Rt Hon Norman Lamb MP
Chair of the House of Commons Science and Technology Committee
House of Commons
London
SW1A 0AA

29 January 2019

Re: Security of the UK's communications infrastructure

Dear Mr. Lamb,

Thank you for your letter on 15 January, and for your questions.

The UK is known for its openness, rule of law, and developed finance industry. This has helped attract investment and high calibre talent from all over the world, and win broad recognition among people in both China and around the World.

Huawei is a leading global provider of information and communications technology infrastructure and smart devices. We entered the UK market 18 years ago, and for nearly two decades we have been working closely with our local partners to deliver innovative products and technologies to our customers. We were fortunate to play an important role in the deployment of the UK's fixed broadband and wireless infrastructure.

We have also made a significant economic contribution to the UK. We have invested and procured two billion pounds in the UK over the past five years, including local procurement. Through these investments we have created more than 7,500 direct and indirect job opportunities.

Huawei and the UK share a broad set of interests, and Huawei is widely seen as an excellent example of productive partnership between China and the UK.

As a private employee-owned company, customer trust is extremely important to us. We are happy to have the opportunity to respond to the questions in your letter.

Q1: What reassurances can you give to demonstrate that your products and services pose no threat to UK national security?

First, our solid track record in security is our strongest evidence. We believe the best way to address any concerns is to let the facts speak for themselves. Over the past 30 years, Huawei has provided network products and solutions to nearly 1,500 telecom operators in more than 170 countries and regions. Our products and solutions deliver stable telecom services to more than three billion people.

Our solid track record in security is evident: Our equipment continues to run stably, and we have experienced no serious security incidents. Recent network outages in the UK and Japan were not caused by Huawei products, which is a testament to the

security and reliability of our products on live networks.

The governments in some countries have labelled Huawei as a security threat, but they have never substantiated these allegations with solid evidence. For us, the lasting support and trust of our customers worldwide speaks volumes.

Second, Huawei has incorporated cyber security into the very DNA of our business management. Cyber security and privacy protection are our top priorities.
Since 2011, Mr. John Suffolk, the former Chief Information Officer of Her Majesty's Government, has been serving as our Global Cyber Security & Privacy Officer (GSPO). With the support and authorization of our Board of Directors, and under the leadership of our GSPO, Huawei has established a sustainable and trustworthy global cyber security assurance system across all aspects of our business, including corporate policy, organization, processes, management, technology, and technical standards.

We have integrated security assurance into all business processes across R&D, supply chain, sales and marketing, project delivery, technical services. This is a fundamental requirement of quality management at Huawei, which we guarantee through a robust set of management systems and technical specifications.

Huawei has also established a Cyber Security Verification Lab, which works independently from other business operations within the company. This lab conducts independent security testing on Huawei products, and provides our customers with verification reports that fully detail the quality and security capabilities of our products. This lab does not answer to any of our business departments, and reports directly to our GSPO to ensure that its reports are independent. To learn more about our approaches and practices in cyber security, please refer to the white paper at the following URL, which is openly available worldwide:

a) Huawei Cyber Security White Paper:
https://www.huawei.com/uk/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016

b) 5G Security Architecture White Paper
https://www.huawei.com/uk/industry-insights/technology/5g-security-architecture-white-paper

Third, open, transparent certifications by third party organizations help ensure that our customers' trust is well placed. As part of a set of arrangements between Huawei and the UK Government, we opened the Huawei Cyber Security Evaluation Centre (HCSEC) in 2010. In 2014, we set up the HCSEC Oversight Board (OB) with members from the UK Government, Huawei, and UK operators. The Oversight Board is tasked with ensuring the centre's independence, competence, and overall effectiveness.

The most recent report by the OB continues to recognize the significance of the HCSEC as an effective security assurance mechanism. The report notes, "The assurance model including HCSEC is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector." To date, HCSEC's evaluations have not detected any malicious vulnerabilities or threats in our products or solutions.

Huawei actively seeks Common Criteria security certification for our products and solutions. This allows independent third-party testing agencies recognized by the Common Criteria Recognition Arrangement (CCRA) to test Huawei products. In addition, the CFI Group, a US-based third-party customer satisfaction research organization, performed an independent analysis of findings from 177 major operators and 123,000 respondents worldwide. According to their report, Huawei's products performed significantly better than all other major providers of telecoms equipment in terms of system stability, reliability, and customer satisfaction. [1]

Cyber security requires an open, progressive, and collaborative approach involving all stakeholders from all countries worldwide. Huawei is a major contributor to industry development and we actively promote shared success. We are creating a robust network of open labs and security labs, and are working with leading partners to take the quality of our products to new levels.

Q2: How do you respond to actions being taken over foreign involvement in communications networks by other nations, such as the UK's 'Five Eyes' allies?

Some Five Eyes countries have indeed taken measures to restrict Huawei's business activities. However, some of these restrictions have been exaggerated or even misinterpreted by the media. For example:

- To date, Canada has not taken any restrictive measures against Huawei products.
- In New Zealand, the government turned down a single 5G proposal submitted for review by one carrier, but the regulatory process is still ongoing.
- Australia has raised extra requirements for the supply of 5G products, but Huawei remains a major network equipment provider in the country.
- Even in the US, existing legislation only restricts the use of federal funds to buy our networking hardware and services; there are no legislative restrictions on Huawei's business activities.

We continue to actively engage with policymakers, customers, and partners in these countries.

We believe that excluding a certain country or vendor does nothing to help effectively manage cyber security. On the contrary, it only serves to create a false sense of security. If banning Huawei from networks would rid the world of cyber security issues, we would certainly be willing to make that sacrifice. But that is not the case.

The ICT industry relies heavily on a global supply chain. A public report published by the US Government Accountability Office (GAO) in 2012 describes a simple laptop

---

[1]Please refer to the letter "Huawei Telecom Equipment's System Stability and Reliability Having an Excellent Track Record with Customer Satisfaction" attached as appendix.

computer with components sourced from 18 different companies. All major telecom equipment vendors have R&D and manufacturing centres in China, and products from these centres are sold around the world, including in Five Eyes countries.

Only one-third of materials used to make Huawei products are sourced in China. The rest are from other parts of the world. Cyber security risks in the ICT supply chain come from the overlapping nature of the chain. The name of one vendor or another stamped on equipment packaging is not indicative of any sort of threat.
In fact, security threats typically don't come from equipment vendors, but from bad actors that exploit vulnerabilities. Equipment vendors are the first line of defence against these bad actors. We believe regulatory policy should encourage equipment vendors and the industry as a whole to transparently share cyber security-related information and jointly safeguard cyber security.

Q3: How do you intend to respond to the HCSEC Oversight Board's latest annual report?

The Huawei Cyber Security Evaluation Centre (HCSEC) – a collaborative arrangement between Huawei, the UK Government, and UK operators – is a key part of our end-to-end global cyber security assurance system. Its goals are to (1) enable open, transparent collaboration between Huawei, the UK Government, and UK operators on cyber security issues; (2) more effectively manage potential security risks; and (3) help Huawei make continuous improvements to its management and technological capabilities as they apply to cyber security.

Huawei welcomes the Oversight Board mechanism. The latest Oversight Board report confirms that the collaborative approach adopted by Huawei, the UK Government, and UK operators is working as designed, meeting its obligations and providing unique, world-class network integrity assurance through ongoing risk management. The report concludes that HCSEC's operational independence is both robust and effective. The latest Oversight Board Report also identifies some areas for improvement in our engineering processes, and we are working to address them.

Cyber security remains Huawei's top priority, and we will continue to actively improve our engineering processes and risk management systems. At our most recent board meeting, we officially signed off on a companywide transformation programme for our software engineering capabilities.

The company will initially invest US$2 billion over the next five years to comprehensively improve our software engineering capabilities. This will help ensure that our products are better prepared for a more complex security environment both now and in the future.

This program is part of a broader effort to redesign our Integrated Product Development process. Technology and networking environments are evolving. Customer and societal expectations for technology are evolving too, as are regulatory requirements. In recognition of these changes, we too are evolving our processes.

It is true that Huawei's software engineering has room for improvement. It is also true

that the operational quality and performance of our products on live networks are top in the industry. Further efforts to improve our software engineering capabilities will help us to maintain a leadership position in the industry and continue providing our customers with more reliable and secure products and services.

Modern communications networks are complex systems that keep evolving in new and innovative ways. Enhancing our software engineering capabilities is like replacing components on a high-speed train in motion. It is a complicated and involved process, and will take at least three to five years to see tangible results. We hope the UK Government can understand this.

Huawei is the only major telecom equipment vendor in the world that has voluntarily embraced such high-level scrutiny from governments around the world. We believe that policymakers should encourage equipment vendors to collaborate with regulators in a more open and transparent way. This will help all parties more effectively identify and mitigate risks. A more encouraging approach is the best way to drive more companies – and the industry as a whole – to engage in constructive public-private partnerships.

Q4: To what extent could Huawei be compelled to assist Chinese national intelligence work using its UK-based hardware or software, or information gathered in the UK?

First, Huawei has never and will never use UK-based hardware, software, or information gathered in the UK or anywhere else globally, to assist other countries in gathering intelligence. We would not do this in any country.

Huawei is a closely watched company. We have 180,000 employees and tens of thousands of partners, and we are subject to extensive regulatory oversight in numerous countries around the globe. Were Huawei ever to engage in malicious behaviour, it would not go unnoticed - and it would certainly destroy our business. For us, it is a matter of security or nothing; there is no third option. We choose to ensure security.

Second, we are aware of concerns about China's National Intelligence Law. Our clarifications are as follows:

1. Regarding this law, the Ministry of Foreign Affairs of the People's Republic of China has clarified that no Chinese law obliges any company to install backdoors. To confirm this interpretation, we have also sought the opinion of a leading Chinese law firm, Zhong Lun, which has been reviewed by Clifford Chance LLP, a well-respected international law firm based in London. The legal opinion confirms that relevant provisions of the Counterespionage Law, the Anti-Terrorism Law, the Cyber Security Law, the National Intelligence Law, and the State Security Law do not appear to empower PRC government authorities to plant backdoors, eavesdropping devices or spyware in telecommunications equipment. In addition, the relevant provisions of China's National Intelligence Law do not appear to have extraterritorial effect

over Chinese companies' overseas subsidiaries and employees, such as Huawei UK.

2. We would like to reiterate that Huawei has never received any such requests, and in the event that we did receive this type of request, we would categorically refuse to comply with it. Huawei is an independent company, and customer-centricity lies at the heart of all we do. We would never compromise or harm any country, organisation, or individual, especially when it comes to cyber security and user privacy protection. This includes the UK.

3. Article 3 of *China's Criminal Law* stipulates that "any act that no explicit stipulation of law deems a crime is not to be convicted or given punishment". No law in China states that a company can be held criminally responsible for refusing to comply with requests such as those mentioned above, e.g., installing backdoors or disabling customer networks. There are no examples of this in China's jurisprudence, either. Therefore, if Huawei were to receive this type of request and refuse to act on it, we would not be subject to legal penalty.

In closing:

The UK is an important strategic market for Huawei. We are working closely with the UK Government and operators to identify and address any concerns about network equipment deployed in the UK, and will continue to work with our local partners to provide the most advanced next-generation communications infrastructure. We are ready and willing to take on any technical challenges to meet the economic and security needs of the UK. We have full confidence in the UK market, which provides one of the most favourable business environments in the world.

We will continue to honour our five-year commitment (2018 to 2023) to procure 3 billion pounds in the UK. This will serve to enhance joint innovation with our customers and collaboration with local research institutes.

If members of the House of Commons Science and Technology Committee would like more details on this reply, please feel free to contact us at any time. As always, you are more than welcome to visit our headquarters in Shenzhen or review our research programs in the UK.

Yours sincerely,

Ryan Ding

President, Carrier Business Group

Huawei Technologies Co. Ltd.

CFI Group
Claes Fornell International

Huawei Telecom Equipment's System Stability and Reliability Having an Excellent Track Record with Customer Satisfaction

As a professional third-party market research company, CFI Group (founded by Professor Claes Fornell from University of Michigan) has independently carried out the satisfaction survey on Huawei's carrier customers. Using their patented technology and top research experts, CFI Group uncovers the business drivers and financial impact of carrier experience for Huawei to deliver better service.

According to CFI 2016-2018 customer satisfaction survey and analysis results, Huawei telecom equipment has been above the industry average in terms of system stability, reliability and overall customer satisfaction for three consecutive years.

- Huawei dominantly leading the competitors in "System stability and reliability": For the recent 3 years, Huawei scored on average 15 points higher than the competitors in the global markets while 5.3 points higher in Western Europe.
- Carriers' overall satisfaction towards Huawei is significantly higher than the competitors: For the recent 3 years, Huawei scored on average 14.9 points higher than the competitors in the global markets while 4.9 points higher in Western Europe.

Note：

① About Huawei customer satisfaction survey: taking 2018 as an example, the survey covers 177 key accounts worldwide and 12,300 customers participated in this survey. Benchmarking competitors include Ericsson, Nokia, ZTE and Cisco.

② About CFI Group: The CFI Group was founded by Claes Fornell, a tenured professor at the University of Michigan's business school. Hailed as the "Father of Customer Satisfaction" and as one of the most influential scholars in marketing science today, he has established the ACSI (American Customer Satisfaction Index) in 1998. The ACSI has a close correlation to the Fortune 500 companies' profit growth, with the profit growth lagging behind the ACSI by 12 months (http://www.cfigroup.com.cn/acsi.htm), and is widely used in customer satisfaction measurement by the telecom operators and equipment manufacturers, such as Ericsson, VDF, etc.

CFI Group
January 27, 2019