Before the Department of Commerce
Washington, D.C.

In the Matter of Developing a Framework to Improve Critical Infrastructure Cybersecurity	)))))	**Docket No. 130208119-3119-01**

AT&T COMMENTS

AT&T Inc. ("AT&T") submits these comments in response to the Request for Information to gather initial information needed to develop the Baseline Framework to Reduce Risk to Critical Infrastructure mandated by the recent Cybersecurity Executive Order.[1] In these comments, AT&T suggests foundational principles to guide NIST in its work, addresses the RFI in connection with the identification of cybersecurity standards and standards gaps generally, and provides specific examples of the standards and practices it has developed to manage cyber risk.

INTRODUCTION

Under Section 7 of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[2] the Director of the National Institute of Standards and Technology (NIST) is tasked with coordinating the development of a Baseline Framework to Reduce Cyber Risk to Critical Infrastructure (the "Framework"). The EO requires that the Framework include "a set of standards, methodologies, procedures, and processes that align policy, business, and

[1] Notice; Request for Information, *Developing a Framework to Improve Critical Infrastructure Cybersecurity,* 78 Fed. Reg. 13024 (2013) ("RFI")

[2] Exec. Order No. 13,636, 78 Fed. Reg. 11739 (2013)

technological approaches to address cyber risks" and it must "incorporate existing consensus-based standards and industry best practices to the fullest extent possible."[3] The Framework must further be consistent with international standards "whenever feasible."[4] It must provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to enable Critical Infrastructure ("CI") owners and operators to "identify, assess and manage cyber risk."[5] The EO places a particular emphasis on "cross-sector security standards and guidelines" applicable to CI and tasks NIST with identifying, within the Framework, "potential gaps that should be addressed through collaboration with particular sectors and industry-led standards organizations."[6] The Framework must include guidance for "measuring the performance of an entity in implementing" the Framework.[7]

THE EO AND THE FRAMEWORK: GUIDING PRINCIPLES

The EO directs NIST to undertake an enormous effort in a very short time. NIST must use that time to focus on developing a Framework that will advance the rapid and widespread adoption of cybersecurity by encouraging technology innovation in the current and future economic and investment climate. Unless it is developed in way that truly "aligns policy, business, and technological approaches to address cyber risks,[8] the Framework, with its ultimate collection of standards, methodologies, procedures and processes, risks becoming a bureaucratic

[3] EO, 78 Fed. Reg. at 11741

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] EO at 11741; RFI at 13024.

impediment to making real improvements in cybersecurity, rather than a flexible and effective tool for collaboration. Put another way, the Framework cannot be our Nation's primary and best defense against the evolving and expanding cyber threat. Rather, inter- and intra-sector cybersecurity innovation in the context of fluid, flexible and trusted private-public partnerships are necessary to eliminate vulnerabilities and defeat malicious actors. The Framework must enable, not inhibit, such innovation, and it must not overburden existing public private cybersecurity partnerships. To that end, it must embrace the principles of efficiency, prioritization, inclusiveness, and innovation.

First Principle: Efficiency

The cybersecurity policy arena is already crowded with procedure, relationships, and standards. The Framework must build upon existing cybersecurity public private partnerships while avoiding duplication of work efforts and the proliferation of standards. Federal law and policy have already established roles and responsibilities for federal agencies working with the private sector and other entities in enhancing the cyber and physical security of critical public and private infrastructures.[9] The Homeland Security Act of 2002 assigned the newly created Department of Homeland Security ("DHS") responsibility for developing a comprehensive national plan for securing key domestic resources and CI and assisting in the development and promotion of private sector CI best practices.[10] DHS's National Infrastructure Protection Plan (NIPP) describes a partnership model as the primary means of coordinating government and

---

[9] GAO-12-92, *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can be done to Promote its Use*, (December 2011) at 5.

[10] *Id.*

private sector efforts to protect CI.[11] Under the NIPP, sector-specific agencies are required to work with their private sector counterparts to understand and mitigate cyber risk.[12]

Trusted partnerships between the public and private sectors are essential for effective national cybersecurity. The private sector needs the best government intelligence, context, advice, warnings and insights to be made available to technology developers, cybersecurity practitioners, and critical infrastructure owners and operators. The communications sector also proactively engages in and leads a wide variety of private sector lead standards in addition to its government partnerships[13]. Within the Communications CI Sector, AT&T has a long history of working in the context of established public private partnerships, both before and after the establishment of the NIPP.[14] The Framework should build upon existing relationships like these and facilitate their evolution into truly flexible and fluid alliances that leverage the technology innovation needed to combat emerging threats.

---

[11] *Id.*

[12] *Id.*

[13] The GAO listed 76 different documents that had been published providing cybersecurity guidance for the Communications Sector. This includes guidance from groups such as the CSRIC and IETF but also from non-governmental organizations such as the Alliance for Telecommunications Industry Standards (ATIS), International Organization for Standardization (ISO), the Cloud Security Alliance (CSA), the GSM Association (GSMA), and the 3rd Generation Partnership Project (3GPP). AT&T also participates in a variety of other industry groups focusing on security such as the Messaging Anti-Abuse Working Group (MAAWG) among others. GAO, *Critical Infrastructure Protection, infra, n.9*, passim.

[14] AT&T participates in or coordinates with many partnerships with government entities, both domestically and internationally, including the National Security Telecommunications Advisory Committee (NSTAC), U.S. Secret Service Cyber Crimes Task Force; Federal Bureau of Investigation's InfraGard©; Network Reliability and Interoperability Council (NRIC); Computer Emergency Response Team/Coordination Center (CERT/CC); Communications Security Reliability and Interoperability Council (CSRIC); Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C); Forum of Incident Response and Security Teams (FIRST); Communications – Information Sharing and Analysis Center (Communications-ISAC);

NIST should recognize that there are cybersecurity work efforts spearheaded by various government agencies. Three years ago Melissa Hathaway, former Acting Senior Director for Cybersecurity at the National Security Council, noted at the time that there "a recent cursory review identified more than 55 government initiative public-private partnerships in the area of cybersecurity".[15] Since then the number of partnerships has grown. Industry stakeholders are constantly challenged by having to support parallel government efforts, especially in the area of cybersecurity standards and best practices. Duplication is inefficient, costly, and distracts from the private sector's main cybersecurity mission. The EO establishes a number of specific work efforts that should be given priority over parallel or related government efforts that could result in inconsistent outcomes or needlessly squander private sector resources.

As an example, the Communications CI sector participates in the Federal Communications Commission's CSRIC, which includes working groups addressing issues related to cybersecurity. The last CSRIC III focused on Border Gateway Protocol security, Domain Name System Security Extension, botnets and a set of potential security controls for communications. As a practical matter, it will be difficult for the private sector to support parallel standards process at both the FCC and the NIST. The FCC should participate in the NIST and DHS public private partnership process through the Government Coordinating Council (GCC), and in this way provide any input it deems material into the Framework. At the same time, the agency should be encouraged to suspend cybersecurity activity at CSRIC pending the

---

ATIS-Network Reliability Steering Committee (NRSC); and the National Cybersecurity Alliance.

[15] FCC, *Cyber Security Certification Program*, Comments of AT&T Inc., PS Docket No. 10-93 (July 12, 2010) ("AT&T FCC Certification Program Comments") at 11.

outcomes of the EO-initiated processes that are the Administration's and private sector's first priority.

The Framework, of course, is ultimately concerned with identifying appropriate standards and best practices. There are many security standards already developed and a wide variety of organizations focusing on security around the world.[16] NIST should leverage existing standards and practices. Because it simply has no time to develop new security standards, practices or norms, in the compressed timetable allotted by the EO, the best outcome would be to leverage those standards that have already been developed.

Second Principle: Priority

The Executive Order recognizes that the framework should provide a "*prioritized*, flexible, repeatable, performance-based and cost-effective approach to help owners and operators or critical infrastructure identify, assess and manage cyber risk." An operating principle throughout the NIST framework process should be to prioritize the most critical principles or standards. If NIST attempts to protect everything or the framework becomes excessively broad it may distract attention away from the most critical areas and effectively limit security or create false sense of security that in the end does more harm than good.

Third Principle: Ecosystem-Wide Consultation

Consistent with Section 6 of the EO, the Framework should be developed in a consultative process largely led by industry with NIST playing both a consultative and a convening role to aid industry in identifying those practices that may enable them to best attain measurable performance pursuant to the Framework's ultimate guidance. Because cybersecurity is a shared responsibility in an interconnected world, the Framework should include all

[16] GAO, *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but more can be done to promote its Use*, (December 2012) *passim.*

ecosystem stakeholders in its consultative process. A broad ecosystem approach, which includes various types of service providers, equipment manufacturers, software developers and end-user customers, is essential to developing effective cybersecurity strategies and responses that can be adopted across sectors through the existing sector coordination process and implemented in specific sectors through the existing Sector Specific Agencies (SSA) and Sector Coordinating Councils (SCC). Finally, the ecosystem is clearly international in scope. NIST should therefore focus on widely accepted international standards, and at all times seek to harmonize its activity with global standards work.[17]

Fourth Principle: Innovation over Regulation

Ultimately, the Framework must reflect the dynamic nature of the cyber threats. Innovation and flexibility are the greatest weapons against varied, nefarious and adaptive cyber threats.[18] NIST should therefore eschew a "checklist" approach and rather preserve private sector flexibility to act proactively and respond quickly. Prescriptive regulation or other requirements could slow response times, exacerbate cyber incidents, and discourage innovative and evolving solutions to new and evolving threats. The objective of this Framework proceeding should be to establish a simple baseline of security leaving flexibility for owners and operators of critical infrastructure to innovate beyond those basic controls as threats evolve and circumstances warrant. CI owners should be provided with a set of flexible and adaptable

[17] EO at 11741. At the World Conference on International Telecommunications U.S. Government policy favored continuing the existing multi-stakeholder process for Internet governance and issues such as cybersecurity, as opposed to more regulatory, top down models proposed by some countries. In order to support a consistent U.S. policy and reinforce a good model for addressing these issues, any Internet-facing standards process at NIST should remain flexible and market driven.

[18] AT&T FCC Certification Program Comments at 7.

principles to both measure and mitigate risk in a cost effective manner, consistent with their operational and business models.

When government policies incent the private sector to prioritize compliance with standards, checklists and the like over the development of innovative ways to address cyber threats, there is a real risk that the nation's cybersecurity defenses will be sub-optimal. Within the Communications CI Sector, compliance with fixed standards would limit the flexibility of communications service providers to manage their networks effectively in response to changing cyber threats and would also deter innovation.[19] Fixed standards and checklists could expose private sector vulnerabilities, providing malicious actors a roadmap to infrastructure penetration.[20] For these reasons, the Framework must operate to encourage, not stifle, innovation.

IDENTIFYING EXISTING STANDARDS AND GAPS

NIST has initially scoped the Framework development process in three parts: (1) identify existing cybersecurity standards, guidelines, frameworks and best practices that enhance the security of CI sectors and other interested entities; (2 specify high-priority gaps for which new or revised standards are needed, and (3) collaboratively develop action plans by which these gaps can be addressed. In this proceeding, NIST should be focused on establishing a Framework that encourages technology innovation through the establishment of baseline principles that CI owners and operators may choose to adopt consistent with their business practices in a way that can improve their cybersecurity posture. In the limited time available to it, NIST cannot afford

[19] AT&T FCC Certification Program Comments at iii.

[20] *Id.*

to be overly inclusive or expansive beyond consensus requirements designed to address a range of common vulnerabilities.

A wide variety of existing standards address security issues, including the ISO/IEC 27001:2005 Information Security Management Standard, SSAE 16/ISAE 3402/SOC1 (formerly SAS 70), SOC 3 (formerly SysTrust), Payment Card Industry (PCI) Data Security Standard (DSS) and similar certifications or audits. Further, an array of security standards have been developed at organizations such as ITEF, ATIS, 3rd Generation Partnership Project (3GPP), GSMA, NIST, and NRIC/CSRIC.[21] Approaches such as the ISO 27001:27005 standards address a systematic way for organizations, independent of their specific lines of business, to examine their information security risks, take account of threats and vulnerabilities; design security controls and risk management processes to address those risks; and adopt management process to ensure that the information security program continues to meet the organizations needs on an ongoing basis. Other approaches, such as PCI standards or the requirements of Federal Information Security Management Act (FISMA) or Health Insurance Portability and Accountability Act (HIPAA), apply more specifically to particular product lines, businesses, or data sets, and are therefore less cross-sectoral. Many of the communications-specific standards

[21] AT&T participates in all of these processes, as well as others. *See supra*, n.13, for a non-exclusive listing of efforts in which it participates. The NRIC, the Network Reliability and Interoperability Council, was the predecessor to the CSRIC at the FCC. There were multiple iterations of the NRIC from 2002-2005. NRIC VI in 2002-2003 published a series of recommendations on cybersecurity best practices and NRIC VII in 2004 conducted a focus group that identified 173 cybersecurity practices. CSRIC II in 2010 refreshed the NRIC best practices identifying 397 total cybersecurity practices. Finally, the short list in the text above is not intended to be all inclusive; s*ee* GAO, *Critical Infrastructure Protection: infra, n.9,* for further identification of standards by CI sector.

bodies such as 3GPP, GSMA, CSRIC and NRIC are specific to network security. Finally NIST itself has issued a series of publications (800-series publications) cataloging security standards for government agencies - including NIST 800-53.

After identifying the many existing security standards, NIST should be careful not to assume that it is appropriate to adopt them all uncritically as part of the Framework. For example, many of the CSRIC practices were developed as part of a process that did not incorporate the requirements and rigor of the National Institute of Standards and Technology Act, the National Technology Transfer and Advancement Act of 1995 or OMB Circular A-119, all of which are required by the EO to be followed in the development of the Framework.[22]

Another fundamental challenge to establishing cross-sector standards and practices is that that different organizations and sectors, and individual companies within those sectors, operate differently and have varying capabilities to respond to cyber threats, with the oft-observed truism that there is no one size fits all approach to cybersecurity. Thus the Framework should take into account the varying capabilities of CI owners and operators of as well as the practicality and the cost effectiveness of the measures proposed. Individual CI owners and operators have the best visibility and knowledge of their infrastructure and how to best manage cyber risks to their business. It will therefore be necessary for NIST to approach the development of best practices in a way that accounts for these differences and doesn't focus on specific standards or technologies. AT&T recommends that NIST focus on a broad set of principles that each sector, through the sector coordinating councils, can then apply to their unique situation on a voluntary basis to fulfill vulnerability and threat mitigation goals developed by CI owners and operators, rather than focusing on specific technology standards.

AT&T's APPROACH TO SECURITY STANDARDS AND PRACTICES

[22] EO at 11741.

It is AT&T's general corporate policy and practice to protect its information resources from unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer, or destruction, and to implement protective measures commensurate with their sensitivity, value, and criticality.[23] AT&T's information resources include any owned or managed systems, applications, and network elements, and the information stored, transmitted, or processed with these resources. AT&T develops and issues specific internal standards and other reference materials in support of this policy (the "AT&T Security Policy and Requirements" or "ASPR"). This includes policies addressing AT&T's workforce; its technology, vendor, contractor and supplier contracts; and overall compliance, as well as related risk-assessment practices. Given the dynamic environment that AT&T supports, the ASPR are continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, operating procedures, tools and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout the corporation.

AT&T considers internal reviews of operations and applications functions for compliance with security requirements essential to evaluating the adherence to the established security procedures worldwide. Business and operations units are encouraged to perform self-reviews to verify compliance with published security requirements. AT&T's internal review of business unit and operational compliance with security requirements consists of a comprehensive review of an organization's adherence to regulatory guidelines and internal policies, controls, and

[23] In order to assist business users in understanding AT&T's comprehensive approach to security and to maximize the benefits of the various security solutions available to them, AT&T provides the AT&T Information & Network Security Customer Reference Guide, which contains an extensive description of AT&T's cybersecurity practices (Attachment A).

procedures, as applicable. AT&T security auditors and assessors evaluate the strength and thoroughness of compliance. Assessors review security policies, user access controls and risk management procedures over the course of a compliance engagement and report the findings to all key stakeholders. AT&T deals with a carefully selected and limited number of well-established trusted core network router and switch vendors, and has trusted relationships with these manufacturers and vendors developed over time. Among the range of activities it performs when conducting due diligence in the selection of network equipment, AT&T may evaluate hardware and software for vulnerability to denial of service attacks; test equipment to ensure data transfers cannot be intercepted or redirected; test software to ensure data transmission security; examine manufacturer's provenance and business history; and consult with NIST or the Department of Commerce.

In furtherance of these activities, AT&T has developed and maintains a comprehensive set of security policies and standards based on leading industry standards such as ISO/IEC 27001:2005. AT&T has undertaken an audit of its enterprise security policies, program and practices, resulting in formal certification to the ISO27001:2005 Information Security Management Standard, including the latest certification which covers hosting and cloud services.

Such certification requires that AT&T: (1) systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts; (2) design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are

deemed unacceptable; and (3) adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

AT&T complies with standards and certifications required for specific lines of business referenced earlier in these comments.[24] In addition, AT&T has made significant investments in the security of its mobile network. AT&T's Radio Access Network (RAN) complies with 3GPP airlink security standards as well as AT&T Security policies which are in turn certified to the ISO/IEC 27001:2005 Information Security Management Standard. The RAN uses secure protocols in order to maintain and manage communication with the mobile station as well as specific procedures including power control and handover management. An important security mechanism that protects the radio link against eavesdropping is encryption, which protects both user data and network control information.

With respect to company security practices that may be broadly applicable across sectors and throughout industry, AT&T employs processes and procedures in each of the following functional categories: separation of business from operational systems; use of encryption and key management; identification and authorization of users accessing systems; asset identification and management; monitoring and incident detection tools and capabilities; incident handling policies and procedures; mission/system resiliency practices; security engineering practices; and privacy and civil liberties protection.

[24] *Supra, n.19, and accompanying text.*

The fact that AT&T has certified to certain select standards, that it participates in a wide variety of standards setting forums, and that it has adopted practices, polices and procedures in categories of standards proposed by NIST, should not necessarily be the basis for an inference that these actions can be applied universally across CI sectors. As discussed earlier, each CI owner or operator is in the best position to understand specific needs, assess which practices or categories of practices will be most beneficial to mitigating their cybersecurity risks and which pose the most significant implementation challenge.[25] .

ROLE OF SECTOR-SPECIFIC AGENCIES

Finally, the RFI seeks information about the role of sector-specific agencies (SSA) and related sector coordinating councils (SCC) in developing and promoting the use of the Framework and what other outreach should occur. In AT&T's view the SSAs and SCCs should continue to function as they do today - bringing together government and industry to identify critical infrastructure at risk, such as in the National Sector Risk Assessment (NSRA), and to develop broad sector specific plans to mitigate those risks. The SSA and SCCs can facilitate implementation of the Framework within a given CI sector, and otherwise fulfill the performance objectives as set by the Sector Specific Agencies in collaboration with DHS. Appendix A provides some high level background on the communications sector partnership with government.

[25] *Supra, n.9, and accompanying text.*

CONCLUSION

Substantial market-based incentives exist for communications service providers to implement effective network protection measures, as evidenced by sophisticated cybersecurity practices currently in place. Innovation, not regulation, must be our nation's first line of defense against malicious cyber adversaries. As NIST develops a Framework designed to address cybersecurity throughout the Internet ecosystem, it should ensure that its efforts are truly designed to align policy, business, and technological approaches to address cyber risks in an efficient and inclusive manner.

Respectfully submitted,

AT&T Inc.

By: */s/ Theodore R. Kingsley*
Theodore R. Kingsley
Keith M. Krom
Peggy Garber
AT&T Inc.
1133 21st Street, N.W.
Washington, D.C. 20036
(202) 463-4627
Counsel for AT&T

April 8, 2013

APPENDIX A

The Communications Sector has a long history of cooperation among its membership and with the Federal government with respect to national security and emergency preparedness. The sector partnership has roots that go back many decades crystallizing with the formation of the National Communications System following the 1962 Cuban Missile Crisis. Over the years the relationship has only been strengthened through a focus on specific operations, planning and strategic activities. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan (NIPP). The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. This strong bond exists 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.

- ***National Security Telecommunications Advisory Committee (NSTAC).*** The NSTAC (www.ncs.gov/nstac/nstachtml) was created in 1982 by Executive Order 12382 and is comprised of up to 30 chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies and is the lead on policy development efforts within the Communications Sector. The NSTAC provides 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 focus include: strengthening national

security; enhancing cyber security; maintaining the global communications infrastructure; assuring communications for disaster response; and, addressing critical infrastructure interdependencies. Recent NSTAC reports have addressed the physical security of core networks, Internet Protocol-based priority services, the reliance of commercial communications on the global positioning system, cloud computing and security controls and communications network resiliency

- ***Communications Sector Coordinating Council (C-SCC).*** The C-SCC (www.commscc.org) was chartered in calendar year 2005 and leads planning efforts within the sector 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 35 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.
- ***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 (wwwncs.gov). 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.

The Communications Sector has recently completed a variety of activities related to cybersecurity. In 2008 and again in 2012, the C-SCC completed work on the National Sector Risk Assessment (NSRA) as prescribed by the National Infrastructure Protection Plan (NIPP) which included assessments of both physical and cyber risks to the communications infrastructure. The C-SCC also has developed a Sector Specific Plan (SSP) which is intended to mitigate both cyber and physical risks. The CSSP and Sector Annual Reports are developed using the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) process in the Department of Homeland Security (DHS).

ATTACHMENT A:

AT&T INFORMATION & NETWORK SECURITY

CUSTOMER REFERENCE GUIDE

FEBRUARY 2012

VERSION 5.1