Before the
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, Maryland 20899

In the Matter of)
)
Information on Current and Future States of) Docket No. 160725650-6650-01
Cybersecurity in the Digital Economy)

COMMENTS OF

HUAWEI TECHNOLOGIES, INC. (USA) and HUAWEI TECHNOLOGIES, CO., LTD.

Donald A. Purdy, Jr. CSO
Dennis J. Amari. Director, Federal & Regulatory Affairs
Huawei Technologies, Inc. (USA)
875 15th Street, Suite 825
Washington, DC 20005

John Howie
Chief Privacy Officer & Head of Cyber Security
Consumer Business Group
Huawei Technologies Co., Ltd.
15375 SE 30th Place
Bellevue, Washington 98007

September 9, 2016

Executive Summary

Huawei appreciates the opportunity to provide these comments in response to the Request for Information ("RFI") of the Commission on Enhancing National Cybersecurity. In these comments, we principally focus on the subjects of Critical Infrastructure, Federal Governance, and the Internet of Things ("IoT"). Huawei believes that information and communication technologies ("ICT") are powerful drivers of innovation, business transformation and economic growth in the U.S. and throughout the world. However, as the pace of technological innovation continues to race ahead, with dramatically faster broadband and wireless connectivity and the explosive growth of cloud computing, big data, IoT, Software-Defined Networks ("SDN") and Network-Function Virtualization ("NFV"), malicious activity in cyberspace has grown apace as well, with a range of malicious actors capable of finding and exploiting vulnerabilities that abound in government and private networks and systems everywhere.

Government and private organizations need to accelerate collaborate efforts to develop, strengthen, and drive the use of standards and best practices for the assessment and management of risk – by all stakeholders in cyberspace – including the entire range of owners and operators of critical infrastructure and providers of ICT products and services. Use of risk-analytic tools such as the National Institute of Standards and Technology ("NIST") *Cybersecurity Framework* ("NIST *Framework*" or "*Framework*")—a standard- and vendor-neutral risk-analytic tool—should be used to help organizations assess their risk posture and chart a path toward a risk status appropriate to their unique requirements and accepted by their organizational leadership.

With encouragement from government, private organizations should collaborate with each other and other government entities—by critical infrastructure sector or subsector, when appropriate—to identify, develop, or improve standards and best practices appropriate to their sector, including for supply chain risk as was done in the communications sector. Because of the leverage that purchasing power has on ICT suppliers and providers, these efforts should also help inform and encourage the use of security requirements for ICT procurement, thereby increasing the availability and use of more secure products and services.

Government and private industry leaders should also: collaborate in communicating with leaders of organizations to identify and raise due diligence/fiduciary duty requirements for Boards and C-level executives on the need to understand, develop and implement an appropriate plan to address their organization's cyber security and privacy risk and preparedness posture; collaborate to expand the Protected Critical Infrastructure Information ("PCII") provisions to allow other government agencies, in addition to the Department of Homeland Security ("DHS"), to provide similar confidentiality protection for information provided by the private sector.

We face significant, security-related challenges related to the Internet of Things (IoT), which will require substantial efforts by government and private organizations, and continued effort by standards bodies.

I. Introduction

Huawei Technologies, Inc. (USA) and Huawei Technologies Co., Ltd. (collectively "Huawei")[1] submit these comments to the Commission on Enhancing National Cybersecurity ("Commission") and NIST in response to the Notice and RFI in the above captioned proceeding.[2] Huawei is a global leader of information and communications technology ("ICT") products and solutions.[3] Continuous innovation based on customer needs drives our more than 170,000 employees globally— including 1,500 employees in the United States—to create maximum value for telecommunications carriers, enterprises and consumers. By leveraging its experience and expertise in the ICT sector, Huawei helps to bridge the digital divide, promote high-quality broadband connectivity for all, strengthen secure and stable network operations, advance the innovative potential of ICTs and assist customers and industries improve efficiencies that drive economic growth.

Huawei commends the Commission, NIST, and the U.S. Department of Commerce for soliciting public comment in support of the Commission's charge to "enhance cybersecurity awareness and protections at all levels of Government, business, and society, to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security."[4] From the perspective of a world-leading supplier of telecommunications network equipment, information technology products and smart devices in

[1] Huawei Technologies, Inc. (USA), based in Plano, Texas, is a subsidiary of Huawei Technologies Co., Ltd., headquartered in Shenzhen, Guangdong Province, People's Republic of China. Continuous innovation based on customer needs drives our more than 170,000 employees globally—including 1,500 employees in the United States—in order to enhance customer experiences and create maximum value for telecommunications carriers, enterprises, and consumers. The company's vision is to enrich life and improve efficiency through a better connected world.

[2] *See Information on Current and Future States of Cybersecurity in the Digital Economy*, Notice and Request for Information, Docket No. 160725650-6650-01, 81 Fed. Reg. 52827 (dated Aug. 10, 2016) ("*NIST RFI*").

[3] *See Id.*

[4] *See* Exec. Order No. 13718, 81 Fed. Reg. 7441 (Feb. 12, 2016).

more than 170 countries that help connect over one-third of the world's population, Huawei is fully aware that cyber threats will never cease, that secure and stable network operations is an important mission, and that cybersecurity is a global challenge—a challenge that must involve the commitment and active participation of all governments, industry and civil society.anti

II. Critical Infrastructure Cybersecurity

The owners and operators of the critical infrastructure sectors have grown increasingly dependent on ICT products and services. Huawei believes that networks and enterprises everywhere are vulnerable to similar kinds of cyber security and privacy threats.

Significantly, common and global standards and disciplines vary across the sectors of the critical infrastructure in terms of detail and maturity; in some cases they overlap, in others they conflict, in yet others there can be redundancy. In addition, there is often insufficient incentive for owners and operators of critical infrastructure to follow recognized standards and best practices, or to use risk analytic tools like the NIST *Framework* to assess their risk and embark on a disciplined path forward to systematically manage that risk.[5]

Huawei continues to believe that perhaps the greatest challenge to more effective, dynamic management of cyber security and privacy risk affecting critical infrastructure remains the establishment and agreement on consistent, effective, and universal—industry-wide—security assurance standards and disciplines. There are a myriad of different bodies and initiatives—quite well intentioned—that are focused on developing or promoting such standards

[5] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), available at: http:www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

and best practices. More focus and order are required if we are to realize our common industry goal of reducing risk, enhancing assurance, and building trust.

Accordingly, Huawei supports collaborative action among government and private sector organizations to develop a global, risk-informed, fact-based, level playing field for ICT products and services based on internationally recognized transparent standards and best practices and other agreed-upon principles and norms of conduct.[6]

Ultimately, Huawei believes that the public-private establishment of baseline security assurance standards for the ICT industry should cover all key components of the end-to-end lifecycle of ICT products, including R&D, product development, procurement, supply chain, pre-installation product evaluation, and trusted delivery/installation, and post-installation updates and servicing. Such a comprehensive approach, informed by risk, is critical to an effective approach to addressing cybersecurity challenges facing critical infrastructure.

Huawei hopes that this approach can be followed internationally to facilitate coordination of efforts regarding principles of privacy, data protection, and cyber security. Given the global nature of the ICT supply chain, it is very important for vendors, service providers, and corporations to have consistent standards and approaches as they conduct business across multiple continents and various countries.

The standards agreed to by nations, international communities, industry or forums can be the foundation for due diligence requirements of leaders of key organizations, as well as for

[6] *See Cyber Security Perspectives--21st century technology and security – a difficult marriage*, Huawei Technologies Ltd., ("Huawei White Paper/1") (Sept. 2012), available at: http://pr.huawei.com/en/news/hw-187387-securitywhitepaper.htm. Huawei encourages the Commission to reflect on efforts of the EastWest Institute ("EWI") which is working with key companies (e.g., Huawei and Microsoft and others) and governments (US, China, Russia, UK, Germany, India, etc.) to seek agreement on contentious cyber issues including promoting the global availability and use of more secure ICT products. *See* http://www.eastwest.ngo/info/increasing-global-availability-and-use-secure-ictproducts-and-services; *and* http://www.eastwest.ngo/cyber.

potential cyber security compliance evaluation of critical infrastructure. Standards organizations and public-private partnerships and collaborations should serve as platforms for the communication and consultation of all parties, including authorities, buyers and sellers, to collaboratively develop or improve standards, evaluate procedures and methodology, and facilitate the consistency and general applicability of the evaluation result.

To address our global cyber security challenge, our collective and collaborative work should be guided by a set of principles that provide a framework for coordinated action to drive progress on an aligned set of strategic priorities, goals and time-based milestones. We should be prepared to accept that the commitment from some parties may initially not be as strong as we would wish due to an inherent lack of trust held by some parties, the issue of local politics and geopolitics, trade protectionism and competitor misinformation; however, recognizing these dynamics, we should not allow any of these issues to be used as an excuse for not taking action.

Huawei believes that a collective effort should be rooted in guiding principles, such as the following:

- Global: Efforts to improve cyber security must properly reflect the borderless, interconnected and global nature of today's cyber environment in terms of governance, laws, standards and sanctions.
- Legal Requirements: Efforts to harmonize and align international laws, standards, definitions and norms must be undertaken, accepting the challenges of cultural differences.
- Collaboration Based: Efforts to improve cyber security must leverage public-private partnerships to maximize our chances of increasing our collective ability to thwart attacks

- Standards Based: Efforts to design, agree on and implement international standards and benchmarks of ICT vendors should set the standard based on the perceived risk level—there has to be a balance between security and risk
- Verification Based: Efforts to design, develop and implement global independent verification methodologies that ensure products conform to the agreed standards and benchmarks should be agreed and adopted.
- Evidence Based: Efforts to improve cyber security must be based on evidence of risk, evidence of the attacker and evidence of loss or impact—we should focus on facts, not fiction.
- Beginning with the Basics: Efforts to improve basic cyber security "hygiene" must be collectively prioritized to drive the entry point of successful attack to a much higher point.

Based on our experience we believe that are certain characteristics, initiatives, or capabilities that an organization need to effectively manage risk of any kind, including cyber security and privacy risk: (1) top-level, organization-wide commitment to address cyber security and privacy risks, commitments that are "owned" by the Board and C-level executives; (2) enterprise-wide risk-management programs that incorporate cyber security and privacy risks; (3) internal organization-wide governance structure to address cyber security and privacy risk, which provides visibility to the Board and C-level executives; (4) articulated cyber security and privacy requirements and baselines, and performance metrics, which are associated with specific business groups and departments, and individuals; and (5) internal compliance, verification, and audit mechanisms to provide the ability to accurately assess risk status, compliance, and accountability, and provide visibility to the Board and C-level; and 6) all subcontractors and suppliers should be required to undergo a multi-point cyber security evaluation, one component of which is the requirement to sign a cyber security agreement.

However, cyber security is not just about technology, and the approach to risk management cannot be either. It also has to be about people, laws, incentives and disincentives. While there is undoubtedly a focus by ICT providers on the design, development and deployment of technology, there needs to be an equal focus on all other processes—human resources, legal, sales, finance, marketing, and supplier management. For instance, in terms of supply chain diversity, 70% of the components used by Huawei come from suppliers outside of Mainland China, with the United States serving as the largest provider at 32%, and the majority of those are high-technology components, with Taiwan and Europe combining to provide 32%.

Huawei believes that the NIST *Framework* can be a valuable tool for any organization, including key companies in critical infrastructure sectors, to use to assess risk, regardless of what standards or best/good practices that organization may use or refer to for guidance, if any. The *Framework* gives organizations one element of what they need to do about the risk they face—a standard-neutral and vendor-neutral tool to assess their own risk and preparedness and give them guidance to chart a course toward a more appropriate security posture given their risk environment. It can also be used for helping an organization compare the risk posture of suppliers and business partners. We believe that the *Framework* can be a good starting point for any organization that wants to better understand, and improve, their risk posture.

An excellent model that can help inform what is necessary to reduce the cyber security risk to critical infrastructure, is the 2014-2015 work and recommendations in the U.S. communications sector of the Federal Communications Commission's ("FCC") advisory body, the Communications Security, Reliability and Interoperability Council ("CSRIC")—known as

CSRIC IV—Working Group 4, to adapt the NIST *Framework* to provide guidance for the communications sector and its sub sectors.[7]

Generally, the CSRIC IV recommendations provide a significant and important resource for individual companies to use the NIST *Framework* to analyze their risk relative to key indicia of preparedness and to plan and prioritize their path toward a capability appropriate to their business needs and risk environment. This can contribute markedly to the FCC's goal of reducing cybersecurity risk to critical communications network infrastructure, enterprises, and consumers.[8] Whether and how this potentially enriched and informed risk posture by individual companies can inform the quality of the broader sector-wide risk assessment and mitigation planning to help reduce the cybersecurity risk is an issue that is worthy of ongoing evaluation.

Given the quality and insight reflected in this important effort, Huawei believes that other critical infrastructure sectors should be encouraged to embark on a similar course, to generate private sector-led guidance based on the NIST *Framework*—or other recognized approaches to assess risk—specific to their industry sector and customized to their risk environment, and to develop a set of best practices and approaches for members of the sector that addresses risks associated with their vendors and suppliers.

Huawei believes strongly that implementation of the 2015 CSRIC IV recommendations to inform communications providers' risk posture, enterprise risk management approach, and path forward toward a target risk posture, is a very important step toward facilitating a greater understanding of the cyber risks for the communications sector, and how to move toward greater

[7] *See Cybersecurity Risk Management and Best Practices,* Federal Communications Commission Communications Security, Reliability and Interoperability Council IV, Working Group 4, Final Report (March 2015).

[8] *See* Remarks of Tom Wheeler, Chairman, Federal Communications Commission, at the Aspen Institute Communications Policy Conference, at 5 (Aug. 14, 2016).

security, assurance, and resilience of communications networks. In 2016, the CSRIC provided guidance on the use of the NIST *Framework* to evaluate ICT vendors and providers from a cyber security risk perspective, including supply chain risk management. That guidance regarding risk was valuable, but Huawei believes it is important to build on that important work by potentially developing additional guidance for the communications sector, in general, and communication providers, in particular, on how to do risk analysis and set risk-appropriate requirements for their vendors and suppliers. The Open Trusted Technology Provider Standard ("O-TTPS," which is identical to ISO 20243) is worth considering regarding the risks from providers and suppliers associated with technology development and supply chain security.

Huawei encourages anticipated action to update the NIST *Framework* to add explicit guidance regarding supply chain risk which could provide greater clarity to users and buyers of ICT, as well providers.[9] Huawei believes that malicious damage may occur in all activities of the global supply chain, so it is important to focus not only on individual activities, but also the entire supply chain. Supply chain threats fall into two major categories: tainted products and counterfeit products. Threats that can cause tainted and counterfeit products include malware, unauthorized parts, unauthorized configuration, scrap sub-part parts, unauthorized production, and intentional damage. Because of the prevalence of vulnerabilities in networks and systems in the face of a wide range and high sophistication of malicious attackers, it is important to address supply chain risk to protect critical infrastructure, government services, the functioning of private

[9] *See* National Institute of Standards and Technology, Request for Information, *Cybersecurity Framework Feedback: What We Heard and Next Steps*, at 8 (June 9, 2016) (noting that supply chain risk management as a topic under consideration by NIST for an update to the *Framework*). The *Feedback* report identifies supply chain risk management as "a critical area of inclusion for the Framework" as identified in public comments submitted to a December 2015 Request for Information, and by participants at a NIST April 2016 Workshop on adoption of the Framework. The report specifically states, "It was clear that this is an area that demands further consideration for inclusion in further updates." *Id*., at 6.

organizations, and the privacy and integrity of proprietary and private information of organizations and individuals.[10] Because of the importance and resonance of the NIST *Framework* in the United States and in many parts of the world, it would be very valuable to have the *Framework* give guidance about supply chain

The buyers and users of ICT must address the critically important issue of supply chain risk as part of their enterprise-wide approach to risk management. For example, to manage supply chain risk, Huawei embeds in our procurement process security control activities such as supplier security qualification and selection, material security testing, supplier security audit, problem improvement, performance management, risk management, vulnerability management, emergency response, traceability and security agreement. All suppliers are required to pass our cyber security qualification requirements and sign a cyber security agreement. Products from all suppliers are required to undergo cyber security testing. Service delivery of all suppliers must also meeting cyber security requirements. To date, Huawei has executed cyber security agreements with more than 2500 engineering and material suppliers.

Because of the importance of accountability and transparency to warranting trust, Huawei encourage audits, reviews and inspections on all technology vendors, including Huawei, in a fair and non-discriminatory manner, as each audit or review enables companies to challenge their thinking, their policies and their procedures, in turn enhancing their capability, product quality

[10] In its March 2012 report, the United States Government Accountability Office ("GAO") warned that the global supply chain of IT products could be putting national security at risk, stating, "Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations. The exploitation of information technology ("IT") products and services through the global supply chain is an emerging threat that could degrade the confidentiality, integrity and availability of critical and sensitive agency networks and data." *See IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361, at 9 (March 23, 2012), available at: http://www.gao.gov/assets/590/589568.pdf. *Also see* Huawei White Paper/1 at 9.

and product security. At Huawei, we already provide our customers and governments with the ability to undertake comprehensive validation and verification of our products.

Huawei also encourages that CSRIC, for the communications sector, consider (and other similar organizations in other sectors) developing a collection or set of voluntary procurement requirements and model questions that individual organizations can adapt based on their respective risk environments and particular supply chains, and direct to their ICT vendors and suppliers and other third party providers. At a minimum, the owners and operators of the critical infrastructure sectors should be encouraged to more consistently ask security/risk-related questions of their vendors and suppliers, whether as an element in giving preference to such suppliers or as mandatory requirements for consideration in the tender. To the extent that members of a sector or subsector – or multiple sectors or government—have common or similar security requirements or questions, this can have the effect of collective purchasing power to drive the availability and use of more secure products and services.[11]

Huawei believes that it is essential to furthering the FCC goals that communication providers assess and mitigate risks related to vendors and suppliers, including supply chain risk in a transparent, objective, and fact-based way, based on international standards and best practices to the greatest extent possible.

[11] *See Cyber Security Perspectives, 100 Requirements when Considering End-to-End Cyber Security with Your Technology Vendors,* Huawei Technologies, Ltd. ("Huawei White Paper/3") (Dec. 2013), included as a supplement to these comments; *and see* Huawei Press Release (Dec. 2014), available at: http://pr.huawei.com/en/ connecting-the-dots/cyber-security/hw-401493.htm. The paper details the 100 security requirements/ questions that we believe, based on our research and input from customers, are the types of questions that the buyers of ICT products and services (including communications carriers) should consider when selecting technology vendors and suppliers. These questions are broken down into categories covering: strategy governance and control; standards and processes; laws and regulations; human resources; research and development; verification; third-party supplier management; manufacturing; delivering services securely; issue, defect and vulnerability resolution; and audit.

To facilitate transparency and accountability of ICT providers, it is very important for ICT providers to allow their processes and internal systems to be opened up to audit and scrutiny from customers and governments. It is this ability to use real customers and experts from many fields and governments to inspect, vet and validate the approach of different ICT providers that truly enables the development and ongoing improvement of world-class processes and integrated systems.

Many global technology vendors such as Huawei license and use software components from many third parties, and this is included within the developed computer code. For example, Huawei's software may be developed by multiple teams in multiple countries. Yet when there is a security issue, or a vulnerability is found, it is crucial that our internal processes and systems give us the ability to forward and reverse-trace the software components that have been developed and pinpoint what products they are in.

At Huawei, we are continuously enhancing our internal systems and processes to enable us to trace-forward from a raw customer requirement all the way through to the computer code that was produced, and also to reverse-trace from the computer code (or patch/modification) all the way back to the raw requirement that required that computer code to be developed. It is critically important for all ICT providers to do the same.

Organizations that are part of a nation's critical infrastructure should be incentivized to address risks related to cyber security and privacy as part of the fiduciary responsibility of organizational leaders (executives and members of a board of directors, if any) to address risk of all kinds. Organizations should have an organization-wide commitment and governance structure to oversee an end-to-end cyber security assurance system that encompasses policy, organization, process, management, technology and specifications.[12]

Any effective program should emphasize the importance of verification—internal oversight, compliance, and audit—and continuous improvement across the gamut of subject areas that are important to assurance, such as: strategy; governance and control; processes and standards; laws and regulations; people; research and development; configuration management; tools and third-party component management; verification; third-party supplier management; supply chain; procurement security; manufacturing; delivering services securely; issue, defect and vulnerability identification and resolution; traceability; and audit.[13]

The FCC and DHS, in collaboration with communications-sector trade associations, could work together to offer webinars and live training/discussion sessions for small and mid-sized communication providers to introduce the NIST *Cybersecurity Framework*, informed by the CSRIC IV report, and present use cases of the application of the best practices that are relevant to each of the five sector segments. It would also be beneficial if they could collaborate to develop a common instrument, template, and/or questionnaire that could be used by smaller companies in the various sector segments so smaller companies with fewer resources will not bear the burden of numerous inquiries from numerous customers asking for similar information requiring completing different forms.

[12] To promote transparency about Huawei's program and facilitate discussion about how to improve end-to-end assurance, Huawei a white paper in 2013 that provides considerable detail about Huawei's assurance program. For a more complete articulation about Huawei's approach to end-to-end assurance, *see* Cyber *Security Perspectives--Making cyber security a part of a company's DNA-A set of integrated processes, policies and standards* ("Huawei White Paper/2") (Oct. 2013), available at: http://pr.huawei.com/en/news/hw-310599-cyber.htm; *and see* Huawei Comments, Developing a Framework to Improve Critical Infrastructure Cybersecurity, Fed. Reg. 132024 (Feb. 26, 2013), National Institute of Standards and Technology, Docket Number 130208119–3119–01, available at: http://csrc.nist.gov/cyberframework/rfi_comments/040813_huawei.pdf.

[13] *See* Huawei White Paper/1, *infra*.

In addition, more broadly, it would be helpful if DHS would work with other critical infrastructure sectors for which it is the sector-specific agency, and with other agencies that are the sector-specific agency for other sectors, to try to encourage development of guidance similar to the CSRIC IV best practices, for priority critical infrastructure sectors, including small and mid-sized companies. We understand that the financial sector has begun work in this important area.

In addition, government and the private sector should consider collaborating to expand the PCII provisions to allow other agencies (*e.g.*, FCC; the Departments of Treasury, Transportation, and Energy; the Federal Energy Regulatory Commission and the Nuclear Energy Regulatory Commission), in addition to DHS, to provide similar confidentiality protection for information provided by the private sector.

III. Federal Governance

Government needs to work with the private sector to drive more substantial progress in reducing risk and increasing preparedness. One concrete step would be for governmental and private industry leaders to communicate an executive message designed to identify and raise due diligence requirements for Boards and C-level executives regarding the need to understand their organization's cyber security and privacy risk and preparedness posture, and develop and implement a plan to move to a more appropriate and sustainable risk/preparedness posture.

This message—in appropriate instances communicated on a sector rather than national basis—would include recommendations that organizations: (1) need top-level, organization-wide commitments to address cyber security and privacy risks, commitments that are "owned" by the Board and C-level executives; (2) need to have enterprise risk-management programs that incorporate cyber security and privacy risks; (3) need an internal organization-wide governance structure to address cyber security and privacy risk, which provides visibility to the Board and C-level executives; (4) need to identify and implement cyber security and privacy requirements and baselines, and performance metrics, which are associated with specific business groups and departments, and individuals; and (5) need to implement internal compliance, verification, and audit mechanisms to provide the ability to accurately assess risk status, compliance, and accountability, and provide visibility to the Board and C-level. This message should include a recommendation that organization use the NIST *Framework*—sometimes characterized, quite appropriately, as "a risk analytic tool"—or a similar analytic approach, to assesss their risk, identify a target risk posture, and develop a plan to reach that target risk posture.

Huawei has independently taken each of the steps detailed above. In addition, government should work with private sector to encourage private industry through Sector Coordinating Councils and the Cross-sector Cyber Working Group, or other formal or informal groups, to leverage their collective purchasing to drive greater availability of more secure products and services by: (1) identifying common security requirements for products and services; (2) encouraging buyers to be more consistent in using security requirements in their procurements; and (3) encouraging buyers with similar requirements to work collaboratively incentivize providers to raise the bar on cyber security and assurance. There is perhaps no greater incentive to motivate providers to raise the bar than the desire to sell their products and services. Not enough is being done to use this important motivator.

IV. Internet of Things

IoT is a generic term for a connected ecosystem of sensors, emitters, displays, input devices and the underlying network, computing systems, storage subsystems and management infrastructure. Some organizations, such as NIST, prefer to refer to this as the "Network of Things."[14] This leads to the first challenge we face – there is no international standard nor consensus in the industry about what IoT really is, what it will look like, how it will work, or even the benefits it will bring to society.

It is forecast that there will be billions of interconnected devices using technologies such as WiFi, 4G/LTE and still-being-defined 5G. Software Defined Networking ("SDN"), Network Function Virtualization ("NFV"), and Cloud Computing will most likely be required to make the IoT work, but there are no architectural blueprints or even global success stories showing how the IoT will be built and the challenges it will bring in reality

Without a true understanding of what IoT consists of, or how it will work, it is difficult to quantify and debate the trends and challenges society faces. However, there are some likely areas of challenge that can be identified.

The first challenge is privacy. Globally there is no uniformity in privacy law, and most international companies run privacy programs that incorporate elements from regional and country-specific law and norms, and use frameworks such as the Generally Accepted Privacy Principles ("GAPP") to bring them together. In this approach, the concept of Notice, Choice and Consent is paramount. Sensors in the IoT ecosystem will be discreet, small and low-powered, and lack the ability to provide notice and record consent from individuals through the lack of

[14] *See* Jeffrey Voas*, Network of 'Things',* National Institute of Standards and Technology, NIST Special Publication 800-183, (July 2016).

display and input technology. Further, these sensor devices may be placed in public places where they will record data on everyone who walks by, making it infeasible to provide individual notices and obtain individual consent in any case, even if the technical means to provide notice and record consent was available. Current notions of privacy will come under pressure and alternate means to guarantee the rights of individuals will need to be researched and, potentially, legislated.

The second challenge that can be reasonably forecast is that due to the low computing power in many IoT sensors, technical security (which requires storage, processing capability, and power) may not be uppermost in the minds of developers. As vulnerabilities in devices are discovered it is possible that these could be exploited en masse, and entire networks could become compromised. There is already evidence that low-powered devices used in home automation systems have been remotely compromised and used to form botnets, designed and used to attack commercial targets. Even if devices could be updated to remove vulnerabilities discovered, devices that are embedded in infrastructure—such as light-poles, transportation structures such as bridges and roads, and in other hard-to-get-to places, or even sealed within permanent structures—may be essentially unmaintainable. The sheer number of IoT devices may simply mean that it will be impossible to apply updates to all of them to remove the vulnerabilities that will inevitably be discovered. As these devices become more powerful and use less energy, it may be possible to perform Over-The-Air (“OTA”) updates, to update vulnerable devices, but the sheer number of predicted devices will likely mean that current approaches to updates with which consumers are familiar, will not be feasible.

The third challenge presented here is the difference between the expected useful life of IoT devices, the life expectancy of the companies that manufacture them, and the life expectancy of individual product lines and services. Consumers are well aware of this problem, and many have drawers full of technology abandoned or made obsolete by manufacturers going out of business or their conscious business decisions. As IoT sensors and infrastructure are deployed, consideration should be given to means that disables the devices if their manufacturer “abandons” them, or the product or service they were built and deployed for is no longer commercially available, and they cannot be successfully repurposed.

Public bodies such as NIST, and international standards organizations, are working to develop reference architectures, interoperability specifications and other mechanisms that will allow the continued evolvement of the IoT. Most established manufacturers are investing heavily in research and development activities, to identify potential challenges.

Regional governmental organizations such as the European Union are promoting research and development activities using public funds, and, like the US Government, are calling for discussion and engagement about the challenges that will be face, and be faced by, IoT.

Conferences and debates organized by industry associations help raise issues to the minds of governments, academics and researchers, and spur companies to innovate and bring solutions to market that can help address challenges.

Commercial research and development by established companies will likely yield the greatest number of solutions to technical challenges.

Collaboration between industry and government will be necessary to address the security and privacy challenges, and governments will need to work with each other if they wish to develop a global marketplace for IoT, with global benefits.

Within the next year or two, NIST should be empowered to continue its research, perhaps by adapting the highly successful *Framework* for IoT to better address the challenges. Agencies of the government can also work with industry associations, academia, commercial entities and others to encourage dialogue, debate, and identification of solutions that address challenges.

Over the next decade, government efforts should focus on continued monitoring of the evolution of IoT, especially for privacy and cybersecurity challenges, and consult with experts both within and outside government to ensure that industry is, itself, adequately dealing with the challenges.

To the extent that IoT becomes part of the nation's critical infrastructure, the government may need to work with the private sector to develop and set minimum standards or best practices, and be prepared to take steps to guarantee that deployment does not result in lawsuits against manufacturers for privacy violations where it can be proven that manufacturers have demonstrably taken good faith attempts to protect individual privacy, such as through the "Safety Act."[15]

In terms of responding to future challenges, one of the greatest concerns the U.S. government should have is that poorly funded and uneducated disruptive startups, and manufacturers with low product margins, bring products and services to market that do not consider the impact on privacy and cybersecurity, and lead to significant issues that are unique to IoT due to the volume of sensors and data collected and processed.

While markets will eventually reward responsible companies that address cybersecurity issues in their products and services, it may be that the current cyber threat climate cannot "take the chance" that only diligent companies will survive and crowd out inferior products and services. The U.S. government may wish to consider endorsing product seals or certifications in

[15] The Support Anti-terrorism by Fostering Effective Technologies Act, enacted as Subtitle G of Title VII of the Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135, enacted November 25, 2002); 6 U.S.C. Sections 441-444. *See also* Final Rule, 6 CFR, Part 25 at 33150.

some capacity, that endorse IoT products and services from companies that embrace individual privacy and software safety through stringent development practices.

Additional work on the NIST *Framework* needs to be undertaken to ensure its applicability in new and emerging technologies. The *Framework* cannot ever be considered “done” or “complete”.

The U.S. government can also remove barriers for adoption of key technologies that demonstrably enhance cybersecurity, in particular cryptography and defensive systems technology that currently does or may in the future be on the U.S. Munitions List (USML).

Within the cybersecurity industry there is largely a consensus around lexicons, with ISO/IEC 27000 being the lead international standard. As new terms are created, the U.S. government should have NIST take the lead in developing and managing a lexicon or lexicons related to IoT.

V. Conclusion

The development of ICTs and networks has contributed to tremendous social and economic progress, encouraging the flow and sharing of information, providing more opportunities for innovations, lowering the costs of innovation, and improving the world's health, wealth and prosperity. Huawei firmly believes that cyberspace has become the “nervous system” through which society operates. And given its importance to society, governments and private organizations must accelerate collaborative efforts to develop, strengthen and drive the use of standards and best practices to assess and manage risk. Risk-analytic tools, such as the NIST *Framework*, should be used to chart a path forward toward a risk status that is appropriate to the requirements of each and every organization that relies on cyberspace. Further public-private collaboration is needed, however, to identify, develop or improve standards and best practices to related to supply chain risks. And as society moves toward a paradigm where connectivity includes not just people but also things, privacy and security challenges will similarly require collaboration by government and industry in order to realize the benefits of IoT to society.

Huawei again appreciates the opportunity to offer its views to the Commission, NIST and the Commerce Department on this important initiative. We hope these comments serve to inform the Commission's important mission in developing recommendations consistent with Executive Order 13718.