Statement of Christopher Boyer
Assistant Vice President Global Public Policy
AT&T Services Inc.
before the
Presidential Commission on Enhancing Cybersecurity
July 14, 2016

Chairman Donilon, Vice Chair Palmisano and distinguished members of the Commission, thank you for providing the Communications Sector and me personally an opportunity to appear before you today to provide our thoughts on enhancing cybersecurity as we move into the next Administration and beyond.

My name is Christopher Boyer and I serve as Assistant Vice President of Global Public Policy for AT&T Services Inc. In that capacity I also serve on the Executive Committee and am the former Vice Chair of the Communications Sector Coordinating Council (CSCC), which represents the Broadcasting, Cable, Satellite, Wireless and Wireline segments under the Department of Homeland Security (DHS) Critical Infrastructure Partnership Advisory Council (CIPAC). The CSCC facilitates physical and cybersecurity coordination and planning activities among the private sector and federal, state, local and territorial and tribal governments.

I also serve as the Chairman of the National Institute of Standards and Technology (NIST) Internet Security and Privacy Advisory Board (ISPAB), a Federal advisory committee responsible for identifying emerging managerial, technical, administrative, and physical safeguard issues related to information security and privacy for Federal agencies. I am also AT&T's Point of Contact (POC) representing AT&T's executive member of the National Security Telecommunications Advisory Council (NSTAC), a Federal advisory committee tasked with providing advice to the President on matters of National Security and Emergency Preparedness (NS/EP). These roles provide me with unique insight into the sector's cybersecurity priorities and concerns, as well as to cross-sector concerns.

I would like to start by providing some background on the extensive partnership that exists between the Communications Sector and the Federal government to address cybersecurity and other matters of national security. The Communications Sector has a long history of cooperation within its membership and with Federal government with respect to national security and emergency preparedness. Our legacy dates back to the 1963 with the creation of the National Communications System (NCS), which President Kennedy established following the Cuban Missile Crisis to develop critical programs and plans to protect the nation's communications infrastructure.

In our view, this lengthy history distinguishes the Communications Sector from most other critical sectors. The strong bond between the sector and the federal government continues largely because of three organizations that have been created in response to earlier threats to the nation's critical infrastructure. Collectively, these organizations, in concert with DHS, which serves as the Sector Specific Agency for the Communications Sector, provide the *policy, planning and operations* framework necessary to address the nation's communications priorities.

- **Policy - National Security Telecommunications Advisory Committee (NSTAC).** The NSTAC (wwwncs.gov/nstac/nstachtml) was created in 1982 by Executive Order 12382. NSTAC is comprised of up to 30 chief executives from major telecommunications companies, network service providers, information technology, defense contractors and aerospace companies. Through a deliberative process, NSTAC's members provide the President with recommendations intended to assure vital telecommunications links through any event or crisis and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture. Key areas of NSTAC's focus include: strengthening national security; enhancing cyber security; maintaining the global communications infrastructure; assuring communications for disaster response; and addressing critical infrastructure interdependencies. Recent reports to the President have addressed Information and Communications Technology (ICT) Mobilization in response to a large scale cyber-attack, the use of Big Data Analytics (BDA) in emergency response, including for a cybersecurity incident, and recommendations on how to help better secure the Internet of Things. Each of these reports may be useful to the Commission as they consider some of these topics in relation to cybersecurity.

- **Planning - Communications Sector Coordinating Council (C-SCC).** The C-SCC (www.commscc.org) was chartered in 2005 to help coordinate initiatives to improve the physical and cyber security of sector assets; to ease the flow of information within the sector, across sectors and with designated Federal agencies; and to address issues related to response and recovery following an incident or event. The 40 members of the C-SCC broadly represent the sector and include cable, commercial and public broadcasters, information service providers, satellite, undersea cable, utility telecom providers, service integrators, equipment vendors, and wireless and wireline owners and operators and their respective trade associations. The C-SCC and IT Sector Coordinating Councils maintain close coordination on a range of policy and operational initiatives.

- **Operations - National Coordinating Center for Telecommunications (NCC) Communications Information Sharing and Analysis Center (C-ISAC)**. In 1982, federal government and telecommunications industry officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 created the NCC. This organization's unique industry - government partnership advances collaboration on operational issues on a 24 X 7 basis and coordinates NS/EP responses in times of crisis. Since 2000, the NCC's Communications Information Sharing and Analysis Center (C-ISAC), comprised of 51 industry member companies, has facilitated the exchange of information among government and industry participants regarding vulnerabilities, threats, intrusions and anomalies affecting the telecommunications infrastructure. Weekly meetings of industry and government members are held to share threat and incident information. During emergencies, daily or more frequent meetings are held with industry and government members involved with the response effort.

Members of the communications industry also participate voluntarily in a variety of other initiatives, including, but not limited to, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), the National Security Information Exchange (NSIE), industry leg security organizations such as the Messaging Anti-Abuse Working Group (M3AAWG) and a variety of other fora that share the goal of enhancing cybersecurity. Indeed, the Communications Sector is a staunch supporter of the voluntary, public-private partnership embodied by these and other organizations.

Even as we engage in these cooperative efforts, however, a principal area of concern for the sector is that we continue to see an increasing interest among certain agencies in the Federal government on prescriptive regulatory responses to cybersecurity threats. In our view, such efforts are misplaced, and in fact counterproductive. Given the constantly evolving nature of the threat, cybersecurity does not lend itself to a checklist or mandated solution. Protecting against cyber threats is a risk management function, and there is no one size fits all solution for all companies. To the contrary, a prescriptive regulatory “solution” would simply set a lowest common denominator bar that would create a disincentive for the innovation and agility needed to respond to an environment that is characterized by nimble and sophisticated hostile actors and constantly-evolving threats.

That dynamic is one reason the NIST Cybersecurity Framework has been successful as a mechanism for responding to that environment. It recognizes the diversity of companies and the need for flexible and evolving solutions, and allows companies large and small to tailor the Framework to their specific business needs commensurate to their risk posture. Many members of Congress, the Administration and other portions of government have also recognized this model as appropriate to address cybersecurity. In fact, the U.S. government is promoting the voluntary, risk management approach espoused by the Framework internationally as an effective model to ward of more regulatory oriented regimes that may arise around the world due to fear of cyber-attacks.

Notwithstanding this consensus in support of the Framework, and its clear record of success, some continue to advocate for imposing cybersecurity solutions upon industry. This would be a mistake. As I noted, these actions would not only prove to be ineffective in addressing cybersecurity but run the risk of making us less secure by directing critical, limited resources towards issues prioritized by regulators as opposed to allowing companies, who best know their business and information systems, to appropriately respond to the risks they are seeing every day. These actions also undermine the existing public-private partnership model. While we recognize the important role of government, and believe that government assistance is vital to our mission, a regulatory approach will undermine that partnership. Our first and foremost recommendation to the Commission would be to explicitly reject a prescriptive regulatory approach and reinforce that government and industry should continue to work cooperatively, building upon the many different voluntary mechanisms that are already in place today. Examples of this are both the Communications sector’s continued work with DHS and the recommendations offered by the Communications sector in FCC CSRIC Working Group #4 from 2015.

With that, I would like to address some specific areas that we were asked to cover in our opening statement. We were asked to speak to three specific areas and then provide recommendations to the Commission. Those areas are: first, the biggest challenges we are seeing to critical infrastructure; second, current approaches that we believe are effective; and third, promising research and innovation that may address those challenges. The following are some high level thoughts in each of those areas followed by a set of recommendations for the Commissions consideration.

Biggest challenges in critical infrastructure today and over the upcoming ten years.

- *Complexity*. As the saying goes, complexity is the enemy of security. While previous concepts like Defense in Depth and perimeter defense continue to have merit, the rapid increase in the number of devices and access points make it more difficult to rely upon a perimeter defense model. The attack surface is growing exponentially, and defending against ever-more sophisticated attackers, including nation states, has created an extremely complex environment that makes it difficult to rely upon a perimeter defense model. We believe that companies should operate under the assumption of not "if", but "when", they will be impacted by a cyber-attack. For this reason, the response to an attack, rather than simply prevention, has become a much more critical component of cybersecurity. Further, as discussed above, as increasing layers of virtual and physical networks are leveraged to provide critical services, such as the Internet of Things, simple regulated solutions are insufficient and could actually prove counter-productive. The complexity of the environment supports the continued evolution of the public private partnership model.

- *Increasingly sophisticated adversaries*. While cyber incidents, to the best of our knowledge, continue to leverage predominantly known vulnerabilities, Nation states and other entities are becoming increasingly more sophisticated in their approaches and attack vectors.

- *Convergence*. With the transition to IP-based and software defined networks (SDN) and Network Function Virtualization (NFV) the communications critical infrastructure will become increasingly reliant on critical assets outside its domain. Examples include operating systems, supply chain vendors, and an increasing dependence upon IT.

- *Need for better computing/network architectures*. For large enterprises, the combination of a highly distributed networks and sophisticated, nation-state and criminal actors, makes it very difficult to prevent attacks. Thus, as I noted earlier, a focus on Response and minimizing the damage from an attack have become increasingly more important. As such, we need to move towards newer computing/network architectures that enable a more flexible, adaptive response, leveraging new tools such as virtualization and the cloud.

- *International Governance*. Many cyber threats originate overseas. The complexity of international collaboration, given a wide variety of legal, policy and cultural landscapes, and lack of a coherent strategy gives rise to concerns about confronting the cyber threat on a global scale.

- *Protecting Against Regulatory Mission Creep.* We have been encouraged by the recognition among most Federal policy-makers that the best way to bolster our nation's overall cyber defense is through reliance upon voluntary mechanisms rather than compulsory standards or obligations. The inherently backward-looking nature of regulation is ill-suited for the challenges of cybersecurity. Our cyber adversaries are highly sophisticated and adaptive, and it is essential that industry be afforded the necessary flexibility and agility to respond to a constantly-changing threat landscape and to continuous innovation by cyber criminals. Both the NIST Framework and the codification of the NIST process via enactment of the Cybersecurity Enhancement Act of 2014 reflect and advance the clear Federal policy preference for reliance upon voluntary mechanisms and industry-driven initiatives to combat cybersecurity threat. We are concerned, however, that some agencies are retreating from the core policy principle that network security is best achieved through voluntary measures rather than through compulsory rules. In addition, there are instances in which agencies appear unaware of the manner in which their regulatory initiatives may conflict with, or adversely effect, salutary cyber-related activities supported by Congress and the Administration, such as cyber threat information sharing. We are also concerned that multiple agencies, at multiple levels of government, are becoming more involved in forging cybersecurity policy proposals. The end result is that critical infrastructure owners increasingly face duplicative and conflicting regulatory obligations that impose significant costs and burdens while doing little to materially enhance cybersecurity. Government must partner with industry to ensure that companies establish and maintain an active and agile cyber defense posture, but it must also recognize the limits of prescriptive mandates in this area and guard against regulatory overreach and the imposition of redundant or conflicting rules.

Current approaches that are proving effective in addressing those challenges.

- *NIST Cybersecurity Framework.* The Communications Sector supports the NIST Cybersecurity Framework. The Framework allows for a flexible, risk management model and non-regulatory approach to cyber similar to what I discussed above and is of particular value to enterprise-risk management. We were involved in the Framework from its inception, including participating throughout its development, and have taken efforts to promote it within our sector. Communications Sector executives have appeared at a variety of events, including with one of our major CEOs appearing at the release of the Framework. The Communications Sector has also worked extensively to adapt the Framework to our sector. One highlight of those efforts was our participation in FCC CSRIC Working Group #4 last year, which involved over 100 representatives from across the industry and culminated in the release of an over 400 page report including use cases, among other materials, for how the Framework could be applied across the each of the 5 key portions of the sector.

- *Public private partnership model.* As noted previously, mandates will not only fail to help address the situation, they will substantially hinder efforts given the evolving nature of the threat. As I described in detail earlier in my remarks, the Communications Sector has a long history of working cooperatively and productively with the Federal government, and continues to support that voluntary partnership model. We believe the Commission should make it a point to reinforce that approach in its recommendations to the next Administration.

- *Information sharing legislation*. The Communications Sector also applauds Congress on the passing of vital cybersecurity legislation last December. The Cybersecurity Act of 2015 included the Cybersecurity Information Sharing Act of 2015, which contains important provisions regarding network monitoring, defensive measures, and information sharing. One of the principal challenges that we faced in information sharing was the continued legal uncertainty around cybersecurity itself and information sharing more specifically. In the past there were a myriad of statutes to review prior to electing to share information, which only served to delay the process and prevent the real time sharing of threat intelligence. The recent legislation is intended to clarify the legal framework around information sharing and the Communications Sector is continuing to evaluate and implement the authorities provided within the legislation. We have formed a CSRIC working group to address information sharing, the CSCC has also formed a strategic information sharing committee, which I currently chair, and we have had DHS and the Department of Justice conduct multiple briefings to both the CSCC and sector attorneys to determine how to proceed. Much of that work is still evolving. Through the combined efforts of DHS and the Department of Justice, in particular the guidance recently issued to implement the legislation, the continued development of the DHS Automated Indicator Sharing (AIS) Portal, and continued efforts within the industry, progress is being made.

Promising research and innovation that may address those challenges in the future

- *More Resilient Computing Architectures (SDN/NFV/Virtualization).* One area that many sector members are focused on is moving towards more distributed architectures where data and security is virtualized in the cloud. This concept allows for security to shift from being a physical appliance to having a security "wrapper" around each instance of various data sets. If there is an attack, the new architecture would make it possible to shift resources around, quarantine data, or limit an attacker's access to resources outside of a specific data set. Thus helping to limit the impact. In effect, the architecture takes a page out of the attacker's playbook to distribute the architecture and enable a more flexible, nimble and resilient response capability.

- *Big Data Analytics (BDA) for security*. NSTAC recently completed a report discussing the use of big data analytics for National Security and Emergency Preparedness. BDA provides potential capabilities to enhance detect and protect functions under the NIST Cybersecurity Framework and response. We recommend the Commission review the BDA recommendations, which describe how government can leverage BDA for these purposes including cybersecurity.

- *Secure Software Development/Software Assurance.* NIST is currently researching tools to better assess or assure secure software development. As networks become more dependent upon software, determining how to promote the use and development of these tools for software developers is becoming increasingly more important.

- *Strong Authentication*. There are also a variety of tools being developed to enhance authentication. The Administration has started discussing this as part of a proposed campaign on the use of 2-factor authentication. Determining how government can better promote stronger authentication in a non-regulatory manner could also benefit security.

Recommendations to propose to the Commission.

- *National Incident Response Plan*. The U.S. government needs to finalize a formal incident response plan that outlines how government will organize itself and work with industry in the event of a large scale cyber disruption. This was a key finding of the recent Cyber Storm exercise conducted this past March. While we understand that the Administration is currently engaged in this activity, it is critical that we have a plan in place before we encounter a large scale attack that may impact critical infrastructure.

- *Eliminate Duplication*. There are currently a wide variety of government initiatives that span a range of agencies. This makes the current process for industry engagement highly inefficient. Also the continued engagement by regulatory agencies undermines the public private partnership process preferred by many in both government and the private sector. More clarity about how government will interface with industry and highlighting that prescriptive regulation will not be effective, and could in fact be a detriment, to better security would both be helpful to enhancing the partnership model with industry. The Commission could partially accomplish this by reaffirming that the sector specific agencies, as designated by the President, are the appropriate interface with industry.

- *International*. Many cyber threats emerge from overseas, increasing the importance of collaboration among international partners. There remains a need for a more concrete strategy for how to address international collaboration and response, and the effective development of global norms.

- *Domestic preparedness*. Beyond the Federal Government there remain concerns around the level of preparedness among other government entities, and in particular at the state and local level. One possible solution to this challenge is to provide incentives/grants to States to assess their risk, and to take measures to ensure the continuity, both physical and cyber, of the essential services they provide to Citizens within their State. The NASCIO Cyber Disruption Planning Guide and efforts by the National Governor's Association should be supported.

- *NIST Framework*. Continue the focus on the NIST Framework. But instead of expending time and resources drafting "Version 2.0"of the Framework, efforts should be directed to the potential application of the existing Framework in other areas as the attack surface continues to evolve. For example, stakeholders should leverage the Framework to develop use cases for security in the IoT domain. The Department of Commerce, NIST and NTIA can play an important role in bringing together disparate industries with a role in the IoT ecosystem to address these concerns.

- *Encourage new technology/resilient network architectures*. Develop/support strategies for how new technology can be leveraged to improve security. Given the increasing complexities of the cyber environment that is we also need to move forward on strategies for how to evolve computing architectures to be more inherently secure. This can include government leveraging its procurement capabilities in adopting new technologies to spur the market, or other initiatives such as the NIST Cybersecurity Center of Excellence (NCCoE).

In closing, let me once again thank this Commission for their ongoing and important work. We appreciate the opportunity to offer our thoughts on this matter and continue to believe that by working together we can help make the world a safer place.