cyber emergency, swift decision-making and rapid deployment of countermeasures may be paramount to preventing disaster. Uncertainty about the legal implications of taking action can cause hesitancy and second guessing in situations where time is of the essence. The best way to ensure that companies respond quickly and confidently to a sudden cyber threat is to remove the legal risks of taking such action. General liability protection and the prompt dismissal of federal and

state claims stemming from the adoption and deployment of cybersecurity measures are essential to the success the voluntary Cybersecurity Program.

B. A Policy Framework that Encourages Robust Information Sharing Will Foster Enhanced Security and Facilitate Effective and Rapid Responses to Cyber Threats.

The open and voluntary exchange of information is critical to addressing the diverse and ever-changing threats that challenge our cybersecurity. Real-time information about new and emerging cyber threats that may impact networks is critical for defending against threats like zero-day exploits, in which bad actors use and share a software vulnerability that is unknown to the developer. Although Internet Service Providers (ISPs) make efforts to share non-personally identifiable threat information with peers and industry groups focused on cyber defense, more can be done to improve this capability.[10] The establishment of a scalable information sharing process to ensure that owners and operators are informed of pertinent real-time cyber threat information would be a valuable resource for enhancing individual company and aggregate industry cyber defenses.

In the context of broader cybersecurity policy, inter-industry and industry-government information sharing potentially conflicts with numerous significant statutory provisions, including ECPA,[11] the Freedom of Information Act,[12] antitrust restrictions on intercompany sharing of proprietary information,[13] and privacy provisions in the Communications Act.[14] As with the liability concerns related to network monitoring and the deployment of cybersecurity

---

[10] In cases where a vendor or service provider is providing direct support related to network security, ISPs may need to share personally identifiable information in order to protect subscribers.

[11] 18 U.S.C. § 2511(1)-(2).

[12] 5 U.S.C. § 552.

[13] 15 U.S.C. §§ 1-2.

[14] 47 U.S.C. § 605.

countermeasures, uncertainty over the applicability of these laws can create procedural impediments to the timely sharing of relevant cybersecurity information.

To effectively alleviate these concerns and promote adoption of the Cybersecurity Framework, federal legislation should make clear that companies are authorized, for cybersecurity purposes,[15] to undertake network monitoring, cyber threat countermeasures, and information sharing notwithstanding any other provision of law. As noted above, this approach recognizes that it is impossible as a practical matter to specifically identify each statutory provision that could impede these efforts now or in the future.

C. Preemption of Conflicting State and Local Laws Will Ensure a Uniform National Framework for Cyber Defense Activities.

The objective of a uniform national cybersecurity policy requires preemption of state and local laws to the extent that they may otherwise impose limitations or obligations that are inconsistent with national policy. These include not only state privacy laws[16] that could inhibit the sharing of threat information and monitoring for cyber threats, but also tort and contract law that could impede the utilization of cybersecurity countermeasures because of liability concerns.

Cable companies face the task of complying with statutory, regulatory, and common law regimes in every state and local jurisdiction in the country, but cybersecurity can only be addressed on a federal level. Threats originate nationally and globally, and deterrence must likewise operate uniformly across state lines. The legal framework for these activities must therefore be uniform across state lines. State-by-state liability and privacy requirements will

---

[15] *See, e.g.*, H.R. 629 (Cyber Intelligence Sharing and Protection Act), 113th Cong., 1st Sess. (2013), § 3(a) (adding § 1104(h)(8) to the National Security Act of 1947) (defining "cybersecurity purpose").

[16] Most states have their own wiretap and electronic communications statutes. *See, e.g.,* Ala. Code §13A-11-30; Cal. Penal Code §§ 631, 632; Ohio Rev. Code Ann. §2933.52. In addition to the federal privacy statutes noted above, cable operators also may be subject to additional privacy requirements under state law and their franchise agreements. Further, forty-six states (plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands) have data breach notification laws. *See, e.g.,* Ark. Code tit. 4, ch. 110 §§ 101-08; Cal. Civ. Code §§ 56.06, 1785.11.2, 1798; Conn. Gen Stat. § 36a-701(b).

create substantial legal uncertainty and ultimately lead to cybersecurity protection that varies by state.[17]

D. Financial Incentives Will Help Alleviate the Financial Burden of Implementing the Cybersecurity Framework.

Finally, the cost of implementing effective cybersecurity practices can be prohibitive for some companies. Effective cybersecurity measures generally require ongoing capital investment, continuous research and development, and the expense of hiring and training skilled personnel. The government should promote investment in cybersecurity by providing grants and other financial support for companies and organizations dedicated to the research and development ("R&D") of creative technologies designed to thwart cybercrime, increase information sharing among providers, and protect consumers.

Congress has previously provided funding to facilitate private sector compliance with law enforcement-related obligations and to promote within the private sector the kind of high-risk, high-reward research that is now needed to support the cybersecurity of our national critical infrastructure. For example, the Communications Assistance for Law Enforcement Act (CALEA) authorizes funding to help defray carrier costs associated with the modification of equipment necessary to establish the capabilities required by CALEA.[18] The Stored Communications Act (SCA) requires government entities to reimburse providers of electronic communications and remote computing services for "reasonably necessary" costs that they incur in searching for, assembling, reproducing, or otherwise providing the content of

---

[17] For example, state wiretap statutes may differ with respect to the manner and extent to which they authorize network providers to take steps to ensure the security and integrity of their networks, or the degree and circumstances under which they permit cyber threat and incident information to be shared with other network providers.

[18] *See* 47 U.S.C. § 1008.

communications, records, and other information to those entities in accordance with the SCA.[19] Programs such as NIST's Technology Innovation Program have helped to promote and accelerate R&D in areas of critical national need.[20] The government should explore ways to adapt or expand similar funding programs to cyber defense.

Cyber criminals are constantly innovating, developing new strategies and tactics to circumvent the most recent generation of tools and assets available on the market. Cybersecurity is essentially an arms race, and network operators must continually develop and invest in new defenses and strategies. Government support of R&D, and tax incentives for investment in and deployment of cyber assets are critical because, as important as cyber defense products and services are, their economic benefits often take time to materialize while their costs are immediate and ongoing. The costs associated with investments in cyber defense assets are especially problematic for small companies, but can also deter investment and R&D by large companies that must decide where and how to spend their development budgets.

The Incentives Working Group of the Department of Homeland Security's Integrated Task Force has identified several financial incentives that will go a long way toward encouraging the adoption of cybersecurity practices. First, the government should offer grants that provide direct federal funding for investment in cybersecurity products and services for critical infrastructure owners and operators, and support research and development projects recommended by Sector Specific Councils. Grant programs would have to be carefully developed and remain technology neutral to promote innovation and to allow companies maximum flexibility to identify the right tools for their individual needs.

---

[19] *See* 18 U.S.C. § 2706.

[20] *See* 15 C.F.R. § 296.

Likewise, the government can offer tax credits and deductions for network providers and critical infrastructure owners and operators who implement cybersecurity measures. Tax incentives should take into account the costs associated with cyber-related personnel, network improvements, and capital investment. As with grants that provide direct federal funding, any tax incentives must be technology neutral and must avoid limiting benefits to companies that adopt specific cybersecurity standards and practices.[21]

II. THE GOVERNMENT'S CYBER POLICY FRAMEWORK SHOULD BE PREDICATED UPON REGULATORY RESTRAINT AND SHOULD NOT CATEGORICALLY EXCLUDE ANY RELEVANT INDUSTRY SECTOR.

As the Obama Administration's Cyberspace Policy Review noted in 2009, the federal government should "be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security."[22] Even the most comprehensive and forward-thinking regulation is likely to restrict or otherwise minimize the overall effectiveness of research and development to combat cybercrime. Energy spent on developing creative and effective solutions will be shifted to focus on regulatory compliance. It is therefore essential that any government effort to facilitate the further development of Internet security does not impede the private sector's flexibility to address ever-changing cyber threats.

Regulatory restraint must figure prominently in all aspects of cybersecurity policy, including the assessment of incentives to promote voluntary participation by the private sector. A clear statement that NIST's voluntary cybersecurity framework will not serve as a predicate

---

[21] The government should consider using tax incentives to encourage the use of cyberinsurance programs. Cyberinsurers can encourage the adoption of cybersecurity best practices by basing cyberinsurance premiums on the insured's level of protection. Whereas incentives that tie government sponsored benefits to the adoption of specific pre-approved cybersecurity standards and practices can lead to technological stagnation, cyberinsurance programs that are driven by market forces can quickly adapt to new innovations and reward private companies for developing new tools and techniques to strengthen cybersecurity. *See, e.g.*, Dep't of Commerce Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy*, at 23-27 (June 2011).

[22] Cyberspace Policy Review, *Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 31, 2009, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

for prescriptive regulatory directives will encourage adoption and participation by the private sector, albeit in a manner appropriately tailored to, and reflective of, each particular company's network architecture and business operations. Many of the proposed incentives identified by the Incentives Working Group contemplate the use of preferential treatment – such as public recognition (the so-called "name-and-shame" approach) and prioritized technical assistance – to encourage compliance with a critical set of minimum security standards. This is the wrong approach. Tying rewards and benefits to a prescribed set of standards creates reverse incentives that would stifle innovation and lead to implementation of only the bare minimum in preventative measures.

Adopting this approach to the Cybersecurity Framework not only risks impairing companies' effectiveness in dealing with cybersecurity threats, it could also facilitate security breaches. Reliance on a common set of government-sanctioned standards and protocols would make it easier for cyber criminals to circumvent security measures and locate "soft spots" in the ecosystem's security. Name-and-shame would likewise call attention to vulnerabilities in critical infrastructure that will draw the attention of those entities intent on launching cyber attacks. Our national cyber defense posture is best served by policies that promote a flexible, solutions-oriented process, that builds on existing industry collaborations and encourages experimentation, while avoiding a constrictive, one-size-fits-all, top-down approach that mandates conformity with prescriptive measures.

It is particularly important that ISPs and other broadband service providers be afforded maximum flexibility to develop and implement diverse cybersecurity practices and protocols to deal with unanticipated problems when they arise. Whatever incentives the Cybersecurity Program eventually offers, they must not be limited to a provider's adoption of a specified list of

standards or practices. Making clear that incentives are available in connection with the adoption of "consensus standards and industry best practices"[23] will promote innovation and allow companies the flexibility required to face future cybersecurity challenges.

Another critical *dis*incentive to strong cyber defense is a policy framework that peremptorily excludes certain sectors, or shifts the costs and burdens associated with ensuring that cyber defense assets and tools conform to that framework. For example, the Executive Order excludes commercial IT products and consumer information technology services from the definition of at-risk critical infrastructure,[24] even though the IT sector has a crucial role to play in securing critical networks.[25] As discussed in NCTA's comments in response to the NIST RFI on the development of a cybersecurity framework, IT products and services represent the gateways through which cyber threats can enter the Internet ecosystem.[26] In a recent study, DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) found that almost half of cyber vulnerabilities to critical infrastructure networks identified last year appeared to relate to inherent flaws in the IT hardware/software solution or deficiencies best addressed by the original IT service provider.[27]

IT products and services are an integral part of broadband architecture, and there is no justification for imposing the cost and technical burdens on ISPs and other network providers to detect and address deficiencies in the performance of IT products and services that are part of

---

[23] *See* Cybersecurity EO at 11741.

[24] *See id*. at 11742.

[25] As set forth in the U.S. Anti-Bot Code of Conduct for Internet Service Providers adopted by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC III), "constituents of the entire Internet ecosystem have important roles to play in addressing the botnet threat . . . it is essential to recognize the shared responsibilities that exist across the broad internet ecosystem," Working Group 7, Final Report on Botnet Remediation, Mar. 2013 at 3.

[26] *See* NCTA Cybersecurity Framework Comments at 24.

[27] *See* ICS-CERT Monitor, Q42012 at 5, *available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf.

their networks. This responsibility is most appropriately borne by the IT sector itself, which has its own manufacturers and service providers and are in a better position to identify issues with the individual components of their own products. ISPs simply cannot be held responsible for deficiencies that may occur at any point in the supply chain. Indeed, the added costs associated with identifying and remediating issues with equipment provided by a third party vendor may inhibit cybersecurity efforts by network operators and owners.

CONCLUSION

The most effective way to encourage adoption of improved cybersecurity practices is to eliminate the obstacles that currently stand in the way. Cable operators and other broadband Internet service providers have ample market-based incentives to maximize the security of their networks, but there are legal and financial difficulties associated with implementing advanced cybersecurity measures. The government can and should take steps to alleviate these impediments, while also avoiding any measures that would tie potential benefits to the adoption of prescriptive practices and protocols.

Respectfully submitted,

/s/ Rick Chessen

Howard J. Symons
Christopher J. Harvie
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Rick Chessen
Loretta Polk
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

April 29, 2013