Summary of
Testimony of Robert Mayer
Vice President, Industry and State Affairs
United States Telecom Association
"Cyber Threats and Security Solutions"

USTelecom represents innovative broadband companies ranging from some of the smallest rural telecoms in the nation to some of the largest companies in the U.S. economy. Its member companies and the entire communications sector stand on the front lines of cybersecurity, defending our country daily from cyber-attacks launched by state-sponsored and non-state actors. This requires our members literally to innovate every single day in order to meet the challenges posed by increasingly sophisticated adversaries.

The single most important step that can be taken to combat this worldwide scourge is giving our companies' security personnel access to real-time, actionable cyber threat information. USTelecom supported the Cyber Intelligence Sharing and Protection Act (CISPA) because it squarely addresses the dual challenges faced by broadband providers dealing with this issue: on one hand, the risks posed by cyber threats themselves, and, on the other hand, the uncertainties and potential legal costs and exposure associated with existing laws when applied to cyber-threat monitoring and response efforts utilized to protect our networks. While safeguards for privacy and civil liberties have been incorporated into CISPA together with other protections, the current legal framework concerning collection, use, and sharing of information is a major cybersecurity challenge facing our nation.

Executive Order 13636 and the accompanying Presidential Policy Directive 21 reaffirm the importance of public-private partnerships in assessing and combatting cyber threats. Our industry is hopeful and optimistic that the processes laid out there will turn out well and will lead to widespread acceptance and adoption. We have been working constructively to date with NIST, DHS, and the FCC. But ultimately the interpretation and implementation of sections 9 and 10 of the Order, and the accompanying PPD-21, may spell the difference between the success and failure of this effort.

Section 9 relates to the identification of critical infrastructure "at greatest risk." Risk designations that are either overly expansive or preemptively underinclusive may undermine many of the elements of a successful framework.

Section 10 of the Order requires federal agencies to review the preliminary framework and determine whether their own current cybersecurity regulatory requirements are sufficient. While the section contains language that would encourage agencies to reduce ineffective regulation, it arguably also serves as a hunting license to regulate, the very thing that would undermine the purported goal of the Order – a partnership with government to make its citizens safer.

Implemented prudently, the Executive Order and PPD-21 will be a triumph of government-private sector cooperation that will enhance our ability to respond to cyber threats. However, we must be on continuous guard against the kind of potential regulatory overreach that would slow our response to cyber-attacks or result in static "Maginot Line" type defenses that our opponents will easily bypass.

Testimony of
Robert Mayer
Vice President, Industry and State Affairs
United States Telecom Association
before the
House Committee on Energy and Commerce
"Cyber Threats and Security Solutions"
May 21, 2013

Chairman Upton, Ranking Member Waxman, Members of the Committee, thank you for giving me the opportunity to appear before you today to present the views of our industry on the cybersecurity threats facing our nation and the possible security solutions. It is both timely and appropriate that this committee, with its jurisdiction covering a range of sectors impacted by this burgeoning threat, take the time to review this issue.

My name is Robert Mayer, and I serve as Vice President of Industry and State Affairs at the United States Telecom Association (USTelecom). I am the past chair of the Communications Sector Coordinating Council (CSCC), one of the current 16 sectors under the Critical Infrastructure Partnership Advisory Council (CIPAC), through which the Department of Homeland Security (DHS) endeavors to facilitate coordination between federal infrastructure protection programs and the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments. Currently, I am the Chair of the CSCC's Cybersecurity Committee and serve as a senior member on the Cyber Unified Coordination Group under the National Cyber Incident Response Plan.

USTelecom represents innovative broadband companies ranging from some of the smallest rural telecoms in the nation to some of the largest companies in the U.S. economy. Our members offer a wide range of advanced broadband services, including voice, Internet access, video and

data on both a fixed and mobile basis. The customers that rely on our networks include consumers, businesses large and small, and government entities at the local, state, and federal levels. Protecting these networks and our customers from cybersecurity threats is our highest priority.

Our member companies – indeed, the entire communications sector, including wireless and cable broadband providers – stand on the front lines of cybersecurity, defending our country every day from cyber-attacks launched by state-sponsored and non-state actors. These attacks range from interruptions that constitute mere nuisances, which are easily interdicted and remediated, to potentially catastrophic events that threaten to cripple our economy and jeopardize our security. Our companies have taken significant steps to protect the integrity of our networks and the security and privacy of our customers. This requires us literally to innovate every single day in order to meet the challenges posed by increasingly sophisticated adversaries.

The Essential Keys – Information Sharing and Liability Protection

In response to the dramatic increase in cybersecurity threats, our industry has been working with Congress and the Administration over the past two years to enhance both the government's and the private sector's cybersecurity posture. The single most important step that can be taken to combat this scourge is giving our companies' security personnel access to real-time, actionable cyber threat information. To that end, USTelecom supported passage of H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), as well as its predecessor legislation in the 112th Congress, because the voluntary and real-time sharing of such threat information will provide both the private sector and the government with the essential tools they need, in a timely

and useful manner, to detect, deter, and respond to malicious cyber activity. We commend the authors of that legislation, Representative Mike Rogers (R-MI), a member of this committee and Chairman of the House Intelligence Committee, and the Intelligence Committee's Ranking Member, Representative Dutch Ruppersberger (D-MD), as well as all who voted for it.

CISPA is important because it is the first bipartisan legislation to pass either House of Congress that squarely addresses the dual challenges faced by broadband providers dealing with this issue today: on one hand, the risks posed by cyber threats themselves and, on the other hand, the uncertainties and potential legal costs and exposure associated with existing laws when applied to cyber-threat monitoring and response efforts that are utilized to protect our networks in a variety of circumstances. The current legal framework concerning the collection, use, and sharing of information remains a substantial barrier to effective communication between and among all relevant public and private stakeholders. Broadband providers believe this continuing legal uncertainty, and its effect in limiting the sharing and use of relevant information about cyber threats, stands as a major cybersecurity challenge facing our nation.

As we meet here today to discuss cyber threats and security solutions, we cannot emphasize enough that the most important role government can play in encouraging efforts to detect and deter cyber threats is to remove that uncertainty and to establish conclusively that cyber threat monitoring and the ability to deploy active defenses are not merely lawful but encouraged. While 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, the simple inability of private sector stakeholders to share information with each other or with appropriate

federal agencies, and to act quickly on that information, without fear of being sued, regulated, or held criminally liable must urgently be addressed.

We were heartened by the strong bipartisan support CISPA received in the House – a real recognition of the careful and thoughtful way in which Representatives Rogers and Ruppersberger worked tirelessly to balance the many important factors involved in developing an effective approach to this issue. Those factors include the critical need for increased real-time sharing of information, and particularly classified information, between government and private sector parties, the necessity of providing liability protections if sharing between and among government and private sector parties is truly to occur in real time and defensive actions are to be taken, ensuring that the appropriate agencies of government play appropriate roles in the process, and the importance of providing safeguards for protecting privacy and civil liberties.

The legislation's limitations on the use of shared information for cybersecurity purposes, the enhanced roles given to the civilian Department of Homeland Security and its Inspector General, and the assurance that companies cannot use shared information as a loophole for consumer marketing are just a few examples of the way in which CISPA's authors endeavored to strike an appropriate balance between our security and our liberty. But the most important principle enshrined in the bill is its recognition that neither private sector companies nor the federal government can or will share cyber threat information with each other in real time – *in other words, in time to avert the real threat at hand* – so long as they remain exposed to the potential threat of class actions, criminal prosecutions, administrative enforcement proceedings, regulatory rulemakings, or other similar legal liabilities. We look forward to continuing to work with the bill's authors and with the Senate to strengthen the bill and hope that, driven by the impressive

bipartisan majority that approved it in the House, it will form the basis for legislation the President will sign this year.

Cybersecurity Executive Order – The Broad Outlines

On February 12, 2013, the White House released its long-awaited Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," establishing a process for the adoption of cybersecurity standards under what it termed a voluntary and collaborative framework.* The Order aims to facilitate national cybersecurity policy goals by directing federal agencies to reduce duplicative and excessively burdensome cybersecurity requirements. We are pleased that the Order reaffirms the importance of public-private partnerships in assessing and combatting threats, a strategy we believe is highly effective.

The Order directs the federal government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that they may better defend against cyber threats. It mandates the rapid dissemination of such reports to private sector partners; expands the Enhanced Cybersecurity Services program to all critical infrastructure sectors; and expands and expedites the processing of security clearances to certain personnel employed by critical infrastructure owners and operators.

* The Executive Order was issued concurrently with a "Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience," also known as PPD-21, which sets forth the roles and responsibilities of federal departments and agencies in "advanc[ing] a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure." PPD-21 identifies the 16 critical infrastructure sectors mentioned above and the Sector-Specific Agency (SSA) "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of [each] sector." The Communications Sector is one such designated sector, and DHS is our sector's designated SSA. PPD-21 supersedes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003.

The Order also calls on the federal government to develop a voluntary cybersecurity framework within one year through a public review and comment process. The framework will include standards and procedures to address cyber risks and will be reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, and operational feedback from owners and operators of critical infrastructure.

A voluntary program will also be established to encourage adoption of the cybersecurity framework by owners and operators of critical infrastructure and any other interested entities, and the federal government will develop a set of incentives to promote adoption of the framework. Sector-specific agencies will report annually to the President on the extent to which owners and operators are participating.

Elements of a Successful Cybersecurity Framework

On April 3rd, the National Institute of Standards and Technology (NIST) convened a workshop to gather stakeholder input on how to develop the framework for improving critical infrastructure cybersecurity. The day-long event marked the official launch of the process described in the Executive Order, and USTelecom has offered detailed comments on both the development of the framework as well as on possible incentives to promote its adoption. Some core principles we provided NIST, as well as others on which only Congress has the power to act, include:

- Promote a true public-private partnership – The framework should promote the use of a true public-private partnership model. Such models have an established, successful history in the telecommunications sector and are ideally suited for the cybersecurity framework. 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.

- Encourage information sharing – The framework should incorporate the Executive Order guidance that directs the federal government to increase the timeliness and quality of information provided about cyber threat information. However, as mentioned earlier, the current legal framework concerning information sharing poses a substantial barrier to two-way communications, one that must be addressed by Congress.
- Preserve innovation – Broadband providers are literally innovating every day in order to combat increasingly sophisticated cyber-attacks. Government should ensure that the framework does not hinder the ability of private industry stakeholders to innovate in the marketplace – for instance, by imposing costly mandates coupled with a lack of viable incentives. 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.
- Develop flexible and non-prescriptive approaches – The framework won't succeed if it's based on a "one size fits all" approach. Because of the continuously evolving nature of cyber threats, industry must have the flexibility to respond quickly and efficiently. And given the importance of cybersecurity to maintaining a strong relationship with our customers, our

industry is continuously revising and updating existing cyber standards to ensure the highest levels of safety. Standards, norms, and best practices can help address current threats, but innovation is needed to guard against future unknown threats. We believe any effort to transform voluntary best practices derived in consensus-based venues into prescriptive mandates would have a serious chilling effect on future voluntary initiatives and partnerships with the federal government.

- All players share responsibility – Any framework must acknowledge the reality that protection of critical infrastructure is a shared responsibility that cuts across all elements of cyberspace and, indeed, the economy. Exclusion of one party or group will create vulnerabilities that could expose other stakeholders to potential threats. 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.
- Examine the business case for cybersecurity investments – When recommending practices, government should be mindful that some companies have business models that allow for cost-recovery of investments needed to shore up cybersecurity protection, while others do not. For the latter group, significant costs could limit the speed and scope of adoption. Therefore the framework should include effective incentives designed to promote participation. 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.
- Establish legal safe harbors for participation – Voluntary adoption of the cybersecurity framework by owners and operators of critical infrastructure and other interested entities will

occur fastest and most efficiently if companies are assured they can spend their limited resources on implementation rather than on lawyers to deal with compliance and litigation issues. The Administration, to the extent the law permits, and Congress, if necessary, should establish legal safe harbors that would encourage participation in the voluntary framework. One such safe harbor would be a strong liability protection regime analogous to that we've sought for information sharing. Another would be preemption of future state and local legislation and regulation. Given the inherent uncertainties surrounding future regulation at both the federal and state level, companies would clearly see in such safe harbors the benefits of adopting the framework. Moreover, such provisions would greatly assist the collaborative aspects of the framework by adding an increased element of trust and good faith between government and industry stakeholders, as well as the predictability of known business costs.

Implementation of the Order Will Determine Its Success

The implementation of the Executive Order is a complex undertaking, intended out of necessity to be carried out in a relatively short time frame. Given this situation, I want to express our industry's hope and optimism that the process laid out in the Order will turn out well and will lead to widespread acceptance and adoption not just by our sector but by all. To date, we have had an extraordinarily good working relationship with NIST, which historically and culturally has a long-standing reputation for working in strong partnership with the private sector to provide guidance on the path toward development of voluntary consensus standards.

We have also developed an effective working relationship with DHS, largely through the public-private partnership efforts of the CSCC and the Communications Information Sharing and Analysis Center (Comms ISAC). To date we have seen a good faith effort on the part of DHS to

implement the Executive Order using the public-private partnership model, which has succeeded in so many other areas of our cybersecurity work. We have had many hours of productive and constructive discussion with DHS on the issues in the Executive Order of greatest concern to us, and these discussions continue on virtually a daily basis. We are hopeful that those concerns will be reflected in DHS's final document, but the words we see on paper will be the real test of how the partnership process has worked.

In that regard, we do want to bring to the Committee's attention sections 9 and 10 of the Order, because the manner in which they are ultimately interpreted and implemented may spell the difference between the success and failure of this voluntary partnership effort.

Section 9 relates to the identification of critical infrastructure "at greatest risk." It is unclear at this juncture how encompassing it will be of our businesses and infrastructure. On one hand, overly expansive designations of critical infrastructure that lead to prescriptive solutions will undermine many of the elements of a successful framework by harming innovation and by leading to predictability and stagnation, outcomes that only make it easier for cyber adversaries to achieve their nefarious objectives. On the other hand, section 9 may preemptively exempt a major portion of the Internet ecosystem from possible inclusion as critical infrastructure. Given the interconnected nature of the Internet, the effectiveness of any cybersecurity strategy is inherently undermined when a major portion of the ecosystem is exempt from consideration even from the very start of the process.

Section 10 of the Order requires federal agencies to review the preliminary cybersecurity framework and determine whether their own current cybersecurity regulatory requirements are

sufficient. Agencies are then directed to propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk. Section 10 also requires that agencies consult with owners and operators of critical infrastructure, and report on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements and make recommendations to minimize or eliminate such requirements. While we are gratified the section contains language that would encourage agencies to reduce ineffective regulation, it arguably serves as a hunting license for departments to regulate, the very thing that would undermine the purported goal of the Order – a partnership with government to make its citizens safer. Indeed, these agencies are explicitly "encouraged" to go on such a hunting trip.

While section 10 does not apply to independent regulatory agencies, the accompanying PPD-21 singles out by name the one such agency most closely associated with our industry – the Federal Communications Commission - and directs that the FCC "to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."

We appreciate and value the contributions the FCC makes to the area of public safety and emergency communications, including the work of its Communications Security, Reliability and Interoperability Council (CSRIC), in which we are active participants. In the rapidly changing environment that cybersecurity presents, regulatory proceedings are incompatible with addressing new threats that can emerge and evolve at lightning speed. That is what has made the voluntary and consensus-driven approach of venues like CSRIC productive and worthwhile.

In closing, let me again thank the Committee for holding this timely hearing. Implemented prudently, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," will be a triumph of government-private sector cooperation that will enhance our ability to respond to cyber threats in rapid and innovative ways. As it is implemented, however, we must be on continuous guard against the kind of potential regulatory overreach that would slow any response to cyber attacks or build static "Maginot Line"-type defenses that our opponents will easily bypass.