SEPTEMBER 13, 2012

INVESTIGATION OF THE SECURITY THREAT POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE

UNITED STATES HOUSE OF REPRESENTATIVES, PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED TWELFTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

COMPILED FROM:

- *http://intelligence.house.gov/hearing/investigation-security-threat-posed-chinese-telecommunications-companies-huawei-and-zte-0*

Opening Statement for Chairman Rogers

Hearing on Threat Posed by Chinese Telecommunications Companies

September 13, 2012

As Prepared

- We invited these companies today as part of our ongoing investigation into the threat posed to the United States by telecommunications equipment manufactured by companies with believed ties to the Chinese government.

- Huawei and ZTE have become dominant global players in the telecommunications market leaving the world increasingly dependent on their telecommunications goods and services.

    - They do not yet dominate the U.S. market, but they seek to expand their footprint here.

    - They reap the benefit of billions of dollars in Chinese government financing, and nicely implement Beijing's explicit desire to be dominant in what China calls a "strategic sector."

    - We have heard reports about backdoors or unexplained beaconing from the equipment sold by both companies. And our sources overseas tell us that there is a reason to question whether the companies are tied to the Chinese government or whether their equipment is as it appears.

    - We have heard reports about their attempts to steal the tradesecrets of other companies, which gives them a competitive advantage and makes us question their ability to abide by any rules.

- At the same time, Chinese intelligence efforts against the United States are growing in scale, intensity, and sophistication.

    - Chinese actors are also the world's most active and persistent perpetrators of economic espionage.

- U.S. firms and cybersecurity specialists speak about an on-going onslaught of sophisticated computer network intrusions originating in China, that are almost certainly the work of, or done at the backing of, the Chinese government.

- Chinese intelligence services and private companies often use Chinese citizens with direct access to corporate networks to steal trade secrets and other sensitive proprietary data.

- Americans have become increasingly dependent on computer networks for every aspect of our lives. Our personal information, our banking information, our transportation infrastructure, medical records, education systems, and government all depend on computer networks.

- We must have trust and confidence in these networks. But those networks are already under attack. As General Alexander, head of U.S. Cyber Command, has recently explained, the U.S. has experienced a 17-fold increase in cyber attacks between 2009 and 2011.

    - Defending against the risk of cyber attacks becomes a bigger challenge when the system itself cannot be trusted. When the equipment and software is provided by companies we cannot trust, then we must constantly worry whether our systems our going to work against us.

    - A sophisticated nation-state actor like China has the motive to tamper with the global telecommunications supply chain, and the United States is a significant priority.

        - The ability to deny service or disrupt global systems allows a foreign regime the opportunity to exert pressure or control over critical infrastructure on which our country depends.

        - The ability to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that assists China's place in the world.

    - Huawei and ZTE provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems. And under Chinese law, ZTE and

Huawei would likely be required to cooperate with any request by the Chinese government to use their systems or access for malicious purposes.

- When vulnerabilities in the equipment, such as backdoors and malicious code, can be exploited by another country, it becomes a priority national security concern.
    - Every piece of this equipment, every code of software, every update, provides that country a means to act against the United States.
    - We must trust our systems if we hope to fulfill the government's most-basic duty to maintain a defense against potential foreign aggression.

- We must get to the truth and see if these companies are tied to or influenced by the Chinese government; whether they provide a means for further economic and foreign espionage by a foreign nation-state known to be a major perpetrator of cyber espionage.

- In February 2011, Huawei issued an open letter to the U.S. government requesting a full investigation into its corporate operations to try to convince us that there is no threat.
    - We decided to give Huawei that investigation.

- In the course of the investigation, the Committee has been disappointed that the companies provided little actual evidence to ameliorate the Committee's concerns.
    - In particular, they did not provide documentation supporting or confirming their claims about their formal relationships or regulatory interaction with Chinese authorities, corporate structure, ownership, operations, or management.
    - We were willing to work with both companies, to find a reasonable way to answer our documents requests. But the companies refused, apparently because to turn over internal corporate documents would potentially violate China's state-secret laws. It is strange the internal corporate documents of purportedly private sector firms are considered classified secrets in China. This fact alone gives us a reason to question their independence.
    - We hope that this hearing finally gives us the opportunity to get fulsome answers and resolve these doubts about your companies.

U.S. House of Representatives
Permanent Select Committee on Intelligence

For Immediate Release:
September 13, 2012

Contact: **Heather Moeder Molino**
Office: (202) 225-7690
Mobile: (703) 615-5371

Chinese Telecommunications Investigation Open Hearing
Opening Statement
Ranking Member C.A. Dutch Ruppersberger
September 13, 2012

Thank you Chairman Rogers. I would like to welcome our witnesses Mr. Charles Ding from Huawei and Mr. Zhu Jinyun from ZTE. Thank you for coming today.

About a year ago, the Intelligence Committee launched an investigation into the threat posed by Chinese-owned telecommunications companies working in the United States. We launched this investigation to determine whether allowing Chinese companies increased access to our U.S. telecommunications market places us at risk for greater foreign espionage, theft of U.S. trade secrets and increased vulnerabilities to our critical infrastructure.

The fact that both companies, Huawei and ZTE, were created and headquartered in China, a country known to aggressively conducts cyber espionage, raises issues. And add to that… the fear that China, a communist country, could compel these companies to provide it information or worse yet spy on Americans using this equipment.

We are concerned about allegations that products from Huawei and ZTE are being subsidized by the Chinese government, so these companies can offer bargain basement prices to unsuspecting consumers. These consumers may have no idea about the national security implications of their purchase. We are looking at all of these issues in our investigation.

In May, I joined a Congressional delegation including Congressman Schiff, Congresswoman Bachmann, and Congressman Nunes on a trip to China where we met with the Chairman of the Board of Huawei and officials from ZTE. We felt it was important to travel overseas to meet with these officials face-to-face and get the facts we need for our investigation. We appreciate the companies meeting with us.

Chairman Rogers and I also sent very detailed letters to Huawei and ZTE requesting a lot of important information, necessary to conduct our investigation. We were disappointed with the lack of direct answers to our in-person questions and vague responses to our letter. We are here today to give them another opportunity to thoroughly and accurately answer our questions.

We already know the Chinese are aggressively:

- Hacking into our nation's networks,
- Threatening our critical infrastructure and
- Stealing secrets worth millions of dollars in intellectual property from American companies.

In fact, the United States Cyber Command estimates $300 billion worth of trade secrets are stolen every year. This jeopardizes our national security and hurts U.S. competitiveness in the world market, costing our country countless jobs and money. As you can see, this is not "political jousting" or "trade protectionism masquerading as national security," we are doing this for very valid reasons.

According to a report recently released by the National Counterintelligence Executive, 6 of the 7 cases prosecuted in 2010 under the Economic Espionage Act involved a link to China. No matter how you do the math, the economic damage from the theft of intellectual property is unacceptable. In addition, the possibility that under current Chinese law even privately owned companies can be compelled to provide information to the Chinese government is even more concerning.

On this issue, other nations have already taken action. Australia recently excluded Huawei from competing on certain contracts dealing with their National Broadband Network. The United Kingdom has implemented costly security procedures for their Huawei equipment. In addition, the European Union is considering additional investigations into Chinese telecommunications companies and considering possible restrictions.

In my role as a leader of the Intelligence Committee, I believe we also have an obligation to protect the national security framework of the United States. That is why we are holding this hearing today and conducting this investigation.

I thank our witnesses from Huawei and ZTE for coming here today and I hope they will answer our questions directly. We look forward to a thoughtful and cooperative dialogue so we can get a better understanding of how these companies operate.

Thank you. Mr. Chairman, I yield back.

########

WRITTEN STATEMENT FOR CHARLES DING

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

U.S. HOUSE OF REPRESENTATIVES

September 13, 2012

Chairman Rogers, Ranking Member Ruppersberger, and Members of the Committee, my name is Charles Ding. I am a Corporate Senior Vice President of Huawei. We at Huawei hope that its participation on this panel is helpful as you pursue your important mission of addressing issues relating to cyber security.

Huawei's Growth Into A Global Company

I have had the privilege to watch Huawei grow from a small start up to a large, multinational organization. We have enjoyed enormous growth for the past 25 years. While we value innovation and entrepreneurship, most of all, we value integrity.

Huawei is an independent, employee-owned company that operates in more than 140 countries. About 70% of our revenue comes from overseas markets. Thanks to our employees' unflagging efforts and our

customer-centric strategy, Huawei has become the second largest provider of carrier network infrastructure in the world and was ranked 351 in the Fortune Global 500 list in 2011. We are proud that Huawei was recognized by Business Week as the most influential company in 2008 and that we won the Economist's Innovation Award in 2010. Huawei has established business relationships with the majority of the top 50 telecom carriers around the world, including Vodafone, British Telecom, France Telecom, Deutsche Telekom, and Telefónica.

In the beginning, as a start-up company, we focused on an underserved market -- rural areas in China. We were the first equipment vendor to establish a sales and service network that covered over 300 regional networks. By 1998, we were able to expand into urban markets in China. By the end of 2000, our revenue had reached $1.9 billion, and we employed 17,320 people.

We experienced our most substantial growth between 2000 and 2012. We were able to expand internationally and significantly grow our business. We won our first major European contract in 2005. Our revenue grew from $1.9 billion in 2000 to $32.4 billion in 2011. And we have expanded from primarily wire line products into mobile, software, core network, and device product lines.

Because of the hard work of our employees and our customer-centric strategy, Huawei has achieved significant success. Moreover, our success is attributable to four key factors.

(1) The explosive growth in the global telecommunications market in China and globally. For example, from 1990 to 2000, fixed line subscribers grew 15 times and mobile subscribers grew 500 times in China.

(2) We have invested significant resources in R&D and have a large R&D work force in China and India. Huawei employs 65,000 dedicated R&D engineers, the most in the industry.

Today, Huawei is the largest patent holder in China. Over the past decade, Huawei has invested more than $15 billion in R&D and has filed more than 50,000 patent applications. Huawei also pays for the use of the intellectual property of others and has paid more than $1.2 billion in royalty fees.

(3) Since 1997, we have relied on advice received from Western consulting firms like IBM and Accenture to reengineer all of our business processes. In fact, in the last five years we have invested over $400 million in management transformation.

(4) Our shareholding structure allows us to attract and retain talented employees. In 1997, Huawei established an Employee Stock Ownership

Program, or ESOP. We grant stocks to high-performing employees. Each year, Huawei determines the number of shares an employee may obtain, based on that employee's job level and contribution to the company. As of December 2011, we had 65,596 shareholding employees.

The ESOP encourages entrepreneurship and hard work-- the backbone of Huawei's success. The ESOP also has allowed Huawei to obtain a substantial amount of capital funding.

Huawei is entirely owned by its employees. No third party -- including government institutions -- has any ownership interest in Huawei. Huawei's success has not been based on favoritism or subsidization by the Chinese government.

Each shareholding employee who is currently employed at Huawei is entitled both to elect and to be elected as a shareholder representative. Such shareholding employees elect 51 people to serve as representatives of the ESOP. Those 51 representatives in turn elect thirteen people to serve as members of the Board of Directors and five people to serve as members of the Supervisory Board.

The current 51 ESOP representatives were elected in December 2010. Of those 51 representatives, 10 joined Huawei right after they graduated. Two of those representatives (Ren Zhengfei and Wang Kexiang) have served in the military. None of the 51 representatives has held a position

at a government agency. The current members of the Board of Directors and the Supervisory Board were elected by the new 51 ESOP representatives in January 2011. Huawei provided background information as to each current member of the Board of Directors and Supervisory Board in its answers to the June 12 letter request.

These factors have allowed Huawei to become the $32 billion company it is today.

Cyber Security Is Vitally Important

Huawei recognizes the vital importance of cyber security, which is a complex, global issue. The focus should not be confined only to companies head-quartered in China. Other companies -- Alcatel-Lucent, Nokia Siemens Networks, Ericsson, and Cisco-- have substantial operations in China, and much equipment used in U.S. networks is developed and manufactured in China.

Since cyber security is a global issue that the whole industry has to face, governments and the whole industry should work together to improve cyber security.

Ensuring cyber security is essential for Huawei's customers. It is also good for our business. Huawei intends to continue as a leading world-wide supplier of telecommunications equipment and services. As a global company that earns a large part of its revenue from markets

outside of China, we know that any improper behavior would blemish our reputation, would have an adverse effect in the global market, and ultimately would strike a fatal blow to the company's business operations. Our customers throughout the world trust Huawei. We will never do anything that undermines that trust. It would be immensely foolish for Huawei to risk involvement in national security or economic espionage.

Let me be clear -- Huawei has not and will not jeopardize our global commercial success nor the integrity of our customers' networks for any third party, government or otherwise. Ever.

Huawei has taken substantial steps to improve cyber security. As a crucial company strategy, it has created and implemented a respected end to end global cyber security assurance system. It has hired as its Global Cyber Security Officer John Suffolk, the former Chief Information Officer of the United Kingdom (U.K.) government, who is in charge of Huawei's cyber security strategy and manages and supervises its implementation.

In addressing the requirements of cyber security, we have built best practices into all of our policies and processes. In this way, cyber security is not an afterthought. Instead, it is the way we conduct our daily business - it is part of our DNA.

At Huawei, we adopt the “many eyes” and “many hands” approach to ensure transparency and security. We positively encourage audits, reviews and inspections of all technology vendors, including Huawei, in a fair and non-discriminatory manner. Each audit and review enables each company to challenge its thinking, policies, and procedures, which in turn will enhance its capability, product quality, and product security. At Huawei, we have already gone the extra mile in this respect.

Huawei proposes that governments and industry leaders come together to develop a global framework for cyber security assurance. Huawei would welcome the opportunity to develop a program in coordination with the U.S. government to address cyber security here.

Huawei Is Independent

Like any corporation, Huawei complies in good faith with the laws, rules, and regulations of the governments in the countries where it does business. Thus, Huawei complies with the laws, rules, and regulations of the Chinese government. However, the Chinese government has no influence over Huawei’s daily operations, investment decisions, profit distributions, or staffing. Nor does the PLA. As previously stated, neither the Chinese government nor the PLA has any ownership interest in Huawei.

We manufacture only products consistent with civilian communications standards. Huawei does not engage in customized R&D or production for military purposes. And as already observed, neither the Chinese government nor the PLA is involved in Huawei's business decisions.

As discussed above, Huawei raises significant funds through its ESOP, such that Huawei is primarily self-funded. That said, Huawei supplements its resources with commercial bank loans, subject to market driven loan conditions. All of the terms and conditions of Huawei's bank loans are based on business negotiation and follow market practice, in compliance with Chinese and international financial regulations. Huawei has financing agreements with 10 Chinese banks and 23 international banks. Huawei is a strategic customer of many international banks, including HSBC, Citi, and SCB.

Huawei has an excellent credit record, without any loan default or waiver history. KPMG has been Huawei's independent auditor since 2000. Huawei's financial liabilities are a small fraction of its total assets and have little effect on its business operations.

Customer financing is a common practice across the telecommunications industry. Customers may contact Huawei seeking help in locating financing for their purchases of Huawei's products;

alternatively, financial institutions may contact Huawei seeking to provide credit support for procurement by Huawei's customers. We may then either refer the customer to a financial institution, or refer the financial institution to a customer. The financial institutions will evaluate project risks in accordance with their internal credit policies and approval procedures and make independent decisions whether to extend loans to the customers and on what terms. To the best of Huawei's knowledge, the financial institutions determine the financing plan in accordance with standard loan processes. The financial institutions also independently and directly negotiate the financing agreement terms with the customers.

Huawei In The United States

Huawei has been in the U.S. for 10 years. We have 1700 employees here. Over the last decade, Huawei has been committed to bringing our innovative products and services to U.S. customers, and to enabling U.S. citizens to have the same access to our high-quality communications services as do more than 3 billion people in other parts of the world. For example, we have introduced our world-leading distributed wireless products to the U.S., which can significantly improve network performance and reduce energy consumption. We are fully aware that, in a high-end market like the U.S., we can only win customers' trust and sustain our development by providing high-quality products and services.

We are striving to become a model investor, employer, tax payer, and corporate citizen in the U.S. In 2011 alone, Huawei procured $6.6 billion of goods and services from US companies. Huawei has invested approximately $500 million in the U.S. in the last five years.

We are committed to openness, transparency, and cooperation so that people get to know Huawei better. We strive to establish good relationships based on mutual trust with customers, governments at all levels, and other sectors of society. Our goal is to create value for customers and for the broader communities in which we operate.

Although we want to expand our presence in the U.S. and thus create more employment and growth opportunities, we have been hindered by unsubstantiated, non-specific concerns that Huawei poses a security threat. We have respectfully asked HPSCI to provide us with any allegations it has that Huawei has engaged in national security or economic espionage. HPSCI has not responded to this request. If HPSCI has specific allegations that Huawei has engaged in cyber espionage, we ask it again to tell us, so that we will have the opportunity to respond and specifically address any concerns the Committee may have.

Huawei's Response To HPSCI's Requests For Information

We recognize that the Committee has been critical of Huawei's answers to the June 12 letter request. We have two main responses to that criticism.

(1) Prior to the June 12 letter request, Huawei provided the Committee with a wealth of information, including very detailed written information about the company. We also have spoken with the Committee at length, in three different sessions. We welcomed the Committee into Huawei's facilities in China and made our top executives, including our president and CEO, available to talk with it.

(2) Huawei did not fully respond to the June 12, 2012 letter request for several reasons. It was literally impossible, particularly in the three week time frame provided for response, for Huawei to respond completely to the sweeping requests in that letter. For instance, demands for "all documents" regarding numerous subjects from Huawei's worldwide locations were logistically impossible to fulfill. These requests sought hundreds of thousands of documents and required that each document not in English be translated. To respond fully would have been exceedingly burdensome. The requests also sought highly sensitive, proprietary business information, which, we respectfully submit, no responsible company, foreign or domestic, would voluntarily produce.

Huawei truly seeks to cooperate with the Committee. That is why I am here voluntarily to answer your questions. Indeed, I believe that the witnesses here today are the first representatives of major Chinese corporations ever to testify before a congressional committee in the U.S. But Huawei must cooperate in a way that protects its legitimate interests and those of its business partners, just as a similarly situated U.S. based company would protect such interests.

Huawei is committed to the U.S. market, the single largest telecom market in the world. Over the past decade, we diligently invested in the U.S. In the next decade, we hope that Huawei can integrate into the U.S. market. We hope that the U.S. information and communications technology industry will prosper with Huawei's participation. We also hope that the American people can enjoy faster network speed and better user experience by using our world leading technologies. We look forward to a productive discussion about the global issue of cyber security today and in the future.

September 11, 2012

中兴通讯股份有限公司
ZTE CORPORATION.
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen, P.R.China
Tel：86-0755-26770000
Fax：86-0755-26771999 Postal Code：518057
http://www.zte.com.cn

Mr. Chairman, Ranking Member Ruppersberger and Honorable Committee Members,

My name is Zhu Jinyun, ZTE's Senior Vice President for North America and Europe. I have a supporting written statement that I urge be included in the record along with my full statement.

I am pleased to appear today to represent ZTE, one of the world's remarkable companies, operating in 140 countries before one of the most important committees in the United States Congress. When I started my career as a young engineer in a corner of China called Shenzhen, I never dreamed I would have an honor like this one.

I had the pleasure of hosting a meeting for your staff in Shenzhen on April 12 and to meet with several of you for a briefing in Hong Kong on May 23. I hope someday you will have the opportunity to visit Shenzhen, and see what a miracle it has become.

To understand ZTE, it is useful to understand Shenzhen. Thirty years ago Shenzhen was a fishing village of about 300,000 people. Today Shenzhen is China's high tech center, much like Silicon Valley, with 14 million residents, most under 30 years old. When you visit Shenzhen, you will feel optimism and hope, freedom and creativity. It is in the air.

The spirit of Shenzhen was born when China's government chose Shenzhen to be the first of four Special Economic Zones (SEZ's) in 1979. The Shenzhen SEZ was created to be an experimental center for free market companies. Today, Shenzhen is home to many of China's most successful high tech companies, including ours; and the Shenzhen Stock Exchange has over 17 million registered investors. When one recalls that, in 1979, everyone worked for the state or an SOE and there were no private companies, Shenzhen's success is impressive.

The concept of the Shenzhen SEZ seems obvious today, but it was revolutionary in 1979. Allow risk takers to develop companies on the free market model. Find out if they could stand on their own and serve people better. Learn whether Chinese companies, for the first time, could change the way China does business.

ZTE's founder and Chairman, Mr. Hou Weigui, was a young engineer at the time, working in China's aerospace sector on general purpose integrated circuit work. He

and six fellow engineers saw the Shenzhen SEZ's unprecedented potential and they leapt at the chance to join in this bold experiment. They left their secure positions and embarked on this new enterprise. They were pioneers. They had no stable income, but they had a vision.

That vision was that they wanted to provide universal telecommunications service to China's undeveloped and rural areas.

This was Mr. Hou's commercial vision, not something imposed or mandated by China's government. And, from the start, he and his team saw it as a private commercial enterprise. In 1985, they launched their company with an investment of 2 million RMB (about $300,000) from three investors, notably a foreign investor from Hong Kong, and set about designing their switch. They supported their research with revenue from contract work for a trading company in Hong Kong.

For the next ten years, we had success in China's rural market. In 1987, we launched our first switch, the ZX60, developed many more over the years and won national respect for our product quality. Mr. Hou's vision was broader and in 1996, he and his team decided to pursue diversified products, serve urban and international markets. This growth plan required capital, and, in 1997 ZTE became the first Chinese telecom company to list on the Shenzhen Stock Exchange.

I grew up in rural China, and like many of my colleagues, attended college, and I joined ZTE in 1998. We wanted to be part of something new and innovative. My first assignment with ZTE was to help develop our next technology – CDMA wireless systems. It was a great time for a young engineer to join ZTE. I knew ZTE's business model was focused on engineering, R&D, innovation. The company was making unprecedented moves, including becoming the first Chinese company to enter into a licensing partnership with Qualcomm – and ZTE remains one of Qualcomm's leading partners to this day. And ZTE was expanding into diversified advanced technologies including development of a mobile communications system for China and around the world.

My first project team was six people. By 2000, we had 900 people working on CDMA wireless systems. We wanted to compete in the China market which remained dominated by giant Western vendors. Even 15 years after our founding, it was still necessary for ZTE to show China's network carriers that our solutions could be trusted. We were able to serve only about 7% of China Unicom's wireless customers, with the balance distributed among Western vendors. But, as a consequence, we became the first Chinese company manufacturing CDMA wireless systems.

Once again, ZTE won a reputation for the quality of its products in the China market. Starting with a simple circuit switch, we had built a core network and applied it to CDMA. That was state of the art product development. We engineers were quite happy that our internal designs actually worked. Our commitment to innovation and product development had paid off. When the world telecom equipment market suffered

a downturn in the early 2000's, ZTE's CDMA wireless systems were in demand and helped carry us through.

Of course, Mr. Hou's vision was global. In 2004, ZTE became the first Chinese company listed both on the Shenzhen and Hong Kong Stock Exchanges.

I was assigned to help develop international markets for our CDMA RAN products. We already had learned to compete in China's developing market. Partnering with Qualcomm, we logically identified India, Africa, and other developing markets for our equipment. Over time, ZTE's wireless equipment platforms have integrated every technology from GSM, to CDMA, to WiMAX, to 3G, LTE and beyond. Our 3G capability carried us through the 2009 economic crisis. Innovation and quality have served ZTE well.

ZTE is a free market success story built on innovation: to supply unserved markets and to help pioneer next generation technologies. And, relevant to your inquiry, ZTE's path has never been government-directed. ZTE started as, and remains today, a company of telecom equipment engineers who pursue commercial opportunity and social responsibility in product innovation. In fact, importantly, *Fortune* magazine ranks ZTE number two among China companies for global corporate social responsibility in 2012.

ZTE started out as a private company with some SOE investment. Today ZTE is owned by over 140,000 public shareholders, including many of the world's leading institutional investors. ZTE is regulated on two stock exchanges, and SOE investment has been reduced to 15.68%. ZTE's Board and management are fully devoted to serving the interests of our 140,000 public shareholders. And, because most of ZTE's business is mostly international, ZTE must comply with laws in countries throughout the world.

While ZTE appreciates its position in China's expanding telecom market, ZTE is focused on its success as a multinational company. ZTE is not an SOE or government controlled. Indeed, ZTE is China's most independent, transparent, globally focused, publicly traded telecom company.

Being a global publicly traded company naturally imposes a set of broadly recognized responsibilities and business norms. ZTE's cooperation with this Committee's investigation is one example. In our view, ZTE has set a new precedent for cooperation by any Chinese company with a US congressional investigation.

Another important example is the need for multinational telecom equipment suppliers to satisfy recognized equipment standards everywhere they do business. ZTE was the first Chinese company ever to be fully certified under the most important international and US equipment standards, including ISO 27001 and NIST FIPS 140-2. Not only is ZTE and its equipment fully certified by the leading standards-setting organizations, ZTE actively participates in these organizations, helping to lead the way

in advancing standards-setting throughout the world, including cyber protection standards.

I am aware of testimony, presented to Congress earlier this year, in which the leading cyber protection experts in the US Defense Department and Department of Homeland Security have advised Congress that the most effective cyber protection is universal application of these equipment standards and Trusted Delivery Models. Not only is ZTE's equipment certified according to the most advanced standards, ZTE has offered a state of the art Trusted Delivery Model to US telecom equipment purchasers since 2010. Today, ZTE has in place a Trusted Delivery Agreement with a highly regarded independent US security assessment laboratory, Electronic Warfare Associates (EWA), which provides assurance to any US carrier purchasing ZTE telecom infrastructure equipment that the equipment will be tested continuously throughout its life cycle.

The reason experts rely upon Trusted Delivery Systems for cyber protection is that, with a reliable Trusted Delivery System, the equipment can be trusted no matter who the supplier is. Trusted Delivery Systems are vendor-neutral. Also, Trusted Delivery Systems have the same effect as highway speed cameras: they deter illegal activity. ZTE is in the vanguard of supply chain risk management and Trusted Delivery.

Given all that ZTE is doing to promote cyber security, the Committee's inquiry whether ZTE may pose a threat to critical US telecom infrastructure is very disturbing for us, as you must expect. The Committee's central question has been: would ZTE grant China's government access to ZTE telecom infrastructure equipment for a cyber attack?

Mr. Chairman, let me answer emphatically: no! China's government has never made such a request. We expect the Chinese government never to make such a request of ZTE. If such a request were made, ZTE would be bound by US law.

ZTE is committed to helping this Committee and its partners in Government and industry to promote cyber security through our cooperation here and in the future. Let me raise a concern about some legislative proposals that have been proposed recently.

Your Committee has suggested there are risks in US network carriers' purchases of telecom operating equipment from foreign vendors, particularly vendors in China. As the Committee undoubtedly understands, virtually all of the telecom equipment now sold in the United States and throughout the world contains components made, in whole or in part, in China. That includes the equipment manufactured and sold by every Western vendor, much of which is made by Chinese joint venture partners and suppliers.

We respectfully suggest that the Committee's focus on ZTE, to the exclusion of the Western telecom vendors, addresses the overall issue of risk so narrowly that it omits from the Committee's inquiry the suppliers of the vast majority of equipment used in the US market. ZTE is a relatively small US telecom equipment supplier in

comparison with most of the Western vendors. Sales of ZTE's telecom infrastructure equipment in the United States comprised less than $30 million in revenue last year. Two Western vendors, alone, last year provided the US market with $14 billion dollars' worth of equipment.

ZTE should not be a focus of this investigation to the exclusion of the much larger Western vendors.

We urge the Committee to consider a serious concern with several pending legislative proposals designed to exclude Chinese equipment suppliers, directly or indirectly, from the US market. One proposal would exclude the companies named in this inquiry explicitly. Others would exclude any Chinese suppliers with "ties" to China's government

Respectfully, neither proposal would protect US national security as comprehensively as implementation of the Trusted Delivery System ZTE offers US carriers. Proposals that specific Chinese companies be excluded from the US market, either directly or indirectly, would constitute obvious unfair trade practices and are so narrow that they would provide no meaningful solution in support of US cyber security.

Proposals based on China government "ties" suffer from the opposite problem. While the word "ties" is undefined, it presumably is meant to be applied broadly. If so, it is readily foreseeable that every supplier of US telecom infrastructure equipment – including the Western vendors and their Chinese manufacturing partners – would be found to have "ties" to China's government. If every vendor with "ties" to China's market is excluded from the US market, where will US carriers purchase telecom infrastructure equipment?

US chip set suppliers have advocated that Congress not adopt these exclusionary measures because they would disrupt supply relationships with Chinese equipment purchasers that are vital to the US economy. ZTE alone has purchased over $14 billion in US equipment in recent years, indirectly creating over 20,000 US jobs. We expect to make even larger purchases going forward. Market exclusion proposals are counter-productive, particularly when reliable, more effective solutions are readily available.

Responsible federal agencies and US telecom carriers have increasingly come to recognize that Trusted Delivery Systems render telecom equipment trustworthy regardless of who the supplier is. Respected international commentators have come to the same conclusion.

For example, on August 4, *The Economist* published an editorial making the following points.

- Just about everybody now makes telecom equipment in China;
- Banning Chinese telecom suppliers is no guarantee of national security;

- The answer is to require greater scrutiny of everyone, not just the Chinese firms;
- Governments should ensure telecom equipment is secure no matter who makes it; and
- This will protect networks; banning companies will not.

The Economist supports the Trusted Delivery Model, and rejects market exclusion, to protect national security.

ZTE's commitment is clear. ZTE is China's most independent, transparent, regulated, globally focused, publicly traded telecom company. We are accountable under legal and social norms everywhere we do business. ZTE's ultimate success depends on our ability to serve as a trusted partner for US telecom carriers. No company has a greater stake in promoting effective US cyber security than ZTE.

And we are readily equipped to help you achieve real results quickly. Our equipment is certified and we are helping design advanced global cyber security standards. Our end-to-end Trusted Delivery System allows US carriers to use our equipment fully confident it is, and remains, safe.

Mr. Chairman, ZTE respects the Committee's responsibility to protect US national security. We came here this morning because we want to help, with the expectation that the Congress and the United States government will provide ZTE with an open and equal opportunity to compete in the United States. We believe that ZTE is the most transparent publicly owned telecom company in China, and that ZTE is the best choice to work in concert with the Congress and the United States government and to be a trusted partner with US vendors in the formation of a truly global and free market telecom community. I thank you for the opportunity to appear today, and I will be happy to answer any of your questions.