Before the
National Institute of Standards and Technology
National Telecommunications and
Information Administration

In the Matter of	**)**	
	)	
Incentives To Adopt Improved	**)**	**Docket Number 130206115–3115–01**
Cybersecurity Practices	**)**	

COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION

USTelecom[1] provides these comments to the Department of Commerce through the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) (collectively "the Department") in the above referenced proceeding.[2] The Department is evaluating incentives designed to promote participation in a voluntary cybersecurity framework being developed by the Department of Homeland Security (DHS).[3] That framework is being designed by the Department and NIST to reduce cyber risks to critical infrastructure (the "Framework").[4]

USTelecom supports the use of incentives to promote increased voluntary adoption of the Framework. In fact, in its recent comments regarding the development of the Framework,

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks.

[2] Federal Register Notice; Notice of Inquiry, *Incentives To Adopt Improved Cybersecurity Practices*, 78 Fed. Reg. 18954 (March 28, 2013) (*Notice*).

[3] Notice; Request for Information, *Developing a Framework To Improve Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 13024 (February 26, 2013) (*Framework Notice*).

[4] *See*, Comments of United States Telecom Association, submitted April 8, 2013, *Framework Notice* proceeding (*USTelecom Framework Comments*).

USTelecom emphasized that incentives should be considered "an integral component" of any public-private approach associated with its implementation.[5]

USTelecom's members already have substantial market-based incentives to invest in, and secure critical communications infrastructure. Regardless of the type of network platform, private companies' business models are fully dependent on having a secure, resilient, always on and reliable network. Any flaws in secure and reliable infrastructures results in member companies losing customers and business in a highly competitive market. As a result, these companies today take substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace.

Despite this strong incentive, there are important criteria to consider for any external incentives developed by the Department for increased involvement in the framework. First, the Department should ensure that any incentives that they recommend are sufficient to meet traditional cost-benefit analyses. The absence of such an approach is likely to serve as a disincentive for companies to implement certain cybersecurity-related measures. Second, it is imperative that whatever best-practices are ultimately adopted, they do not transform into de facto government mandates. The value of incentives intended to steer the private sector towards adoption of the Framework is dependent upon the value of the framework itself. A rigid, top down, checklist or regulatory approach will have little value and applicability in an environment with emerging cyber threats and runs the risk of distorting the marketplace by driving the private sector towards inefficient, rote checklists that could make us less secure. Finally, there are specific incentive proposals that warrant consideration by the Department, including regulatory safe harbors for firms that adopt the framework.

[5] *USTelecom Framework Comments*, p. 16.

I. Incentives Must Align With Traditional Cost-Benefit Analyses.

The Department should ensure that any incentives proposed by NIST or the federal government align with traditional cost-benefit analyses. Through a viable incentives program, the federal government can help facilitate broader adoption of sound cybersecurity practices across *all* critical infrastructure and key resources.

Research has consistently shown that one of the most significant obstacles to cyber security improvement across critical infrastructure is cost.[6] The absence of cost-effectiveness could act as a disincentive for companies to implement certain cybersecurity-related measures. This issue was recently acknowledged by a cybersecurity working group within the Communications Security, Reliability and Interoperability Council (CSRIC). In a report released last month, CSRIC concluded that consideration must be given to the financial barriers that may limit the speed and scope of adoption of cyber-related solutions.[7]

For example, the CSRIC report notes that financial barriers can result from an inability to quantify costs or benefits associated with implementing specific recommendations, such as those related to cybersecurity. Cybersecurity related measures often require on-going capital and operating expenses; the larger the investment, the greater the expectation by management for rigorous cost-benefit analyses.[8] These financial considerations are even more critical in the current economic environment where investment decisions are constrained by budget limitations.

---

[6] Testimony of Larry Clinton, President & CEO Internet Security Alliance, before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives, *Cybersecurity: Threats to Communications Networks and Private-Sector Responses*, February 8, 2012 (available at: http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CT/20120208/HHRG-112-IF16-WState-LClinton-20120208.pdf) (visited April 29, 2013).

[7] CSRIC Working Group 7 - Botnet Remediation, Final Report, *U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs), Barrier and Metric Considerations*, March 2013.

[8] *Id.*, p. 11.

As Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President, noted last year when discussing federal agency cybersecurity efforts, agencies must implement the "most cost effective and efficient cybersecurity controls for Federal information system security," since agencies must "defend their information systems in a resource-constrained environment."[9]

II. Incentives Should be Designed to Support Innovation; Government Mandates Will Not Support Technology Innovation in Cyber Space.

In order for incentives to be broadly adopted, they must be flexible and non-prescriptive given the broad nature and significant number of stakeholders within the Internet ecosystem. 'One-size-fits-all' approaches to cybersecurity will be unworkable, and, as such, will neither be desirable nor effective regardless of any incentives that may be developed.[10] Solutions must allow the different participants in the ecosystem to tailor their solutions around business models that may or may not provide sufficient cost revenue mechanisms. The government should continue to encourage the use of best practices, which are developed using an ongoing, dynamic, and practical consensus process that moves at a more rapid pace that better corresponds with the dynamic nature of the cybersecurity environment.

---

[9] *See*, White House Blog, *Federal Departments and Agencies focus Cybersecurity Activity on three Administration Priorities*, March 23, 2012 (available at: http://www.whitehouse.gov/blog/2012/03/23/federal-departments-and-agencies-focus-cybersecurity-activity-three-administration-p) (visited April 25, 2013).

[10] Letter from Walter B. McCormick, Jr., President & CEO, USTelecom; Michael Powell, President & CEO, National Cable & Telecommunications Association; Steve Largent, President & CEO, CTIA – The Wireless Association, to Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, November 21, 2012 (available at: http://www.ustelecom.org/news/filings/multi-association-letter-administration-cybersecurity) (visited April 8, 2013) (*Multi-Association Letter*). As noted there, mandated practices and rules will undermine cybersecurity efforts by leading to uniformity and predictability; thereby making it easier for cybercriminals to prey on consumers and businesses. In addition, with "speed-of-response to cyber emergencies often measured in seconds, not hours or days, providers must be able to take decisive action without regulatory second-guessing or the need for a lengthy review and approval process."

The widespread use of consensus-based standards demonstrates the strong commitment of industry stakeholders to implementing robust cybersecurity measures. More importantly, these voluntary guidelines and established industry norms should be viewed as measures that are complementary to the ongoing innovation within the communications sector. While standards, norms and best practices may be adequate to address some known/current threats, we continue to see many entities that are the leading edge of adopting standards and practices that can fall victim to cyber attacks. Innovation is essential to guard against unknown/future threats given the constantly evolving nature of cybersecurity.

Along these lines, the Department must carefully balance the desire to encourage the adoption of the Framework, with the need to ensure that innovation continues to thrive. In other words, the Department must ensure that market realities are not distorted by directing too much effort towards adopting a Framework that ultimately exacerbates the cybersecurity challenge by directing the private sector towards a framework of standards and practices that is outdated and easily circumvented by adversaries. Such an outcome could crowd out investments in innovation and future services that may have a greater and more beneficial impact on increased cybersecurity.

III. Remarks on Specific Incentives.

USTelecom has identified numerous incentives that may be considered for adoption in the cybersecurity context. The incentives are grouped into categories reflecting those that would be beneficial; those with a marginal or questionable impact; and those that would be harmful to increased cybersecurity efforts.

A. The Implementation of Certain Incentives Would Greatly Benefit Increased Cybersecurity Efforts

There are incentives developed in other contexts that the Department should implement in order to encourage increased cybersecurity efforts. These include the implementation of safe harbors, increased information sharing, tax incentives, the use of appropriate and rationally constructed subsidies, and targeted grants.

First, the Department should consider some form of safe harbor. Establishing a safe harbor from future federal and state regulations for the implementation of the Framework would clearly incentivize companies to adopt enhanced cybersecurity measures. Given the uncertainties surrounding future regulation at both the federal and state level, companies would clearly see the benefits from adopting the Framework, given its inherent certainties and known business costs. Moreover, the establishment of a safe harbor provision would greatly assist the collaborative aspects of the Framework by introducing an increased element of trust and good faith between government and industry stakeholders.

Second, USTelecom and others have commented at length on the importance of increased information sharing in the cybersecurity environment.[11] While it is critical that private industry stakeholders can share information on cybersecurity threats with their federal government counterparts, the current legal frameworks concerning such sharing remains a substantial barrier

[11] *See e.g.*, comments submitted in response to the *Framework Notice*; Comments of Verizon and Verizon Wireless, p. 2 (emphasizing the importance of removing existing legal barriers to information sharing), Comments of CTIA – The Wireless Association, p. 15 (stating that companies actively engaged in cybersecurity "need to be able to communicate with competitors, federal government agencies, academia and subject matter experts to identify issues and create solutions before there is a problem."); ITTA Comments, p. 3 (stating that the cybersecurity Framework "should facilitate information-sharing between government and the private sector and should encourage widespread intelligence-sharing and limit provider exposure when engaging in good faith in such activities."); USTelecom Comments, pp. 12 - 14. Referenced comments are available at the NIST *Framework Notice* website (available at: http://csrc.nist.gov/cyberframework/rfi_comments.html) (visited April 29, 2013).

to effective information sharing between all relevant public and private stakeholders. The most important role government can play in encouraging efforts to detect and deter cyber threats is to enact legislation that removes this uncertainty and conclusively establishes that cyber threat monitoring and active defenses (*i.e.*, countermeasures) are lawful and encouraged. USTelecom is encouraged that the President's Executive Order on cybersecurity has been described as a "down payment" on future government legislation to secure U.S. critical infrastructure and networks.[12] The bipartisan passage of the "Cyber Intelligence Sharing and Protection Act" is an important step towards realizing this goal.

Third, the Department should also consider the use of tax incentives to encourage increased adoption of the Framework and/or cybersecurity measures. Tax incentives (whether in the form of tax credits or deductions) have been used successfully in a broad range of areas to achieve desired public policy outcomes. For example, in 2010, more than 7 million households claimed a residential energy tax credit to install qualified energy improving measures in their home.[13] Similarly, targeted tax incentives have been used to increase the number of first-time home buyers, and to assist families with paying for future expenses associated with college. The application of such tax credits in the cybersecurity environment would be tremendously beneficial.

Finally, the use of targeted subsidies and/or grants for the direct purchase of cybersecurity products and services may be helpful for increasing some companies' adoption of

---

[12] *See*, White House Press Release, Executive Order on Improving Critical Infrastructure Cybersecurity, February 12, 2013 (available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0) (visited April 8, 2013).

[13] Charlie McCrudden, *IRS Stats Suggest Residential Energy Tax Credit Helped Millions of Homeowners Install High Efficiency HVAC Products in 2010*, September 10, 2012 (available at: https://www.acca.org/archives/industry-resources/government-affairs/hot-air/7575) (visited April 24, 2013).

the Framework. Federal subsidies and grants have been used successfully in other contexts in order to achieve important public policy goals when the conditions for obtaining such subsidies do not discourage their use,[14] and their application in the cybersecurity environment could be appropriate. This is particularly the case since costs have previously been identified as one of the single biggest obstacles to the implementation of improved cybersecurity measures. Indeed, as President Obama's Cyber Space Review concluded "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost or complexity."[15] The use of targeted, rationally constructed subsidies and federal grants would help bridge this gap, by directing monetary resources towards increased cybersecurity measures.

B. The Benefits from Other Incentives are Marginal or Unclear

There are other incentives that would have a marginal or questionable impact on enhanced cybersecurity efforts, or are otherwise unclear in their potential impact. These include preferential procurement procedures, and prioritized technical assistance.

---

[14] For example, the Universal Service Fund, overseen by the Federal Communications Commission, is a program that increases access to advanced telecommunications services to consumers, particularly those in low income, rural, insular, and high cost areas at rates that are reasonably comparable to those charged in urban areas. Similarly, the Rural Utilities Service oversees various programs providing access to low-interest loans supporting deployment of telecommunications facilities in rural areas. Both subsidized programs partner with communications providers in the impacted areas, thereby leveraging the business and technical expertise of these companies. On the other hand, when companies perceive that "grants" are accompanied by onerous "strings" or conditions, as in some of the attempts to encourage the more widespread adoption of broadband services, companies are discouraged from applying for such subsidies.

[15] White House Cyberspace Policy Review, *Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, p. 31 (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited April 25, 2013).

First, any benefits flowing from preferential procurement considerations would depend largely on how such incentives are structured. USTelecom maintains that preferential procurement benefits should not necessarily be predicated upon the adoption of the Framework. For example, it is possible that improved cybersecurity could result by granting such procurement benefits to innovative companies operating outside of the Framework. It is also possible that such preferential consideration could become a barrier to entry for some companies, by adding excessive overhead costs to the risks being addressed. In any event, the Department should carefully construct such procurement considerations to ensure that they are equitably applied, and do not serve to undercut their intended purpose.

It is also unclear whether prioritized technical assistance would lead to improved cybersecurity measures or Framework adoption. While this assistance may be beneficial for companies with more limited resources, it may be unnecessary or redundant for larger companies. Moreover, depending on the perceived value of such prioritized assistance, the Department may need to consider whether limited federal resources should be directed towards such an effort.

Finally, the creation of new regulations or legislation modeled on the SAFETY Act would at best have a marginal impact and could in fact be harmful to cybersecurity efforts. In general, the SAFETY Act provides liability protections for providers of certain anti-terrorism technologies, whether in the form of products or services. The utility of applying the SAFETY Act in the cybersecurity context is unclear. To the extent that legislation modeled after the SAFETY Act was tied to the adoption of specific technologies and solutions for cybersecurity it could be unhelpful given the evolving nature of the threat. However, as noted above, broad

based liability protections in return for the adoption of a flexible, industry led, adaptive cybersecurity framework could indeed be helpful.

C. The Implementation of Certain Benefits Would be Harmful to Increased Cybersecurity Efforts

Finally, the Department should avoid certain proposals that would likely harm increased cybersecurity efforts. These proposals include incorporation of cybersecurity measures into the rate base; public notification of disclosures; and new regulations focused on cybersecurity related issues.

First, inclusion of cybersecurity investments in the rate base would be harmful to increased cybersecurity efforts. Because the services of many USTelecom members are no longer rate of return regulated there would be no benefit to including such costs in the rate base. Moreover, unlike other utilities (*e.g.* electric and water), communications providers are not monopolies within any respective market. As a result, forcing such providers to include cybersecurity related costs in the rate base would distort the competitive marketplace, while penalizing providers implementing improved cybersecurity measures.

For example, in any particular market USTelecom's members (which include traditional wireline phone companies) face competition from cable providers, overbuiliders and multiple wireless providers. They also face robust competition from non-facilities-based providers in the voice market (*e.g.*, Skype, Vonage, etc.) and video market (*e.g.*, Netflix, Hulu, etc.). Local telephone companies recovering cybersecurity related costs would be forced to raise the price for their respective rate regulated services, while their non-rate regulated competitors would not. Such market distorting influences would adversely the maintenance and deployment of communications critical infrastructure, and should be avoided.

Second, it would be harmful to the overall cybersecurity efforts to require the public disclosure of cybersecurity attacks. As USTelecom has previously noted, the owners and operators of communications critical infrastructure take the protection of their networks from cyber-attacks seriously. The public disclosure of such attacks will do little – if anything – to compel such owners and operators to avoid security breaches, since they already have substantial incentives to do so.[16] In fact, rather than act as an incentive, the public disclosure of such breaches would only serve to educate the attackers and increase the risk.

IV. Conclusion

USTelecom supports the use of incentives to promote increased voluntary adoption of the Framework. Any such incentives must align with traditional cost-benefit analyses, and should be designed to support innovation. The implementation of safe harbors, increased information sharing, implementation of tax incentives and rationally constructed subsidies or targeted grants are examples of incentives that would encourage increased cybersecurity efforts.

Respectfully submitted,
UNITED STATES TELECOM ASSOCIATION

By: 

Kevin Rupy
Robert Mayer

607 14th Street, NW, Suite 400
Washington, D.C. 20005

April 29, 2013

[16] *See e.g.* Comments of USTelecom at the FCC, *Cyber Security Certification Program*, PS Docket No. 10-93 (submitted July 12, 2010).