Before the
U.S. Department of Commerce
National Institute of Standards and Technology

In the Matter of	)	
	)	
Developing a Framework To Improve	)	**Docket Number 130208119–3119–01**
Critical Infrastructure Cybersecurity	)	

COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION

Kevin Rupy
Robert Mayer
David Cohen

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

April 8, 2013

Table of Contents

* * *

Before the
U.S. Department of Commerce
National Institute of Standards and Technology

In the Matter of	**)**	
	)	
Developing a Framework To Improve	**)**	**Docket Number 130208119–3119–01**
Critical Infrastructure Cybersecurity	**)**	

COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION

USTelecom[1] provides these comments to the Department of Commerce (Commerce) and the National Institute of Standards and Technology (NIST) (collectively "the Departments") in the above referenced proceeding,[2] regarding the development of a framework to reduce cyber risks to critical infrastructure (the "Framework"). In order to develop an effective Framework that is optimized for addressing cyber-security-related risks across all sixteen critical infrastructure sectors, the Departments' efforts should be informed through eight guiding principles.

First, the Framework must acknowledge the shared responsibility of all stakeholders who collectively comprise the vast Internet ecosystem. Because of the interdependent, interconnected and global nature of cyberspace, an effective cybersecurity Framework must ensure that the costs of protecting and securing this evolving ecosystem are borne by all participants who are positioned to improve the resiliency and security of the Internet ecosystem and not inappropriately shifted to downstream entities.

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

Given the rapid and ever-changing nature of the cybersecurity threat, a successful Framework must be flexible and adaptable. This acknowledges the difficulty of predicting in advance the manner and means by which network providers will have to respond to cybersecurity threats. The Framework should also avoid a counter-productive regulatory approach which would divert resources and attention from deterrence to compliance with particular rules that will quickly become outdated.

The Framework should be based on mutual interest and trust. It should reflect the primacy of the public-private partnership model which has an established, successful history and is ideally suited for application in the current context.

The Framework should foster increased information sharing between private industry and government stakeholders. The continuing legal uncertainties surrounding such information sharing, and their effect on limiting the sharing of relevant information about cyber threats, stands as a substantial cybersecurity challenge.

The Framework should encourage the development of business-case analyses that are vital to securing funding for investments in cybersecurity. Some companies will have business models supporting cost-recovery for cyber-related efforts, while others may not, and the Framework must address this potential barrier to successful implementation of effective cybersecurity measures. The Framework must also recognize that in instances where the need to invest goes beyond the ability to make the business case, incentives will be necessary to promote adoption of best practices.

Finally, the Departments must ensure that the Framework promotes efficient and integrated coordination of federal governmental cybersecurity efforts. In particular, there is urgent need for greater federal level coordination regarding the increasing number of federal agencies with involvement in cybersecurity issues.

I. The Framework Should Treat the Protection and Security of Critical Infrastructure from Cyber-Threats as a Shared Responsibility Across all Participants who are part of the Internet Ecosystem.

The Framework developed by the Departments must acknowledge the interdependencies between the broad and diverse range of stakeholders throughout the Internet ecosystem, given the profound cybersecurity threat to a broad range of areas – including national security, economic security, civil liberties and privacy. A Framework that focuses on a single solution or discrete industry segments would be the equivalent of a modern-day Maginot Line – a formidable single line of defense that creates the illusion of security, but is easily circumvented.

An effective Framework must acknowledge the basic tenet that protection of the Internet Ecosystem is a shared responsibility and that all participants have "skin in the game." The voluntary Cybersecurity Framework developed by the Departments must therefore apply to application and operating system developers, device manufacturers, Internet service and cloud service providers, search engine and website owners, anti-virus and security vendors, and others who are deemed critical infrastructure sectors under Presidential Policy Directive/PPD21.[3] The Framework must lead to efforts to hold entities responsible for creating vulnerabilities accountable and deter any efforts by any stakeholder group to shift burdens downstream to other sectors or enterprises.

The Internet is a highly complex global system of networks, the product of connections that allow for interaction between hundreds of millions of systems and devices each day.

[3] Presidential Policy Directive/PPD-21, *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, February 12, 2013 (available at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil) (visited April 8, 2013).

Though these structures differ in terms of size, capacity, function, and purpose, together they form an expansive and dynamic ecosystem through which massive amounts of data are transferred and exchanged. Any discussion of cybersecurity must therefore address all aspects of the Internet environment, to include products, functions and services, such as those provided by the above listed participants. Such a holistic approach is essential, based on the organic nature of the Internet. In this sense, the Internet has developed an organic quality insofar as it continually grows and adapts in response to newly added systems, functions and services.

For example, a study from Cisco concluded that in 2008 the number of devices connected to the Internet exceeded the number of people on earth – and by 2020, Cisco projects there will be 50 billion devices connected to the Internet. [4] Similarly, while concepts such as cloud computing were viewed as a "risky bet" a mere seven years ago,[5] cloud computing is emerging as one of the most vibrant competitive industries in today's marketplace. Analysts expect that spending on public cloud services will increase 20 percent in 2012, to $109 billion, from $91 billion in 2011. By 2016, such expenditures could nearly double, to $207 billion.[6] As such, the Framework developed by the Departments must acknowledge the broad and diverse nature of products, services and devices that comprise the Internet.

Doing so would help ensure that any resulting policy initiatives flow throughout the Internet ecosystem. This is particularly important, since participants in the Internet ecosystem

[4] Arik Hesseldahl, *Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting*, All Things Digital website, July 14, 2011 (available at: http://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-internet-is-and-how-big-its-getting/?mod=googlenews) (visited April 4, 2013).

[5] Bloomberg Business Week, *Jeff Bazos' Risky Bet*, November 13, 2006 (available at: http://www.businessweek.com/magazine/content/06_46/b4009001.htm) (visited April 4, 2013).

[6] *See*, Hardy, Quentin, New York Times Bits Blog, *Information Technology Spending to Hit $3.6 Trillion in 2012, Report Says*, July 9, 2012 (available at: http://bits.blogs.nytimes.com/2012/07/09/information-technology-spending-to-hit-3-6-trillion-in-2012-report-says/) (visited April 4, 2013).

operate in both an autonomous and interdependent fashion. As a result, changes in one product or service may significantly implicate other entities within the Internet ecosystem. Consequently, it is impossible to isolate individual components of the Internet, since regulating some components (*e.g.*, broadband networks) would in no way guarantee the security in other equally important components (*e.g.*, software products).

For example, the 2010 attack on Google and at least thirty-three other companies from an entity in mainland China demonstrated how various Internet components are inextricably linked.[7] The theft of Google's information, including a password system that controlled millions of users' access to a variety of web services, including business services, was initiated when hackers sent an instant message to a single Google employee in China. The instant message linked to a website that enabled hackers to manipulate the employee's personal computer. Using that *single computer* as an access point, the hackers gained further access to Google's network at its headquarters in California. From there, they accessed a critical software repository that contained the information that they stole. The hackers transferred the stolen information to another set of computers in Texas, and from there to an unknown location. The attack on Google highlights how vulnerabilities in a *single* area within the Internet ecosystem can cause reverberations throughout the *entire* Internet ecosystem.

Exploitation of vulnerabilities can be achieved through any number of access points throughout the Internet ecosystem. Indeed, some of the most newsworthy events in recent years

[7] See, David E. Sanger, John Markoff, *After Google's Stand on Chine, U.S. Treads Lightly*, New York Times, January 14, 2010 (available at: http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=1&ref=technology) (visited April 4, 2013).

have highlighted the vulnerabilities contained in software (*e.g.*, Conficker and Stuxnet),[8] consumer websites (*e.g.*, the recent wave of attacks against six major American banks),[9] hardware (*e.g.*, acknowledgement that imported electronics are sometimes pre-loaded with malware),[10] and even consumer end-users. As noted in the recent report from Mandiant, once a hacker has breached any of these individual vulnerabilities, its ability to impact other segments of the Internet environment is increased.[11] The Framework must therefore be developed in a way that acknowledges the diversity of products, services and devices that comprise the Internet.

II. The Framework Should be Designed to Ensure Approaches That are Flexible and Non-Prescriptive.

For the Framework to be effectively implemented, it 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. Solutions must allow the different participants in the ecosystem to tailor their solutions for their different business models and access to resources.

A recent report issued by the Government Accountability Office (GAO) underscores this point by cataloguing the voluminous cybersecurity guidance currently available from national

[8] David Sanger, New York Times, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, June 1, 2012 (available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html) (visited April 4, 2013).

[9] Nicole Perlroth, New York Times, *Attacks on 6 Banks Frustrate Customers*, September 30, 2012 (available at: http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html) (visited April 4, 2013).

[10] Geoff Duncan, Digital Trends, *DHS aware of imported electronics pre-loaded with malware*, July 11, 2011 (available at: http://www.digitaltrends.com/international/dhs-aware-of-imported-electronics-pre-loaded-with-malware/) (visited April 4, 2013).

[11] *See e.g.*, Mandiant Report, *APT1, Exposing One of China's Cyber, Espionage Units*, pp. 34 – 36. *See also*, New York State Office of Cyber Security website, *Cyber Security Advisories* (available at: http://www.dhses.ny.gov/ocs/advisories/) (visited April 4, 2013).

and international organizations for entities within all seven critical infrastructure sectors.[12] These wide-ranging and detailed guidelines highlight the futility of attempting to develop a one-size fits all solution across even one of the seven critical infrastructure sectors.

The extensive and evolving catalogue of standards, best practices and guidance – which GAO acknowledges is not all-inclusive[13] – has been developed over several years through various public-private frameworks across all seven critical infrastructure sectors, and GAO acknowledges that much of this guidance is "tailored to business needs of entities or provides methods to address unique risks or operations."[14]

Stakeholders within the communications sector are already leveraging existing industry practices and norms, as demonstrated by the detailed record of standards contained in the GAO report. The guidance documents for the communications sector contained in the GAO report cover a variety of topics such as telecommunication industry security standards, network engineering standards, and security configuration guides. GAO concluded that the standards listed in the report are "all widely used within the sector."[15] GAO also found that while the use of cybersecurity guidance is not mandatory, private entities voluntarily implement such guidance to mitigate risks, protect intellectual property, ensure interoperability among systems, and encourage the use of leading practices.[16]

[12] Government Accountability Report, *Critical Infrastructure Protection, Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, December, 2011, GAO 12-92 (*GAO Report*). The seven critical infrastructure sectors are: banking and finance; communications; energy; health care and public health; information technology; nuclear reactors, material, and waste; and water.

[13] *GAO Report*, p. 53.

[14] *Id.*, p. 2.

[15] *Id.*, p. 16.

[16] *Id.*, p. 32.

The widespread use of these 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 are adequate to address known/current threats, innovation is essential to guard against unknown/future threats given the constantly evolving nature of cybersecurity. Mandated federal cybersecurity standards, norms or best practice would negatively impact this innovation and would prove to be counterproductive to ongoing cybersecurity efforts. Furthermore, any effort to transform voluntary best practices derived in consensus-based venues into prescriptive mandates would have a serious chilling effect on future partnership and voluntary initiatives.

The Departments should foster this mutually beneficial environment by developing a flexible, non-prescriptive Framework to ensure that private industry stakeholders can continue to respond to cyber-threats in a rapid and efficient manner. As USTelecom noted in a letter to the White House last year, 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."[17]

Given the continuously evolving nature of the cyber threat, it is imperative that private industry stakeholders are afforded the flexibility to respond to such threats in a rapid and

[17] 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*).

efficient manner. A prescriptive Framework would run counter to this reality by imposing time-consuming, bureaucratic inertia into the cyber-threat response process.

III. The Framework Should Promote Innovation as a Key Goal.

Innovation is the most important and effective means to combat cyber threats and USTelecom is encouraged that the Departments acknowledge its importance in the Notice.[18] Private industry stakeholders must continually innovate not only to stay competitive in the marketplace, but to remain ahead of constantly evolving cyber-related threats. Given the importance of a fertile environment for innovation, it is imperative that the Departments ensure that the Framework does not hinder the ability of private industry stakeholders to innovate in the marketplace.

In light of the rapidly changing, and constantly evolving nature of cyber threats, the most realistic weapon in developing effective cybersecurity is private sector innovation and flexibility. Cybersecurity is a fundamental component to the business models of private entities in the communications sector, given the importance to its customers and to its own economic viability. In a highly competitive market, the risk of reputational harm is a strong incentive against complacency and cybersecurity prevention, detection, mitigation and response capabilities are an essential element of business continuity plans. As a result, private entity stakeholders substantially invest in innovative technologies and these efforts have resulted without overly prescriptive norms. The Departments should therefore enshrine innovation within the Framework as an essential policy goal. When the Department of Commerce completed its notice

[18] *Notice,* p. 13025 (stating that "[s]teps must be taken to enhance existing efforts to increase the protection and resilience of this infrastructure, while maintaining a cyber-environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties.").

of inquiry in 2011 on innovation and the Internet Economy,[19] it concluded that the federal government has an interest in "avoiding fragmented and unpredictable rules that frustrate innovation."[20] Indeed, the May 2009 report to the President, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," made clear that maintaining an Internet environment that promotes innovation was a "top priority for the nation."[21] The Departments should also ensure that the Framework does not impose technological and/or costly mandates, and includes viable incentives.

IV. The Framework Should Promote a Partnership Based on Mutual Interest and Trust.

Only through cooperative efforts can critical cybersecurity goals be successfully attained. Cybersecurity is a highly complex issue that impacts a global set of stakeholders that include public and governmental entities. In such a complex environment, when attacks of a serious nature occur, the general practice is to immediately engage multiple stakeholders (*e.g.*, ISPs or government entities) who have unique perspectives and capabilities that must be brought to bear to address the threat. A cooperative approach has been consistently identified by many key organizations as an essential component of the nation's cybersecurity strategy.[22] It is imperative

[19] http://www.commerce.gov/news/press-releases/2011/06/08/commerce-department-proposes-new-policy-framework-strengthen-cybersec (visited April 3, 2013).

[20] Green Paper, The Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy*, p. vi, June 2011 (available at: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf) (visited April 8, 2013).

[21] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications* Infrastructure (2009) (available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) (visited April 4, 2013) (*Cyberspace Policy Review*).

[22] *See e.g.*, Center for Strategic and International Studies Report, Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, December 2008, pp. 43 – 48 (stating that the U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and

that the framework be based on the primacy of the public-private partnership model. Such models have an established, successful history and have been widely embraced by government and industry alike.[23] The public-private partnership model is ideally suited for incorporation into the Framework, and USTelecom has commented at length on the many benefits of such an approach.[24]

Being that the majority of critical infrastructure at issue is privately owned, cooperative efforts between public and private entities are a pragmatic approach to effective cybersecurity. Moreover, the consultative nature of such an approach has the greatest likelihood of success, due to its collaborative nature.

responsive activities) (available at: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf) (visited April 4, 2013); *see also*, *Cyberspace Policy Review*, p. iv (stating that the Federal government should enhance its partnership with the private sector); *see also*, Intelligence and National Security Alliance Report, *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*. November 2009, p. 3 (stating that an effective public-private partnership for cyber security would provide the abilities to detect threats and dangerous or anomalous behaviors, to create more secure network environments through better, standardized security programs and protocols and to respond with warnings or technical fixes as needed) (available at: http://www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx) (visited April 4, 2013).

[23] As DHS Secretary Janet Napolitano concluded in a speech on cybersecurity issues, "[t]o be most effective, we in government must work closely with the private sector, and include it in our work as a full partner from the very start." Secretary's Web Address on Cybersecurity, *A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack*, October 20, 2009 (available at: http://www.dhs.gov/ynews/gallery/gc_1256070988236.shtm) (visited April 4, 2013). President Obama framed his Administration's policy more emphatically, when he stated, "[s]o let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity." Cross Sector Cyber Security Working Group, Incentives Subgroup, *Incentives Recommendations Report*, September 2009, p. 6.

[24] *See e.g.* USTelecom Comments, FCC Proceeding, GN Docket No. 09-47, submitted November 12, 2009; *see also*, USTelecom Comments, FCC Proceeding, PS Docket No. 10-93, submitted July 12, 2010; *see also*, USTelecom Comments, NIST Proceeding, 100721305–0305–01, submitted September 20, 2010; *see also, Multi-Association Letter*.

Private entity and government stakeholders also have a shared, mutual interest in ensuring the security of all critical infrastructure. Private entity stakeholders already have strong market-based incentives to secure their infrastructure since they operate in highly competitive marketplaces, and their business models are fully dependent on having a secure, resilient and reliable network.[25] Because failures in the cybersecurity realm would result in substantial losses of both customers and revenue, companies invest billions of dollars annually to expand and enhance the security of their networks and infrastructure.[26] For government stakeholders, the national security and public safety concerns related to effective cybersecurity have been well documented. Collectively, private entity and government stakeholders have compelling reasons to work together in a cooperative and effective manner.

Finally, government and private stakeholders can accomplish more working through a collaborative and cooperative effort where each side brings complementary competencies, resources, and capabilities. For example, private stakeholders have valuable entrepreneurial and innovative insights that are of tremendous value to the cybersecurity effort. Additionally, these stakeholders have important insights into cybersecurity approaches that can or cannot work in a competitive marketplace. For its part, the federal government has vast resources in the form of extensive expertise, access to critical resources and a diverse and substantial user base.

V. The Framework Should Foster Increased Information Sharing and Liability Protections for Private Industry Stakeholders.

The Departments must ensure that the Framework fosters increased information sharing between private industry and government stakeholders. USTelecom's members strive to protect their broadband networks and customers from cybersecurity threats. In doing so, however, they

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

[26] *Id.*

face the dual challenge of the risks posed by cyber threats themselves and the uncertainty associated with existing laws when applied to cyber-threat monitoring and response efforts that are utilized to protect their networks during a variety of circumstances.

The current legal frameworks concerning the collection, use, and sharing of information between and among network operators and with the government remains a substantial barrier to effective information sharing between all relevant public and private stakeholders. USTelecom believes that this continuing legal uncertainty, and its effect in limiting the sharing of relevant information about cyber threats, stands as the primary cybersecurity challenge facing our nation today.

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, but the inability of private sector stakeholders to share information with each other, as well as with federal agencies, must ultimately be addressed.[27]

The Executive Order emphasizes the sharing of information on a 'one-way' basis (*i.e.*, from the federal government to private stakeholders), and the Departments should ensure that this guidance is fully implemented into the final Framework. By increasing the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities, the

[27] *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).

federal government and private sector will be able to more efficiently detect, deter and respond to cyber threats.

The Departments will therefore need to ensure that the Framework fosters the development of mechanisms that foster the rapid dissemination of reports to private sector partners. Among other things, the Framework should quickly implement the expansion of the Enhanced Cybersecurity Services program beyond the Defense Industrial Base to all critical infrastructure sectors. In addition, the Framework should fully implement the Executive Order's expansion and expedite the processing of security clearances to certain personnel employed by critical infrastructure owners and operators.

VI. The Framework Should Encourage the Development of Business-case Analyses That are Vital to Securing Funding for Investments in Cybersecurity.

Given that the majority of critical infrastructure is controlled by private companies, the Framework developed by the Departments must acknowledge the realities of the commercial marketplace. Even within individual critical infrastructure sectors, some companies will have business models supporting cost-recovery for cyber-related efforts, while others may not. The Departments' final Framework must acknowledge these realities since they represent a significant barrier to adoption and successful implementation of effective cybersecurity 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 by a botnet remediation working group, CSRIC concluded that consideration must be given to the technological, consumer, operational, financial and legal barriers that may limit the speed and scope of adoption of cyber-related solutions.[28]

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.[29]

Consumer/market barriers can also arise that may limit the ability of providers to implement some cybersecurity measures. For example, implementation of some solutions may be viewed by customers as ineffective (*e.g.*, customers choosing not to participate) or undesirable (*e.g.*, privacy, restrictive terms and conditions). These factors – collectively or individually – must be taken into consideration by the Departments as they develop and implement any Framework that may require material incremental investment in systems or human resources.

In addition to acknowledging these marketplace realities, the Departments should solicit use-cases or studies that show how these obstacles can be overcome. The Departments should also make such studies widely available to government and industry stakeholders so that they may inform the Framework Development process.

VII. The Framework Must Recognize That in Instances Where the Need to Invest Goes Beyond the Ability to Make the Business Case, Incentives are Necessary to Promote Adoption of Best Practices.

In some circumstances, the absence of business models that support cybersecurity related cost-recovery will mean that the Framework must include the development and availability of

[28] 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.
[29] *Id.*, p. 11.

viable incentives to promote the adoption of such measures. The Framework should include incentives that are designed to promote participation by stakeholders in cyber-security related efforts. These incentives should be considered an integral component of any public-private approach associated with implementing the Framework.

Through an effective incentives program, the federal government can help facilitate broader adoption of sound cybersecurity practices across *all* critical infrastructure and key resource sectors and within the federal government's own operations. The government should seek to encourage the broader adoption of cybersecurity practices that have already been demonstrated to be effective, while continuing to adapt existing best practices to keep pace with changing cybersecurity developments.

There are a number of positive incentives the federal government could consider to foster increased cybersecurity, including tax incentives to help improve cybersecurity, as well as direct funding and/or grants for cybersecurity research and development. In addition, the cybersecurity landscape could be evaluated in order to identify areas where existing regulatory regimes could be streamlined to alleviate any duplication and ambiguities. Similar measures have been raised in other venues, including leveraging the purchasing power of the Federal Government and reducing regulatory complexity.[30] Collectively, such incentives could bridge the gap between what private sector business plans can support for cybersecurity investment and what might be needed to achieve the additional cybersecurity enhancements desired by policymakers.

Government can and should encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad scale investment to critical infrastructure and key resources through carefully targeted incentives for industry stakeholders. This is the same

[30] Testimony of Larry Clinton, President Internet Security Alliance, House Subcommittee on Telecommunications and the Internet, May 1, 2009.

conclusion reached in The White House's cybersecurity report, which stated that "[t]he Federal government should consider options for incentivizing collective action and enhance competition in the development of cybersecurity solutions."[31] Possible incentives that the report identifies include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification and tax incentives. USTelecom believes that such measures will help foster an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted sound security practices.

VIII. The Framework Must Eliminate Wasteful and Redundant Duplicative Efforts.

The Framework must enshrine greater coordination of federal governmental cybersecurity efforts. The Departments should ensure that consideration will be given to "issues relating to harmonization of existing relevant standards and integration with existing frameworks."[32]

In particular, there is an urgent need for greater coordination at the federal level regarding the increasing number of federal agencies becoming involved with cybersecurity issues. USTelecom's members participate in numerous cybersecurity initiatives spread across multiple government agencies, where coordination is often lacking. For example, these companies are currently engaged in activities at the Department of Homeland Security (DHS), through participation in efforts involving the Communications Sector Coordinating Council (CSCC), and at the Federal Communications Commission (Commission), through the CSRIC.

As more agencies move into the cybersecurity realm, there is an increasing level of redundant efforts and clouded authority. For example, a search for the word "cybersecurity" on

[31] *Cyberspace Policy Review,* p. 28.

[32] *Notice,* p. 13025.

the federal government website "Regulations.gov," yields 150 proceedings for notices, proposed rules and rules since January 2010, from a broad range of agencies, including the DHS, the National Institutes of Health, the Tennessee Valley Authority and the United States Coast Guard.[33] A slight change to the spelling of cybersecurity – to "cyber security" – generates 369 separate proceedings.

This is not to say that these agencies should refrain from engaging in cybersecurity issues. Of course, the various agencies must be mindful that every proceeding that they conduct separate from other agencies will place demands on scarce resources from the private sector. This scarcity of resources requires the private sector to choose which proceedings to participate in, meaning that proceedings with limited or disparate participation could develop incomplete factual records. Such a result increases the possibility of reaching erroneous conclusions. Moreover, inasmuch as all of the separate agencies are not participating in, or attempting to track and reconcile the various outcomes of, these hundreds of proceedings, the coordination of federal government cybersecurity policymaking becomes impossible. For this reason, there needs to be a central authority to direct the nation's singular cybersecurity policy.

As one witness before the House Subcommittee on House Committee on Homeland Security, Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology, testified, "[t]he sheer number of extremely important issues that transcend agency boundaries suggests that the coordination of any national cybersecurity strategy must reside within the one

[33] Using the search tools available on the regulations.gov website, USTelecom conducted a search for documents issued by federal agencies that were: 1) Notices; 2) Proposed Rules; and 3) Rules. The search results identified documents issued in 421 separate proceedings from 45 different agencies during the referenced timeframe.

organization responsible for ensuring that the government acts as one government."[34] The Framework must address this current situation by eliminating such redundant and wasteful efforts.

IX. Conclusion

USTelecom encourages the Departments to adhere to the above referenced principles as it moves forward with the development of the Framework. By following these principles during the development process, the Departments will ensure that the Framework is optimized for addressing cyber-security-related risks across all sixteen critical infrastructure sectors.

Respectfully submitted,
UNITED STATES TELECOM ASSOCIATION

By: ______________________________
Kevin Rupy
Robert Mayer
David Cohen

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

April 8, 2013

[34] Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing, Securing America's Cyber Future: Simplify, Organize and Act, Before the House Committee on Homeland Security, Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology, Hearing on Reviewing the Federal Cybersecurity Mission, March 10, 2009.