EXHIBIT A

DECLARATION OF JOHN SUFFOLK

I am John Suffolk, the Global Cyber Security and Privacy Officer for Huawei Technologies Ltd, and I have been employed in this role, or a similar role, since 1 October 2011. Prior to this I worked for the United Kingdom Government where for 7 years I was Her Majesty's Government Chief Information Officer and Senior Information Risk Owner. I have worked in Information Communications Technology in multiple roles for 40 years, undertaking substantial large scale business transformations and have been heavily involved with security and privacy, including security at a classified level.

I am submitting this Declaration in response to the FCC Docket Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Notice of Proposed Rulemaking - WC Docket No. 18-89.

In my opinion, the objective of the Notice of Proposed Rulemaking to protect the security of U.S. telecom carrier networks is laudable, but the proposed rule will not achieve this objective.

The threats to carrier network security are varied, and cannot be addressed effectively by singling out a specific country or selected companies. There are five main reasons why this proposed action cannot achieve its objective, and may indeed be counterproductive:

1. The ICT supply chain is global;
2. Because the ICT supply chain is global, the risk is from the cumulative supply chain, not the vendor whose name happens to be on the "box" or who provides the named application;
3. The global supply chain generates thousands of security vulnerabilities from vendors of all countries, including the United States;
4. Governments and companies could do more to protect themselves; and
5. Huawei's approach to security by design development and deployment improves the security of its products and the supply chain.

1. The ICT supply chain is global

In March 2012, the GAO published a *report "IT SUPPLY CHAIN National Security Related Agencies Need to Better Address Risk"*[1] that examined the inherent risks in the supply chain. The report, although dated some 6 years ago, identified that a simple laptop might contain components from 18 separate companies. The world has continued to utilise global supply chains since 2012, and if anything the situation is more complex now than it was then. **Excluding one country or specific companies from that country will not achieve the stated goal.** In fact, the GAO report observed that four "national security-related departments" – the Departments of Defense, Homeland Security, Justice, and Energy – had stated

[1] https://www.gao.gov/assets/590/589568.pdf

that they have not "determined or tracked the extent to which their telecommunications networks contain foreign-developed equipment, software, or services" because "doing so would provide minimal security value relative to cost."

It is wrong to assume that the label on a vendor's box, or indeed a computer application, conveys that the contents are solely from that named vendor. Take Huawei for example. Huawei uses a global supply chain like every other ICT vendor and service provider. In general, around one third of what is in Huawei equipment is from Huawei/China and the remainder from the rest of the world, including the USA, Europe, Japan, South Korea, Taiwan. **The name of the vendor, or vendor's home country, does not determine the source of the product and cannot be used as a key criterion for a source of threat.**

This is true for other companies such as Nokia: some of its equipment is made in China, with components purchased from Chinese companies, and indeed Nokia has a joint venture with a Chinese Government-owned entity, Nokia Shanghai Bell.

The same is true of Ericsson, which also has a joint venture with a Chinese Government owned entity, Nanjing Ericsson Panda Communication Co. Ltd., has some manufacturing based in China, and sources components from Chinese companies.

Both Nokia and Ericsson provide substantial communications technology within the United States within the classified and non classified areas.

The Chief Executive of Nvidia, Jensen Huang, recently stated in an article, "It is definitely better - and it's actually vitally important - that the world continues to have a collaborative and open business relationship. … If you just think about Nvidia, China is one third of Nvidia's business. However, remember, everything we sell to China goes through our distribution partners, gets integrated into computers, it gets integrated into data centres and clouds." He went on to say, "Almost everything is made everywhere in the world. An iPhone is made in Taiwan, Korea, China, and the United States all at the same time. It is impossible for any product to be created in just one country. We are so interdependent. I think that's a statement of fact, it's not a political statement, it is not a policy statement. It is just a statement of fact."[2]

It is clear that to achieve the stated objective of the FCC based on the criteria of where something is built, or where components come from, the USA would need to make all of its own ICT components locally or have total control over every global process and supply chain. This is completely infeasible as a practical

[2] http://www.datacenterdynamics.com/content-tracks/servers-storage/nvidia-ceo-there-will-not-be-a-us-china-trade-war/99973.fullarticle

matter, and could not be achieved without closing down most ICT companies, or infrastructures, telecommunications networks, and cloud services in the USA.

2. **Because the ICT supply chain is global, security risks arise from the cumulative supply chain, not the vendor whose name happens to be on the "box" or who provides the named application**

The world is now connected with a wide range of cloud computing infrastructures providing applications and services to all parts of the world. It is not possible to understand and limit the components in this interconnected world. According to an article in Wired **many of the world's well known and used cloud data centres use servers built in Asia and China**.[3] The article states "The move away from U.S. network equipment stalwarts is one of the best-kept secrets in Silicon Valley. Some web giants consider their networking hardware strategy a competitive advantage that must be hidden from rivals."

Facebook, which has been a leader in "open computing", since as long ago as 2014, helped open up the data centre market. As reported in the Register[4], "the rise of Facebook helped to ruin the data centre hardware market, caused IBM to sell its x86 business to Lenovo, spurred HP to embark on an ambitious "Moonshot" server, and encouraged Dell to go private. … But most importantly of all, it propelled a scrappy group of Taiwanese and Chinese equipment makers into Western markets, and shook up the IT supply chain in the process."

Today, much of US Business and Infrastructure runs on hardware and software from Asia.

Even today global companies such as Microsoft, Facebook, and Google have partnerships & supply agreements for their global products and services – including cloud data centres that are used by much of American business. For instance, as reported by Microsoft, "*Xiaomi and Microsoft sign[ed a] strategic MoU in cloud, devices and AI areas*"[5] that *" will help in strengthening Xiaomi's leadership in mobile, smart devices and services, and contribute to the acceleration of its international expansion."*

As previously detailed, non-Chinese companies have extensive access to Chinese vendors and utilise Chinese manufactured products in their global product lines, as well as operate extensively in China.

---

[3] "Exclusive: Google, Amazon, and Microsoft Swarm China for Network Gear", *Wired*, https://www.wired.com/2012/03/google-microsoft-network-gear/ (March 30, 2012)
[4] https://www.theregister.co.uk/2014/02/20/facebook_hardware_feature/
[5] https://news.microsoft.com/2018/02/23/xiaomi-microsoft-sign-strategic-mou-cloud-devices-ai-areas/

The CEO of CISCO, Chuck Robbins, stated that Cisco has *"worked with carriers in China to build their networks"*[6] and when we examine widely available data, Apple, Nike and 18 other U.S. companies have $158 billion at stake in China.[7]

Similarly, China Daily[8] stated "*in 2016, Apple had 766 global suppliers, among which 346 were on the Chinese mainland. Additionally, about 3 million Chinese workers were working for Apple that year and the number has increased in 2017. The process of building iPhones requires 8,700 mid-level engineers. In the US, there were only 7,000 such college graduates in 2014. In China, there were 240,000 skilled workers and engineers at Foxconn, Apple said in 2015*". In summary half of iPhones are manufactured in central China's Zhengzhou city.

If US Government policy were to be executed fairly to achieve the stated objectives of FCC then the Apple iPhone, to name one such product, should be banned from the USA. This is not to single out Apple, though; the same is true of nearly every other mobile handset marketed under a US brand name.

3. The global supply chain generates thousands of security vulnerabilities

I have demonstrated that the world is interconnected with a global supply chain, and it is clear that simply excluding a country or a small number of vendors, will do nothing to achieve the stated objective of "*protecting against national security threats".* Let me elaborate:

- In 2017 Huawei's external global supply vendors notified Huawei of over 250 vulnerabilities that they had identified in the components they had provided to Huawei. That is, vulnerabilities found by other vendors in their products that had been imbedded in Huawei products. As far as we are aware Huawei is the only vendor to have signed cyber security agreements with all of their high technology vendors to notify Huawei when they become aware of a vulnerability in their products.
- The total number of vulnerabilities published by some (not all vendors publish their vulnerabilities) totalled 14,713 in 2017.[9] All but one of the top ten vendors by volume publishing vulnerabilities were US technology companies. All of these products are potentially a national security risk, but the solution is not to ban them from the market but to encourage vendors to adopt openness, transparency and commitment to improving the security of all things digital.
- The issue is not about whether there is a vulnerability; it is about whether it can be exploited for illegal or immoral activity. 2017 saw major issues being

[6] https://www.cnbc.com/video/2018/02/28/cisco-ceo-have-worked-with-carriers-in-china-to-build-their-networks.html
[7] https://www.marketwatch.com/story/trade-war-watch-these-are-the-us-companies-with-the-most-at-stake-in-china-2018-03-29
[8] http://www.chinadaily.com.cn/business/tech/2017-09/19/content_32191283.htm
[9] The responsible public disclosure database of known vulnerabilities, by type, vendor severity etc. https://www.cvedetails.com/browse-by-date.php

generated through malware such as Wannacry, Petya, Locky, Apache Struts and many more, as well as major hardware issues such as the Intel, AMD, and Arm design issues and abundant open source software vulnerabilities . The threats do not originate from the equipment manufacturer or software developer, but from external actors who target these vulnerabilities. The manufacturers and developers are the first line of defence against these threats. Once again this demonstrates that cyber security is a global issue which must be addressed globally. **The actions proposed by the FCC do not address these cyber security issues and will not improve the security of the US infrastructure.**

4. Governments and companies could do more to protect themselves

As discussed above, prohibiting technology from one country or a few companies will not improve cyber security resilience of any country or company. We all rely on a global supply chain and that global supply chain generates potential threats to all countries and companies. The wide range of security issues in the past few years have not come from one single country or set of vendors.

However, it has always been clear from all research on best practices that countries and companies could do more to protect themselves by just adopting basic cyber hygiene.

The USA, through NIST, and Europe through ENISA with other bodies, have been productive in issuing what they see as best practices. These are also well documented by organisations such as:

- SANS Institute, CIS Critical Security Controls: Guidelines[10]
- Centre for Internet Security, Follow our prioritized set of actions to protect your organization and data from known cyber-attack vectors[11]

There are also many international standards such as the ISO 27000 range as well as cloud computing assessments including CSA – we are not short of knowing what to do to protect ourselves from all but the most determined of attackers.

Whilst we have these best practices, and we have had them for many years, substantial evidence shows the basics of cyber security hygiene are not executed – even within the US Federal Government and even in classified areas.

A recent report from Bitsight[12] identified that a sample of 1,200 US Federal Government contractors fell well short of security expectations, *"across industries including aerospace and aviation, business services, healthcare and wellness, engineering, technology, and manufacturing, who provide critical products and services directly to the federal government and are central to*

[10] https://uk.sans.org/critical-security-controls/guidelines
[11] https://www.cisecurity.org/controls/
[12] https://www.prnewswire.com/news-releases/contractor-cybersecurity-gaps-put-us-federal-government-at-risk-300599150.html

national security, the national and global economy, and the environment." Two key findings were:

- Nearly 50% of contractors have a BitSight grade below C for the Protective Technology subcategory of the NIST Cybersecurity Framework, **a sign that many are not following best practices for network encryption and email security**.
- Nearly one in five users at Technology and Aerospace/Defence contractors have an outdated internet browser, making these employees and their organizations **highly susceptible to new variants of malware.**

The results of poor cyber hygiene and lack of management focus can be seen in major data breaches such as Yahoo, Office for Personnel Management, Target Stores, eBay, Equifax and many more. Indeed research by Synk[13] showed that 24% of breach root causes were down to companies using components with known vulnerabilities.

5. Huawei's approach to security by design development and deployment sets a high standards bar that few can match

All the factors discussed in the preceding sections do not mean that Huawei can escape its corporate social responsibility to ensure that the products and services it develops and operates conform to best practice, are designed and built with security and privacy in mind, are tested rigorously and independently and have the governance in place to ensure that the risk of insider threat is minimised to the lowest possible value.

As the Global Cyber Security and Privacy Officer who reports directly to our Founder, Mr Ren Zhengfei, I am accountable for security and privacy across the whole organisation and sit on the Global Cyber Security (and Privacy) Committee. In my seven years at Huawei I can confirm that I have had full and unfettered access to all Huawei people, facilities, documentation etc. I can confirm that my suggestions, requirements and instructions have been fully debated and implemented, or are being implemented. I can confirm that I have never been unduly influenced by any person within Huawei, or outside of Huawei, to reduce, stop, or alter any requirement I might have had that would, in my view, improve security by design, development or deployment – or indeed do anything that would weaken the safety and security of the products and services we produce.

That is not to say that we are perfect, or that we produce perfect code all of the time or that we execute every process right first time – no company in the world can say that. But, as far as I am aware, our practices and standards are as robust and sound as any other telecom equipment vendor in the world.

[13] https://snyk.io/blog/owasp-top-10-breaches/

I have previously published significant detail of the lengths we go to, to ensure our products and services are designed, developed and deployed to ensure the highest levels of security. I have summarised some of the key points below.

Strategy, Governance and Control	Huawei has a long standing executive committee, the Global Security & Privacy Committee that is chaired by a rotating Chairman. This committee sets overall strategy, monitors execution and takes remedial action where necessary. This committee is made up of the senior executives who have responsibility for business processes, business groups and functions and who ensure security and privacy is imbedded into their operations. They are held to personal account for the success of their processes, and their operations independently audited to ensure compliance.
Building the basics: Processes and standards	Huawei has adopted since the late 1990s global repeatable processes across the organisation. Originally designed and implemented in cooperation with IBM, Huawei is a process driven organisation – it is true to say we have a process for everything. This is crucial because security and privacy has been built into these processes. Huawei automates processes where possible for efficiency and quality. Processes and supporting IT build in control and checkpoints, escalate to management for higher approval and review and provide auditing and traceability capability. We positively encourage customers and regulators to audit our processes and are a world leader in transparency in this area. Where a process can be measured against an international standard we will adopt this. Huawei has achieved many international certifications from many standards and certification bodies including for ISO standards, counter terrorism protection in supply chain, cloud operations, TQM for Six Sigma and TL9000, product standards such as FIPS for encryption and common criteria for products. Our portfolio of international certifications and accreditations are extensive.
Laws and Regulations	The law is complex, variable and ever-changing. Even if there is a law in a country, the ways of enforcement might differ greatly or there might be different interpretations of the same law or code. Laws, codes, standards and international controls add complexity and risk to a supplier and a business. We ensure at a global level and local level that we adopt all applicable laws and regulations. We have a substantial in-house legal team and we employ external legal counsel in many countries in which we operate.
People matter	Many companies say that their people are their most important asset, which is true. However, from a security perspective they can also be their greatest weakness. The way people are employed, trained, motivated and their performance managed, often determines the difference between success and failure – not just for cyber security but also for the delivery of the overall company strategy. Huawei has comprehensive people management systems. Performance management and appraisal systems are globally adopted, with peer based reviews. We have published conduct guidelines and annually all employees are retrained and re-examined on the adoption of Huawei business conduct guidelines. Failure to adopt appropriate conduct will result in dismissal and this is evidenced, internally every month, where following independent review of behaviour those that have not adopted the highest levels of legal and ethical behaviour are dismissed or formally disciplined.

Research and Development	Companies do not want to use their scarce capital to buy high-technology products from companies who do not have rigorous R&D processes that deliver consistent high quality, safe products. Nor do they want to see vendors having to make investment decisions between 'do they invest in a new product' or 'do they invest in making all products safe and secure'. Just as quality cannot be bolted onto a product neither can cyber security; At Huawei we demonstrate our long-term commitment to enhancing their R&D approach to accommodate appropriate cyber security design, development and deployment, as well as investing in the next generation of products. Since the late 1990s we have developed and refined our Integrated Product Development (IPD) process, initially with the support of IBM, Based on PACE, enhanced using Microsoft support and measured against SDL, and independently audited our process versus reality using the BSIMM methodology from Cigital. R&D is underpinned by comprehensive IT support, full capability to fully control and automate complex product development including: automated code scanning for quality and known code issues; full traceability to ensure any code changes are traced back to the developer or forward to the product the code ended up in; full third-party management control to ensure known components from known third-parties are used; full vulnerability/ defect management to ensure known defects are resolved before product launch. A tight "gated" development process that provides independent checkpoints on whether a product can progress to the next stage. Full digital signature capability to sign software to protect against tampering and full (no-man-in-the-middle) automated processes to take signed software from R&D into manufacturing with zero touch.
Verification: Assume nothing, believe no one, check everything	Whilst a robust R&D process is fundamental to quality and to safe and secure products, R&D can be under pressure to launch new products quickly without the right testing and verification. Having in place a multi-layered "many hands" and "many eyes" approach to independent verification reduces the risk of unsafe products being distributed. A balance of end-to-end checks and balances supplemented with tiered independent security verification ensures a "no shortcuts" approach and protects customers' investment and services. I, as Global Cyber Security and Privacy Officer, have full veto rights to block any product or solution if I am not satisfied with the security quality of the product. We have a full independent security test lab, that reports to me directly, to independently test products after R&D have developed/ changed the product and before launch. We also use, and customers are free to adopt any verification method they wish, a wide range of security testing companies from the USA, Europe and Asia to validate our products. We adopt security standards and certifications where they exist. We also have two independent labs, not under Huawei control, one in the UK and one in Canada that independently assure our products. We believe our products are more stringently validated than any other commercial vendor in the world.
Third-party supplier management	Many large high-technology companies use third-party companies for hardware components, software components, delivery support and installation. If the third-party's technology or processes have security weaknesses, this can significantly increase the weaknesses of the vendor's products and services as they are integrated into the product the customer will receive. End-to-end cyber security means a vendor must work with its suppliers to adopt best practice cyber security approaches. We were the first, and we still believe today to be the only vendor, that has required all of its technology vendors to sign cyber security agreements, and work with us to improve the security of our supply chain. Our work with third-parties is rigorous, comprehensive and auditable.

Manufacturing	Manufacturers of products must take in all of the components from whatever their source country of origin and security standard, manufacture an end-product for a customer and ensure that throughout every stage of manufacturing and product shipment, no security risk has inadvertently or intentionally been introduced. In manufacturing we have operated a fully total quality management approach for over 15 years. We adopt Six Sigma, and are at 5.9. We conform to all TQM certifications and security certifications including TAPA and CTPAT and our remote centres conform to ISO28000. We were one of the founding members of the supply chain standard OTTPS, helped formulate the standard, promoted its adoption, and are only one of two organisations to have achieved it. We have a zero touch mechanism where software is automatically taken off protected environments in R&D and loaded onto equipment. We have secure cages to avoid tampering and use secure international shipping companies.
Delivering services securely	There is not much point in focusing on designing your products with security in mind if when you come to deploy your technology, or support and maintain the technology, this is not done in a secure way. Customers rightly want to ensure when equipment is supporting their business that its operation and maintenance is safe and secure including upgrades, patches and fault fixing – they expect security throughout the life of the product. Engineers are fully controlled in their environment, ensuring express permission is obtained from customers before action on their networks. Spare parts, return and faulty components are all tightly controlled to ensure protection of any personal data.
When things go wrong: Issue, defect and vulnerability resolution	It goes without saying that no responsible company can give a 100% guarantee when it comes to security. Therefore, a company's ability to respond effectively to issues and learn lessons from what has gone wrong is critical to both the customer and the vendor. Knowing what to do in a "crisis", ensuring senior executives are informed to make speedy decisions and working effectively with customers and stakeholders ensures that normal service is restored quickly and safely. Our PSIRT Team works diligently with security researchers, third-parties and our own product teams to professionally resolve and disclose vulnerabilities. Our end-to-end tracing capability enables us to, within hours, pinpoint what products might be impacted by vulnerabilities ensuring that we can provide speedy response to our customers.
Traceability	When things go wrong being able to quickly identify where it has gone wrong, what hardware or software component caused the issue and identifying where else that component is used is crucial to timely recovery. However, that is not enough; root-cause analysis demands an ability to forward and reverse trace every person, every component from every supplier in every product for every customer. Our internal IT enables us to fully trace forward any code or component. Who developed code, what product that code ended up in and what customers received that product. We can trace back from customer equipment through manufacturing, through code development to who asked for a requirement to be added.
Audit	Rigorous audits play a key role in assuring the Board and senior company officials, and assuring your customers, that the appropriate policies, procedures and standards are being executed to deliver the required business outcomes. We apply the ABC model – **A**ssume nothing; **B**elieve no one; **C**heck everything. From internal audit, to independent testing; from customer audit to regulator reviews; to third-party reviews Huawei fully opens up all of its processes controls, documentation and products for independent audit. We believe we are the most audited, inspected, reviewed and examined ICT company in the world, and all of this demonstrates that a product or service from Huawei is a safer product or service.

6. Summary

In summary I have demonstrated that the ICT supply chain is global and it is not possible to achieve the FCC's stated objective by limiting products from one country. I have demonstrated and proven without doubt that through this global supply chain the USA, like every other technology based country, runs its infrastructure with components and software from around the world. The name of the vendor is not relevant nor is the name on the box.

I have demonstrated that every vendor has vulnerabilities in their products and that every vendor must contribute to the improvement in cyber security.

I have demonstrated that far from Huawei being a risk to security, we are in fact a champion of best practices, a champion of openness and transparency and a champion of protecting user data. As stated by our Founder *"we will never put the commercial interests of our company ahead of security"*.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 28, 2018.

John Suffolk