# Submission No 149

## Inquiry into potential reforms of National Security Legislation

**Organisation:** Huawei Technologies (Australia) Pty Limited

# Submission from Huawei Technologies (Australia) Pty Limited (Huawei Australia) to the Parliamentary Joint Committee on Intelligence and Security on the Potential Network Security Reforms

**20 August 2012**

# Equipping Australia against Emerging and Evolving Threats

## About Huawei

Huawei is a privately owned global technology company that operates in over 140 countries. Our technology supports almost half the planet's population.

We employ 150,000 people. We are used by 45 of the world's top 50 telecommunications operators and, as at the end of 2011, our products and solutions had been deployed by more than 500 telecommunications operators in 140 countries.

We are essentially a science and engineering based company: we have 7,500 employees with PhDs and 62,000 employees engaged in research and development. As of 2011 we have 36,344 patent applications filed in China, 10,650 patents filed under the Patent Cooperation Treaty and 10,978 patent applications filed in other jurisdictions. We have been awarded 23,522 patent licenses, 90% of which are invention patents. We have 23 R&D centres around the world, 34 joint innovation centres with key customers and 45 training centres.

Overall, about 70% of our revenue is generated outside of China.

We source 70% of our materials from non-Chinese companies with the US being the largest provider of components with 32% of our materials sourced through 185 US suppliers. China provides 30% of our components (which are mainly low tech mechanical parts, cables and final assembly), Taiwan 22% and Europe 10%. We source products from Australian owned and/or Australian based suppliers.

Huawei Australia has approximately 900 staff, a local Board of Directors and is working with all of Australia's major operators.

50% of Australians already use at least one Huawei product for their telecommunications needs.

## Executive summary

As a major equipment vendor with a reach in over 140 countries, we are primarily interested in providing a global perspective to the proposal to impose obligations on the Australian telecommunications industry to address security risks (item 16 of the Committee's Terms of Reference).

We appreciate the challenges that the network security reforms are intended to address. We are committed to playing a leading role in cyber-security globally and to ensuring our customers are confident in the integrity and security of our products. We believe our business will grow in a regulatory regime which puts a premium on security – provided that such regulation is applied in a non-discriminatory way.

We believe security outcomes are best delivered by a competitive, well-informed marketplace – so we strongly support the flexible and outcomes-based approach suggested by the Discussion Paper. We believe this model would reflect the importance of competitive and innovative vendors like Huawei in the market and the contributions they make to security outcomes.

Given the commentary surrounding the proposed reforms, we do have concerns that the security standards proposed in the Discussion Paper will be imposed in a way that discriminates against particular vendors, or vendors from a particular country of origin with little or no benefit for security outcomes.

We believe it is essential that any specific requirements imposed are objectively justified, vendor neutral and give affected industry players a genuine opportunity to understand and address specific concerns. We believe the principle of non-discrimination should be clearly set out in any legislative reforms.

Network security regulation which is consistent with non-discrimination and open access to markets is important to achieving security outcomes – it would increase competition, innovation and investment, which are all essential to security. It would:

- increase Australia's access to the latest technologies, foster competition and innovation and result in lower end-user prices;
- improve Australia's competitiveness in the region and globally;
- be the only approach which can be rationally enforced, given the complexity of the global supply chain (for example, the fact that every major telecommunications equipment provider's supply chain structures are similar); and
- support Australia's trade commitments, obligations and relationships.

Finally, we believe that effective reforms should:

- **be flexible and outcomes-based** – noting that network security standards which mandate the use of particular technologies or standards can be quickly rendered inadequate or redundant;
- **address the role of all stakeholders in the security equation** – including Australian and offshore governments, equipment vendors, carriers/CSPs and end users. The complex and globally interconnected nature of today's telecommunications mean that there is a limit to the effectiveness of domestic regulation since much network traffic will be vulnerable to access outside Australia. Accordingly, a broader strategy to work towards "end-to-end" security outcomes is needed;

- **clearly emphasise the need for appropriate risk assessment** – network security threats are growing in number and threats are increasingly unpredictable. We believe that any obligation on carriers/CSPs should be based on what is reasonable and proportionate in the circumstances;

- **not require major business decisions or network designs to be provided to the Government** – this approach is not consistent with an "outcomes based" model and goes significantly further than the notification models adopted in comparable jurisdictions; and

- **have a graduated and proportionate enforcement regime** – as the Discussion Paper notes, there are already relevant enforcement mechanisms and national security provisions in the *Telecommunications Act 1997* (Cth) (**Telco Act**). In our view, only incremental changes to the enforcement mechanisms in the Telco Act are required.

# Introduction

Huawei is pleased to have this opportunity to comment on the Attorney-General's Department's discussion paper, *Equipping Australia against Emerging and Evolving Threats* (**Discussion Paper**).

As a major telecommunications equipment vendor in Australia (rather than a carrier/CSP) we are not in a position to comment on the interception or intelligence gathering issues canvassed in the Discussion Paper. Our submission addresses only the proposal to amend the Telco Act to impose new obligations on the Australian telecommunications industry to address security risks, as set out in Term of Reference 16 (**Network Security Reforms**).

We acknowledge the importance of ensuring telecommunications legislation is sufficient to address growing threats to network security and we welcome the opportunity to contribute to the Network Security Reforms.

We strongly support measures which will create real improvements in the security of Australia's telecommunications networks. We believe a holistic and end-to-end approach to security is required, which addresses the broad range of security threats faced by networks,[1] and does so at each of the infrastructure, services and applications layers. In our view, confidence in the security and integrity of telecommunications networks is in the interests of all players in the Australian telecommunications industry, including the government, noting that:

- vendors are increasingly required by their customers to meet stringent security requirements – particularly as competition in the market intensifies. As a supplier to 45 of the world's top 50 telecommunications operators we understand these competitive pressures well. We are investing significant resources to ensure our products are secure and to assure our customers of this security;

- carriers/CSPs need to demonstrate their networks are safe and secure to win business, particularly in the market for security-conscious government and enterprise customers. This drives carriers/CSPs to require higher security standards from vendors; and

- end users' confidence in the security of telecommunications services and the integrity of telecommunications networks is essential to drive uptake in services. This will be important to realise the Australian Government's strategy of leveraging the digital economy to improve Australia's "*productivity, global competitive standing and improved social wellbeing*".[2]

Simply put, good network security is good business.

However, it is important the Network Security Reforms do not simply amount to additional red tape. They need to be effective in achieving better network security. To be effective, the Network Security Reforms need to focus on actual security risks rather than irrelevant criteria such as the country of origin of a vendor. They must also be proportionate to the regulatory costs imposed on industry (and, indirectly, on end users).

---

[1] These include threats to availability, integrity and confidentiality: ITU-T, *Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications* (10/03).

[2] Department of Broadband, Communications and the Digital Economy, *Australia's Digital Economy: Future Directions* (2009) available at http://www.dbcde.gov.au/__data/assets/pdf_file/0006/117681/DIGITAL_ECONOMY_FUTURE_DIRECTIONS_FINAL_REPORT.pdf.

Our submission is intended to explain how the Network Security Reforms could achieve this objective:

- **Section 1** outlines our view of what effective Network Security Reforms would look like;
- while we are supportive of the proposed Network Security Reforms, **Section 2** outlines some areas where the approach set out in the Discussion Paper could be adjusted to improve the effectiveness of the reforms; and
- **Section 3** outlines Huawei's Cyber Security Global Policy.

# 1 What would effective Network Security Reforms look like?

The security of telecommunications networks is a significant and growing issue both in Australia and worldwide. We support the Australian Government taking steps to address this issue and believe the Discussion Paper sets out a sensible way to proceed. In this section we outline how the Network Security Reforms would most effectively promote improvements in network security – with the ultimate goal of improving confidence in Australia's telecommunications networks to maximise the opportunities created by the digital economy.

## 1.1 Effective reforms should be consistent with thriving competition and open markets

Every carrier, CSP and equipment vendor has a commercial interest in improving the security of their networks and equipment. We believe that competition in the market improves security outcomes and we welcome the Discussion Paper's acknowledgement that the free market creates incentives to ensure networks are secure.[3]

The Discussion Paper notes that competitive neutrality is an "important element" of an effective regulatory system.[4] Indeed, the Discussion Paper recognises the role of a competitive marketplace in achieving security outcomes – but notes that market players may have "incomplete information about the national security environment".[5] This can be addressed by ensuring stronger engagement between the Government and the industry. It is not a matter which should compromise Australia's commitment to open and competitive markets.

Similarly, we note that the security thresholds adopted in the Discussion Paper – "competent supervision" and "effective control"[6] – appear on their face to be competitively neutral. We fully support these standards provided that they will not be used to discriminate against any vendor – including based on their country of origin. To achieve the goal of better network security the Network Security Reforms should be consistent with open competition – and recognise that the most effective and innovative security measures emerge from a competitive environment where carriers, CSPs and vendors are able to compete on a level playing field.

We believe a commitment to competition should be a central tenet of the Network Security Reforms, for the following reasons.

[3] Discussion Paper, p 31.

[4] Discussion Paper, p 34.

[5] Discussion Paper, p 31.

[6] Discussion Paper, p 35–36.

(a) **Security improvements emerge from competitive pressures**

As we note in section 1.2 below, effective end-to-end security outcomes require input from all stakeholders.

As competition among players in the telecommunications sector has grown there is increasing competitive pressure to demonstrate the security and integrity of equipment, software and other components of telecommunications networks. Equally, there is increasing pressure on all stakeholders to introduce additional safeguards to reduce security vulnerabilities.

In the short term, demonstrating the security of their equipment is fundamental for market players to win business. Competition creates pressure to develop innovative security solutions, to identify security weaknesses and to address them as quickly and effectively as possible.

In the long term, promoting confidence in the integrity of telecommunications networks is essential for the industry and to driving growth in the use of telecommunications services. Ultimately the goal of all market players will be to ensure end-to-end security outcomes.

Competition has driven Huawei to invest significant resources in promoting network security and addressing the supply chain through the adoption of standards globally across the industry. In terms of our contribution to industry standards globally, we:

- have joined 132 domestic and international industry standards bodies, including the 3GPP, IETF, IEEE, ITU, BBF, OMA, ETSI, CCSA, and ATIS;
- occupy 180 leadership positions in these forums, including chairpersons of the ETSI, ATIS, IEEE-SA, OMA, TMF, and CCSA, WFA, and W3C; and
- are actively involved in these forums. For example, in 2011, we submitted more than 5,000 standard proposals as part of our engagement with these industry forums.

We have been recognised as a market leader in contributing to global telecommunications network and equipment standards. For example, in 2011 we received the TM Forum's Industry Leadership Award and an Outstanding Contributor Award.[7]

We believe our commitment to security has been a key factor in our commercial success. Network security is critical to network operators. We work with 45 of the world's top 50 telecommunications operators. We have achieved this market position by establishing open and transparent telecommunications solutions that meet the high standards of the world's tier 1 operators.

We also supply equipment for next generation fibre networks in the United Kingdom, Singapore, Malaysia and New Zealand (among others) – and this has often involved significant engagement and investment to

[7] The TM Forum is a global, non-profit industry association focused on enabling service provider agility and innovation. See http://www.tmforum.org/.

ensure our customers and regulators have absolute confidence in the security of our products.[8]

Our success demonstrates the significant efforts we have undertaken in this area – and that we make the necessary investments to satisfy our customers of the integrity of our products. We believe these investments set a new benchmark for security.

A competitive marketplace is essential to spurring market players like Huawei to continue to invest in market-leading security solutions. Preventing a vendor from competing in a market purely because of its country of origin will deprive that market of such security benefits.

It is important to recognise that, for a "technology taker" like Australia, which has only a small local equipment industry,[9] a competitive marketplace requires that all foreign vendors can compete and innovate in the Australian marketplace.

(b) **There is no evidence that "closed" ecosystems or barriers to trade improve security**

In our view, there is no evidence that supposedly "closed" ecosystems which discriminate against vendors from particular countries deliver better security outcomes.

As an example, Huawei does not have a meaningful presence in or market share of US tier 1 carrier networks, yet there is no evidence that this has made any difference to the security of those networks nor is there any evidence that its networks are any more secure than those in the United Kingdom or New Zealand (despite the fact that we have worked closely with major network operators in those countries, including supplying equipment for their next generation fibre networks). On the contrary, threats to US telecommunications networks continue to grow.[10] For example, the number of incidents reported by US federal agencies to the US Computer Emergency Readiness Team increased from 5,503 incidents in 2006 to 42,887 incidents in 2011.[11]

In fact, recent developments in the US suggest that even ardent advocates of national security such as Senator John McCain are moving

---

[8] Huawei, *Huawei Opens Cyber Security Evaluation Centre in the UK* (Press Release, 6 December 2010) available at http://huawei.com/au/about-huawei/newsroom/press-release/hw-u_151000.htm. The centre was developed to test end-to-end solutions (both hardware and software) for its ability to withstand growing cyber security threats and UK government security standards.

[9] An April 2012 IBISWorld report notes that "The Telecommunication, Broadcasting and Transceiving Equipment Manufacturing industry in Australia is constrained by a small local market, a lack of locally sourced components and investment in research and development, and high costs. Industry operators tend to concentrate on small niche markets, which are often outside the radar of large foreign transnational companies": IBISWorld, *Telecommunication, Broadcasting and Transceiving Equipment Manufacturing in Australia: Market Research Report* (April 2012) available at http://www.ibisworld.com.au/industry/default.aspx?indid=266.

[10] In February 2011, the Director of National Intelligence noted that there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009: see United States Government Accountability Office, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure* (Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, 26 July 2011) p 6, available at http://www.gao.gov/assets/130/126702.pdf.

[11] United States Government Accountability Office, *Cybersecurity: Threats Impacting the Nation* (Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, 26 July 2011) p 9, available at http://www.gao.gov/assets/130/126702.pdf.

away from prescriptive regulation which limits competition, and are instead looking to promote information-sharing and to "*leverage the ingenuity and innovation of the private sector*".[12]

(c) **An open vendor ecosystem will maximise the availability of emerging technologies for Australians**

We believe that an open ecosystem is particularly important to ensure Australians have early access to emerging technologies (particularly given the very limited domestic manufacturing industry). Foreign vendors like Huawei are driving innovation – including in security technologies, techniques and solutions. In terms of our contribution to innovation:

- we invest approximately 10% of our revenue in research and development each year;
- our research and development spend for 2011 totalled US$3.76 billion (about 10% of the Australian Government's annual budget) and over the past decade totalled more than US$15 billion. This was achieved through 23 research and development centres worldwide; and
- as of 2011, Huawei had 36,344 patent applications filed in China, 10,650 filed under the Patent Cooperation Treaty and 10,978 filed in other jurisdictions. We have been awarded 23,522 patent licenses, 90% of which are invention patents.

The same applies to other vendors in China: indeed, China has now surpassed the US in terms of total patent filings.[13]

Discriminatory security reforms would limit investment, innovation and the availability of new technologies for Australian consumers, businesses and governments. As noted by the President of the Business Council of Australia:

> *Foreign investment is critical because it underpins our exporting industries, provides access to technology and know-how and makes a vital contribution to innovation*.[14]

Discouraging investment and innovation will ultimately be to the detriment of network security outcomes.

**Accordingly, the best way to promote security is to ensure the Network Security Reforms are consistent with an open, thriving and competitive marketplace.**

## 1.2 Effective reforms would address the role of all stakeholders

As noted above, we understand and support the imperative of protecting national security.

---

[12] Michael S Schmidt, "Senators Force Weaker Safeguards Against Cyberattacks", *New York Times* (27 July 2012) available at http://www.nytimes.com/2012/07/28/us/politics/new-revisions-weaken-senate-cybersecurity-bill.html.

[13] Steve Lohr, "When Innovation, Too, Is Made in China", *New York Times* (1 January 2011) available at http://www.nytimes.com/2011/01/02/business/02unboxed.html .

[14] Tony Shepherd, President, Business Council of Australia, "Chasing the fast boat to Asia", *Sunday Morning Herald* (20 December 2011) available at http://www.smh.com.au/business/chasing-the-fast-boat-to-asia-20111219-1p2dc.html.

However, it is important the Network Security Reforms recognise that effective security involves inputs from many stakeholders – security is a responsibility which needs to be shared between governments, software suppliers, equipment vendors, network operators and end users. Network Security Reforms cannot be effective unless they form part of a broader strategy which addresses the responsibilities of each of these stakeholders in an end-to-end model (and covering security at the infrastructure, services and application layers). As the International Telecommunications Union has recognised:

> *Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution*.[15]

We note that many of the recently reported recent network security breaches in Australia have resulted from human errors or deliberate breaches by internal staff – rather than inherent weaknesses in network architecture or equipment.[16] The Australian Government's Defence Signals Directorate has also indicated that at least 85% of the targeted cyber intrusions that it responded to in 2010 could have been prevented by following just four mitigation strategies, being:

- patching applications;
- patching operating system vulnerabilities;
- minimising the number of users with administrative privileges; and
- "white-listing" applications so that unapproved programs are unable to run.[17]

This suggests that even government users could take basic steps to prevent security intrusions – and that responsibility for security should not lie wholly with carriers/CSPs or vendors.

Further, the globally interconnected nature of today's telecommunications means that there is a limit to the ability of domestic regulation to achieve security outcomes on an end-to-end basis. For example, Australian internet traffic is estimated to grow over four-fold from 2011 to 2016, a compound annual growth rate of 36%.[18] The vast majority of growth is in international connectivity: for example, regionally, international bandwidth requirements grew by 47% between 2007 and 2011.[19] This means that the majority of Australian network traffic will be vulnerable to unauthorised access at a point *outside* Australia and cannot be entirely protected by any reforms enacted by the Australian Government.

In this context, there is a clear limit to the effectiveness of Network Security Reforms which are aimed solely at Australian carriers/CSPs. We recognise that reforms directed at carriers/CSPs are worthwhile and should be pursued.

---

[15] ITU-T, *Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications* (10/03).

[16] See, eg, ABC News, *Medicare privacy breaches 'only the beginning'* (3 March 2010) available at http://www.abc.net.au/news/2010-03-02/medicare-privacy-breaches-only-the-beginning/347648 and ABC News, *Vodafone says security breach a 'one-off'* (10 January 2011) available at http://www.abc.net.au/news/2011-01-09/vodafone-says-security-breach-a-one-off/1899268.

[17] Australian Government Defence Signals Directorate, *Top 35 Mitigation Strategies* (2012) available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm.

[18] Cisco, *VNI Forecast Highlights: Australia* (2012) available at http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html#%7ECountry.

[19] TeleGeography, *International Bandwidth Demand Grows 45 Percent* (18 July 2012) available at http://www.telegeography.com/press/marketing-emails/2012/07/18/international-bandwidth-demand-grows-45-percent/index.html.

However, we suggest that they form part of a broader strategy to address security vulnerabilities on an end-to-end basis. This would include greater inter-governmental co-operation, the further development of global security standards, a greater focus on educating and monitoring access to telecommunications systems and data, promoting a more coordinated approach to security issues by carriers/CSPs and vendors, as well as better end user education.

In our view, the Network Security Reforms should be part of a holistic solution to improve network security standards.

**Effective Network Security Reforms need to form part of a broader strategy which will address the role of all stakeholders in Australia and elsewhere.**

## 1.3 Effective reforms should be dynamic, flexible and outcomes-based

Protecting network security is a dynamic process – it needs to be flexible and allow industry players to quickly respond to new and unanticipated types of security threats.

We agree with the concerns previously expressed by other members of the Australian telecommunications industry that it is not appropriate for the Government to impose prescriptive technical requirements. We therefore welcome the Discussion Paper's preference for an

> *approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it*.[20]

In our view a dynamic, outcomes-based approach has the following advantages.

### (a) Flexible, outcomes-based regulation will be more effective

Detailed and prescriptive regulation is not well suited to the emerging security challenges facing telecommunications networks worldwide. This is because network security standards which mandate the use of particular technologies or standards can be quickly rendered inadequate or redundant.

We note that these same concerns have been expressed in the US. The US Telecommunications Industry Association has noted, for example, that

> *imposing rigid regulatory requirements that by their nature will be unable to keep up with rapidly evolving technologies will require industry to focus on meeting obsolete security requirements rather than the actual threat at hand, which will in effect make critical infrastructures and the customers that they serve less secure*.[21]

### (b) Carriers/CSPs are best placed to identify appropriate compliance strategies

In our view, the Discussion Paper is correct in noting that carriers/CSPs themselves will be best placed to identify the most effective and efficient

[20] Discussion Paper, p 35.

[21] Telecommunications Industry Association, *Innovation White Paper: Securing the Network* (24 July 2012) available at http://www.tiaonline.org/policy/white-papers.

way to achieve compliance rather than Government dictating particular technical solutions to be adopted.[22]

In our experience as an equipment vendor, carriers/CSPs can comply with an obligation to exercise "competent supervision" and "effective control" over their networks (as referred to in section 3.2 of the Discussion Paper) in many ways, including for example through:

- implementing hardware/software solutions;
- taking measures to address personnel risks (such as monitoring of network use and human "checks and balances"); and
- limiting electronic access to sensitive information/data and physical access to network components.

Furthermore, carriers'/CSPs' typical contractual arrangements with vendors will normally include significant technical and security requirements which apply to the vendor's equipment and will provide the carrier/CSP with a full suite of indemnities, suspension and termination rights in the event of a breach by the vendor.

The most appropriate technologies and strategies to achieve security objectives will depend on many factors including the network topology, the existing technology, the costs of the solutions and capital available. Equally, the available solutions will change over time due to market and technological developments. In our view, an outcomes-based approach allows carriers/CSPs to adopt the solutions which are most appropriate for their networks.

**(c) Carriers/CSPs will have increased regulatory certainty, more autonomy over compliance and greater ability to manage costs**

An outcomes-based approach will provide carriers/CSPs with flexibility to achieve the Government's desired outcomes in the most efficient way possible. We believe that that an outcomes-based approach is the only option that complies with the Discussion Paper's principle that the regulatory system "*not be resource-intensive for industry to comply with*".[23]

Finally, we note that carriers/CSPs are familiar with outcomes-based legislation in Australia and that it has been successfully adopted in areas such as interception capability requirements (see further section 2.3 below). We believe outcomes-based legislation is tried, tested and effective.

**We commend the approach proposed in the Discussion Paper; we believe effective Network Security Reforms should reflect a flexible, outcomes-based approach.**

# 2 Refining the Network Security Reforms

While we are supportive of the proposed Network Security Reforms, in our view some aspects of the approach outlined in the Discussion Paper would limit the reforms' effectiveness.

[22] Discussion Paper, p 35.

[23] Discussion Paper, p 34.

## 2.1 Greater emphasis is needed on applying security standards in a technology neutral and vendor neutral way

We note that the Discussion Paper proposes introducing obligations based on the concepts of "competent supervision" and "effective control". We support these as obligations and they appear to be technology neutral and vendor neutral.

However, the Terms of Reference suggest that the Network Security Reforms are intended to mitigate "*the risks posed to Australia's communications networks by certain foreign technology and service suppliers*".[24] In this context, we continue to have concerns about:

- the lack of an unequivocal commitment in the Discussion Paper to security standards being technology and vendor neutral; and
- the risk that apparently neutral standards will be applied by regulators in a way that discriminates against vendors based on their country of origin and not on a proper assessment of security risk.

An important safeguard to ensure the competitive neutrality of any reforms is that affected stakeholders have the opportunity to understand and address specific concerns – rather than being subjected to regulations which are based on rumours and accusations instead of objective evidence and legitimate security concerns.

Application of the apparently neutral obligations of "competent supervision" and "effective control" in a way that discriminates against vendors from a particular country – especially if there is no right of review or response – could significantly affect the ability of those vendors to compete effectively in Australia. In our view, such regulatory risks could also affect the attractiveness of Australia as an investment destination and the willingness of foreign firms to do business in Australia more generally.

### (a) Open access for vendors would be beneficial to network security

We believe open access for vendors would be beneficial to competition and innovation – which would enhance security. As noted in section 1.1 above, thriving competition offers the most compelling incentives for all stakeholders to protect network security. For example, in the highly competitive equipment vendor market security issues play a critical role in establishing a competitive edge. Competition promotes a far greater diversity of products and services, including security products and services.

In Australia we have supplied network equipment to many of Australia's major carriers and we are proud of our reputation as a competitor in the market. We believe competition has led to substantial improvements in network security – both for our own products and for the industry as a whole.

Regulation which decreases competition would ultimately result in sub-optimal security outcomes.

[24] Discussion Paper, p 7.

**(b) Open access for vendors increases the availability of telecommunications services and benefits of the digital economy**

Vendor competition also delivers better prices for carriers/CSPs and this leads directly to lower prices for government, business and consumer end users.

We believe the vibrancy of the telecommunications equipment market in Australia has led to real benefits for Australian consumers in terms of price and innovation. For example, the Australian China Business Council has noted the

> *strong evidence pointing to the positive effect of trade on prices across a range of categories including telecommunications … contributing to further downward pressure on prices in Australia*.[25]

Indeed, the Council has noted that

> *Trade with China has helped keep inflation low. Over the past few years significant increases have been observed in the prices of sectors such as housing, health and education products. However, price deflation has been evident in telecommunications equipment and clothing – two significant imports from China. From June 2007 to June 2011, telecommunications equipment import prices decreased at an annual average rate of 10 per cent, while clothing import prices decreased at 0.6 per cent. This compares with an increase in the consumer price index of 3.2 per cent within the same period.*[26]

The Council has also noted that:

> *Analysis by the ABS … suggests that relatively low average annual rates of price inflation for telecommunication services over the past decade (0.9 per cent) may have contributed to the comparatively strong growth observed in per capita consumption of communication services. The cheaper mobile phones made in China has facilitated the social revolution in communication by Australian households.*[27]

We believe the importance of open markets and their contribution to lower prices and increased use of telecommunications services in Australia should be an important consideration for the Committee.

We believe access to innovative, market-leading technologies from leading global corporations such as Huawei is essential for Australian businesses: enabling them to grow, add value and export back into global supply chains and technology markets.

We also believe discriminatory regulation risks resulting in higher end user costs, less equipment availability and reduced innovation. This should be particularly important given the cost of living pressures facing Australians and the level of government investment in

---

[25] Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 3.

[26] Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 10.

[27] Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 30.

telecommunications infrastructure, which is aimed at improving Australians' access to affordable telecommunications.

**(c) Implications for Australia's commitment to free trade**

Approaches that target particular vendors or vendors from particular countries could also raise concerns about Australia's World Trade Organization (**WTO**) commitments, which require any barriers to trade to be no more trade-restrictive than necessary to fulfil the legitimate objective of protecting national security.

Under the *General Agreement on Tariffs and Trade* (**GATT**), WTO members are essentially required not to discriminate against imported products on the basis of their country of origin. If the Network Security Reforms result in discrimination against vendors on the basis of their country of origin, it is likely that this would place Australia in breach of its WTO obligations under the GATT.

In particular, we note that the "national security" exceptions to this obligation apply in very limited circumstances. These exceptions are unlikely to support the discriminatory application of domestic regulation in a way that imposes unfair barriers on certain foreign vendors.[28]

We believe similar concerns would arise in relation to Australia's commitments under the *Agreement on Technical Barriers to Trade*.

**(d) Open access is the only rational approach given the complexity of the global supply chain**

Finally, we note that an approach which targets vendors from particular countries would be impossible to rationally enforce given:

- the complexity of the global supply chain;
- that every major telecommunications equipment provider has substantial manufacturing and R&D bases in China; and
- that major telecommunications vendor have very similar global supply chain structures.

While the Discussion Paper may have focused on telecommunications networks, it needs to consider all technology from all vendors.

A single piece of equipment, such as a laptop, can include components from all over the world, from Canada, Ireland, Poland, Italy, the Czech Republic, the Slovak Republic all the way to China, Israel, Japan, Malaysia, the Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam and many others.

The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies.[29] Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, SAP, Boeing, IBM and Alcatel-Lucent are all located there to name but a few.

---

[28] Namely, in relation to fissionable materials, traffic in arms or measures taken in times of war or other emergency in international relations: *GATT* art XXI.

[29] ChengDu Hi-Tech Industrial Development Zone, *West Park*, available at http://www.chengduhitech.co.uk/Location/West_Park.asp.

Every major telecommunications equipment provider has a substantial base in China. Alcatel-Lucent has its largest manufacturing base globally in China and is backed by a Chinese Government State Owned Enterprise;[30] Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the largest supply centre of Ericsson in the world;[31] Nokia-Siemens has 14 wholly owned or joint ventures in China, and its factory in Suzhou manufactures a third of its global production of wireless network products.[32]

Cisco also has a huge presence in China, with R&D centres in six major cities. Over 25% of all Cisco products are produced by Chinese partners, and the company announced a US$16 billion investment in China that includes training 100,000 network engineers with China's Education Ministry and the opening of 300 centres at vocational colleges to train students in networking technologies.[33]

Conversely, in terms of Huawei's supply chain diversity, about two thirds of our components come from suppliers outside of China (32% from the US and 32% from Taiwan and Europe).

Given this context, making distinctions between vendors based on their country of origin is neither rational nor effective. Indeed, the US Telecommunications Industry Association has noted that:

> "*The global ICT industry depends on a globally flexible supply chain, characterised by intense competition and fluctuation in price and supply of different inputs. Indeed, market demands are such that it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. As a result, TIA believes the focus of security concerns should be in how a product is made – not where*".[34]

We believe that the Network Security Reforms need to be applied in a competitively neutral way and that this concept should be hard-wired into any legislative reforms. In this respect, we note that of the key countries which have enacted network security reforms (which are outlined in the Annexure), *none* of those countries have adopted laws which are technology or vendor specific.

## 2.2 There needs to be a clear emphasis on risk assessment

It is also important that the obligations are proportionate – they should balance the reduced network security risks against the costs which would be imposed on carriers/CSPs. While the Discussion Paper notes that compliance would be assessed "based on a risk assessment to inform the level of engagement required",[35] there is no indication that the security obligations themselves would reflect a proportionate, risk management approach.

---

[30] "ASB chairman seeks bigger, global role", *China Daily* (17 November 2011) available at http://www.china.org.cn/business/2011-11/17/content_23943450.htm.

[31] Panda Electronics, *Nanjing Ericsson Panda Communication Co Ltd*, available at http://www.panda.cn/SJTCMS/html/pandastock/stocken200811/28647428.asp.

[32] Nokia Siemens Networks, *Nokia Siemens Networks celebrates another milestone in China*, 16 December 2011, available at http://blogs.nokiasiemensnetworks.com/news/2011/12/16/nokia-siemens-networks-celebrates-another-milestone-in-china/.

[33] Joe McDonald, "Cisco Announces $16B China Expansion", *USA Today* (11 January 2007) available at http://www.usatoday.com/tech/products/2007-11-01-425344141_x.htm.

[34] Telecommunications Industry Association, *Innovation White Paper: Securing the Network* (24 July 2012) available at http://www.tiaonline.org/policy/white-papers.

[35] Discussion Paper, p 36.

In our view it would not be rational to impose significant new costs on the Australian telecommunications industry (costs which will inevitably be passed through to Australian businesses and consumers) in circumstances where there will be little impact on overall security – for example, because of weaknesses in overseas telecommunications networks or end users' failure to adopt simple security measures.

Any requirements imposed need to be based on the level of risk and a realistic evaluation of the effectiveness and cost of implementing security measures. It also needs to recognise that even if carriers/CSPs are adopting "competent supervision" and "effective control" over a network, it will not be possible to guarantee security outcomes given:

- as noted above, there are many other stakeholders involved in ensuring security outcomes – including end users themselves;
- the complexity and scale of telecommunications equipment and software is continuing to increase drastically. For example, the move from closed, dedicated telecommunications infrastructure to IP-based systems and open signalling protocols means that there are increasing opportunities for vulnerabilities; and
- the sheer number of security vulnerabilities and instances of breaches is increasing exponentially. For example, in 2011, the incidence of smartphone malware increased 7 times over that in 2004.[36]

Even Governments and large enterprises with significant resources devoted to IT security have suffered from cyber-attacks and unauthorised intrusions into their networks.[37] These breaches demonstrate that security breaches may occur despite "best efforts" being undertaken. It is precisely for these reasons that hypersensitive communications such as those of the Department of Defence are carried over secure private networks instead of public networks.

In the Annexure to our submission, we have outlined the regulatory approaches taken by other countries to improve telecommunications network security. We note that some countries have limited their network security regulation to networks which serve critical functions (such as power grids). Each country which has adopted network security laws which apply to public telecommunication networks specifically requires network operators to adopt a risk management approach – such as by reference to what is "appropriate" or "state of the art" – rather than requiring them to guarantee complete security.

We believe this is the only practical approach to managing the challenges of network security and that the Network Security Reforms should incorporate a concept of proportionality (for example by requiring carriers/CSPs to take reasonable steps to achieve the required security outcomes).

## 2.3 There should not be a government role in reviewing or approving procurement decisions or network designs

We have significant concerns about the proposal to oblige carriers/CSPs to provide information to the Government, in advance, about significant business and procurement decisions and network designs.[38]

---

[36] F-Secure, *Mobile Threat Report* (Q4 2011) p 7, available at http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf.

[37] CRN, *Hackers claim Aus government email breach* (9 November 2011) available at http://www.crn.com.au/News/279565,hackers-claim-aus-government-email-breach.aspx.

[38] Term of Reference 16(b) or, as set out in the Discussion Paper, "an obligation for [carriers]/CSPs to provide Government, when requested with information to assist in the assessment of national security risks to telecommunications infrastructure": Discussion Paper, p 34.

As noted above, carriers/CSPs have a critical business interest in ensuring their networks are secure. Security is critical to winning business in a competitive telecommunications market.

Australian public network operators such as Telstra, Optus and VHA are tier 1 operators with significant experience managing and a keen appreciation of national security issues. To the extent the Australian Government is concerned about a "a lack of awareness of national security risks"[39] on the part of carriers/CSPs, we support the Discussion Paper's proposal to dealt with this problem through engagement by the Government with carriers/CSPs to share knowledge and disseminate information on an "as needs" basis. This is preferable to a regime where significant procurement decisions must be notified to the Government as proposed.

(a) **The proposal is not outcomes-based**

This regulatory approach misses the point that carriers/CSPs are far better at making procurement decisions and that they have a critical commercial interest in making their networks secure. Any suggestion that Government approval be required of carrier/CSP procurement decisions is anathema to a modern, competitive telecommunications industry.

Consistent with the rationale for an "outcomes-based" approach, we believe compliance needs to be assessed on results and without undue scrutiny of carrier/CSP legitimate business decisions. We believe this type of scrutiny would discourage carriers/CSPs from being able to make rational, timely commercial judgments about managing risk.

(b) **The proposal goes well beyond what is required in other jurisdictions**

A notification obligation would go far beyond what has been adopted in other jurisdictions. We are not aware of any developed jurisdiction which requires network operators to seek Government approval for procurement decisions or network designs.

The European approach has been to:

- permit regulators to request information from operators to assess operators' compliance with security standards; and
- impose an obligation on operators to notify regulators only in the event of an actual security incident.

We believe this is a more proportionate and workable approach.

There are existing reporting regimes in Australia which could be applied and which would better reflect an outcomes-based approach. For example, the *Telecommunications (Interception and Access) Act* provides for carriers/CSPs to provide annual interception capability plans so that the Government can be satisfied that their networks can be intercepted for law enforcement. In our view it would be far more appropriate and less invasive for these types of alternatives to be considered. We request the Committee give consideration in its report to options such as:

- "exception"-based reporting system (as adopted in the European Union); and/or

[39] Discussion Paper, p 33.

- regular reporting about the provision of high level information about risk identification and mitigation strategies (similar to the model adopted in Australia in respect of interception capability).

Alternatively, we consider that accreditation of a network's security via industry bodies such as Communications Alliance may be a viable alternative, noting that the Discussion Paper expressly contemplates "*a role for third parties in providing audit and assurance services*".[40]

If the Committee believes additional measures are justified to meet network security goals, we believe independent verification of vendor hardware and software for use in critical networks may be an alternative (as has been adopted for Huawei equipment being used by BT in the United Kingdom). However such verification would at the very least need to:

- apply to all vendors in a non-discriminatory fashion;
- be undertaken by independent third parties; and
- ensure any audits or verification are performed efficiently.

## 2.4 The enforcement regime should be proportionate and appropriate

As the Discussion Paper notes, there are already relevant enforcement mechanisms and national security provisions in the Telco Act. In particular we note that:

- carriers/CSPs are required to do their best to prevent their networks and facilities from being used to commit offences and to assist authorities to safeguard national security;[41]
- carriers/CSPs may be requested to suspend the supply of a carriage service where reasonably necessary to prevent or reduce the likelihood of certain emergencies;[42]
- the ACMA has a broad power to give carriers/CSPs binding directions (including about national security matters);[43] and
- the Attorney-General may direct a carrier/CSP not to use or supply a carriage service, if the Attorney-General considers that the use or supply is or would be prejudicial to security.[44]

Accordingly we do not see a need for Network Security Reforms to involve a significant overhaul of the enforcement regime – particularly at the harsher end of the scale. In our view, only incremental changes to the enforcement mechanisms in the Telco Act are required.

For example, we note that the ACMA already has powers to give directions to a carrier/CSP "in connection with performing any of the ACMA's telecommunications functions or exercising any of the ACMA's telecommunications powers".[45] However, we agree with the Discussion Paper's suggestion that a power of direction should only be used in the event of a breach,

[40] Discussion Paper, p 37.

[41] Telco Act s 313.

[42] Telco Act s 315.

[43] Telco Act s 581(1).

[44] Telco Act s 581(3).

[45] Telco Act s 581.

after close consultation with the carriers/CSP involved and applying the safeguards set out in the Discussion Paper.[46]

We also acknowledge that it may also be appropriate for a Court to order financial penalties in the event of a breach. However, in our view it would be essential that a "breach" is defined as a failure by the carrier/CSP to take reasonable steps to ensure "competent supervision" and "effective control" over their network. This is consistent with similar legislation enacted in Europe, which refers to whether risks are "appropriately" managed or takes into account whether mitigation measures are "state of the art". If a security issue is undetectable, entirely new and could not have been prevented by taking reasonable steps, in our view a carrier/CSP should not be liable so long as it took all reasonable remedial steps once the issue was detected.

### 2.5 Should the regime apply to existing network infrastructure?

Finally, we note that the Discussion Paper states that the new obligations:

> *will require the application of mitigation measures to existing infrastructure. The security obligations would apply to existing and new infrastructure. Government recognises that it would need to work closely with industry to ensure that there is a reasonable transition period.*[47]

We understand that carriers/CSPs are extremely concerned about the costs and technical complexity of applying the proposed regulatory regime to existing infrastructure. We appreciate these concerns and believe that the Committee should consider whether it would be appropriate for regulation to impose significant additional costs on investments which have already been made.

## 3 Huawei and Cyber Security

### 3.1 Cyber Security as a Global Corporate Policy

Huawei has always understood that to provide the level of confidence required in a small number of markets by customers who have been "challenged" by their local or regional political or commercial environments to "buy local" or "buy Western" may require us to provide independent assessments of our products and processes along with dedicated localisation to ensure that the integrity of the supply and support flow is maintained to a high degree of security assurance.

We have established and implemented an end-to-end global cyber security assurance system. We emphasise that our commitment to cyber security will never be outweighed by the consideration of commercial interests. It is our primary responsibility and guiding principle to ensure the stable and secure operation of our customers' network and business (especially in times of natural disasters such as earthquakes and tsunamis and other emergencies); we understand that cyber security concerns of the industry and society are increasing.

### 3.2 Designing security from within – "built-in" not "bolted-on"

- Huawei has established standardised business processes globally and has identified Key Control Points (**KCPs**) and Global Process Owners (**GPOs**) for each process. In addition, Huawei has established a Global Process Control Manual and a Segregation of Duties Matrix that are applicable to all subsidiaries and business units. The GPOs are responsible for ensuring the overall internal control effectiveness, in light of changes in operational environment and risk exposures.

[46] For example, that directions would be preceded by engagement with the relevant carrier/CSP and a graduated suite of other enforcement mechanisms: Discussion Paper, p 37.

[47] Discussion Paper, p 39.

- From a governance perspective, there is a standing Board Committee dedicated to cyber security chaired by a Deputy Chairman. On this Board sits the main Board Members and Global Process Owners who have a role in ensuring that cyber security requirements are imbedded in processes, policies and standards and that they are executed effectively. If there is any conflict, or resource issue, then this committee has the power, remit and seniority to make decisions and change the business without reference to anyone else.

- Huawei Auditors use the Key Control Points and the Global Process Control manual to ensure processes are executed and that they are effective. Audits, external inspections and third-party reviews all validate what is happening against what should happen. Individual personal accountability and liability (the rules and regulations) are built into Huawei's Business Conduct Guidelines that specify how we must behave in our daily operations. Every person is updated through online exams every year to keep knowledge current and this forms part of our Internal Compliance Programme.

### 3.3 Going Forward - Together

Guiding Principles

1. **IT'S 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

2. **IT'S THE LAW:** Efforts to harmonise and align international laws, standards, definitions and norms must be undertaken, accepting the challenges of cultural differences

3. **IT'S COLLABORATIVE:** Efforts to improve cyber security must leverage public-private partnerships to maximise our chances of increasing our collective ability to thwart attacks

4. **IT'S STANDARDS-BASED:** Efforts to design, agree on and implement international standards and benchmarks of ICT vendors should set the highest, not lowest, requirements and standards

5. **ITS VERIFICATION-BASED:** Efforts to design, develop and implement global independent verification methodologies that ensure products conform to the agreed standards and benchmarks should be mandated

6. **IT'S 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

7. **IT'S DOING THE BASICS:** Efforts to improve basic cyber security "hygiene" must be collectively prioritised to drive the entry point of successful attack to a much higher point

This submission favours and supports international collaboration, openness and trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the seven billion citizens on the planet.

## Annexure: comparison of public telecommunications network security obligations in selected jurisdictions

| Jurisdiction | Security obligation | Notification obligations | Verification obligations | Penalties |
|---|---|---|---|---|
| EU (Directive 2009/140/EC) | Providers of electronic communications networks and services should be required to take measures to safeguard their integrity and security in accordance with the assessed risks, taking into account the state of the art of such measures. | Both the European Network and Information Security Agency and the national regulators should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of networks or services as well as comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of networks or services. | No specific reference to audits. | National regulatory authorities should have the power to issue binding instructions relating to technical implementing measures.<br>In order to perform their duties, they should have the power to investigate cases of non-compliance and to impose penalties. |
| UK (*Electronic Communications and Wireless Telegraphy Regulations 2011*) | Network and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and services.<br>The measures must include measures to prevent or minimise the impact of security incidents on end-users.<br>Network providers must also take:<br>• measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks; and | Network providers must notify Ofcom of:<br>• a breach of security; and<br>• a reduction in the availability,<br>which has a significant impact on a public electronic communications network.<br>Service providers must notify Ofcom of a breach of security which has a significant impact on the operation of a public electronic communications service.<br>Ofcom may notify the public, other regulators, regulatory authorities in other member States and the European Network and Information | Ofcom may carry out or arrange an audit of the measures taken by a network provider or a service provider at the provider's own cost. | Penalties may include:<br>• a fine of up to 10% of turnover (max £2 million);<br>• suspension of the provider's entitlement to provide electronic communications networks or services;<br>• payment of compensation to provider's customers; and<br>• liability for any civil claims. |

| Jurisdiction | Security obligation | Notification obligations | Verification obligations | Penalties |
|---|---|---|---|---|
| | • all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network. | Security Agency. | | |
| Ireland<br>(*European Communities (Electronic Communications Networks And Services) (Privacy And Electronic Communications) Regulations 2011*) | An undertaking providing a publicly available electronic communications network or service shall take appropriate technical and organisational measures to safeguard the security of its services, if necessary, in conjunction with undertakings upon whose networks such services are transmitted. These measures shall ensure the level of security appropriate to the risk presented having regard to the state of the art and the cost of their implementation.<br>The measures referred to must at least:<br>• ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,<br>• protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or | In the case of a particular risk of a breach of the security of the public communications network, the undertaking providing the publicly available electronic communications service must inform its subscribers concerning such risk without delay and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, any possible remedies including an indication of the likely costs involved.<br>There are other notification provisions which are specific to personal data. | The regulator may audit the measures taken by an undertaking providing publicly available electronic communications services and issue recommendations about best practices concerning the level of security which those measures should achieve | Penalties may include:<br>• a fine of up to €250,000;<br>• a court order requiring data or material to be forfeited or erased; and<br>• a direction to undertake specific measures or refrain from some activity. |

| Jurisdiction | Security obligation | Notification obligations | Verification obligations | Penalties |
|---|---|---|---|---|
| | disclosure, and<br>• ensure the implementation of a security policy with respect to the processing of personal data. | | | |
| New Zealand | None, however government agencies must comply with the NZ Information Security Manual. | | | |
| Canada | None. | | | |
| Singapore | None, however the regulator has issued a *Secure and Resilient Internet Infrastructure Code of Practice*. | | | |
| Malaysia | None, however a Security, Trust and Governance Department is tasked with ensuring the reliability and the security of Malaysian networks. | | | |
| United States | There are no legislative provisions directly creating security obligations. However, there are certain Executive Directives related to protection of critical infrastructure. Additionally, the FCC in practice requires foreign entities which acquire 25% of shares in a radio-telecoms licensees to enter into a Network Security Agreement. | | | |
| South Africa | None, however security obligations apply to certain "critical" databases (which may include telecommunications databases). | | | |