



**Submission from Huawei Technologies New Zealand Limited on
the Telecommunications (Interception Capability and Security)
Bill**

13 June 2013

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 over 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 had 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 (including Germany, Finland, US, Sweden, Italy, France, Russia, India, China), 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 also source products from New Zealand and Australia.

Huawei New Zealand has approximately 120 staff, 90% of whom are local.

INTRODUCTION

1. Huawei is grateful for the opportunity to submit on the Telecommunications (Interception Capability and Security) Bill (**the TICS Bill**). If the Committee requires any further information, please contact Andrew Bowater, Public Affairs Manager, Huawei Technologies (New Zealand) Company Limited via e-mail to andrew.bowater@huawei.com or (09) 368-0661.

EXECUTIVE SUMMARY

2. As a major equipment vendor with a reach in over 140 countries 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.
3. We believe security outcomes are best delivered by a competitive, well-informed marketplace – so we strongly support a flexible and outcomes-based approach. We believe this model reflects the importance of competitive and innovative vendors like Huawei in the market and the contributions they make to security outcomes.
4. Given the commentary surrounding the proposed reforms, we do have concerns that the security standards proposed in the TICS Bill will be imposed in a way that excludes particular vendors from being able to participate in key projects with little or no benefit for security outcomes.
5. We believe it is essential that any specific security requirements imposed are objectively justified, vendor neutral and give affected industry players a genuine opportunity to understand and address specific concerns.
6. Network security regulation which is consistent with objective criteria and international standards is important to achieving security outcomes – it would increase competition, innovation and investment, which are all essential to security. It would:
 - (a) increase New Zealand’s access to the latest technologies, foster competition and innovation and result in lower end-user prices;
 - (b) improve New Zealand’s competitiveness in the region and globally;
 - (c) 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 they would all procure components from various countries).

POLICY POSITION

7. We support the policy objectives that Government has stated that it is seeking to achieve with the TICS Bill, as described by clause 18 of the regulatory impact statement. Clause 18 provides that steps taken to meet national security concerns

should be proportionate, fair, risk based and should not unduly distort “competition or innovation in telecommunications markets”.

8. We believe that the effect of this provision would be to require the Government to manage any security concerns in a manner that is based on objective criteria, international standards and applicable to all vendors.
9. We also note that the principles set out in section 8 of the TICS Bill requiring network operators and the Director to avoid unduly harming competition would also support this approach.
10. Against this backdrop, the current drafting of the TICS Bill does not give best effect to the objectives described above because:
 - (a) According to the regulatory impact statement, the regime allows selective enforcement that would enable specific vendors to be excluded from projects rather than focusing on how to mitigate security risks. (We note that clauses 19-25 of the regulatory impact statement records that the practical effect of the Bill could be to reduce the number of vendor choices in limited parts of the network and our business is specifically referenced in that context);
 - (b) The definition of “areas of specified security interest”, is too broad and leads to uncertainty as to what points of networks actually require extra special protections;
 - (c) There is not enough emphasis given to establishing mechanisms and objective criteria that will provide for security assurance, whoever the vendor is; and
 - (d) There is a lack of attention given to achieving competitive neutrality across all the markets impacted by the TICS Bill (over and above those that directly impact on us).
11. Further we are concerned about the lack of timeframes in the TICS Bill as any delays caused by the processes required could cause significant delays in a tender process as well as in any project deployment or expansion. This would significantly impact on efficiency, operating costs and competition amongst vendors as well as network operators, which will adversely affect consumers and impede New Zealand’s economic growth in the long term.

PRACTICAL SUGGESTIONS FOR MANAGING NETWORK SECURITY

Use of internationally accepted standards with independent quality assurance

12. There are many global businesses that are able to maintain rigorous standards of quality and assurance while manufacturing anywhere in the world.
13. The reason for the comfort in relation to global players is that they manufacture to recognized industry standards and their systems and processes are subject to rigorous independent audit.

14. In a similar vein, telecommunications equipment vendors could be required to manufacture to recognized industry standards, and where there could be a security risk, equipment could be made subject to independent testing, and systems and processes subject to independent audit.
15. There are a number of internationally recognized standards for testing equipment, notably Common Criteria as the most widely accepted with 26 countries members of the Common Criteria Recognition Arrangement (CCRA). New Zealand is one of the Certificate Authorising Members of the CCRA. Typically Common Criteria is used for defence and government networks, however Huawei support the implementation of Common Criteria for critical national infrastructure projects for all equipment regardless of vendor to be deployed in those networks
16. In addition, global standards organizations such as the International Telecommunications Union – Telecom (ITU-T) in Geneva have already published guidelines around cyber security, namely the “**Cyber Security Strategy Guide**”¹ which provides a guideline into best practices for governments. The ITU-T has also approved standard X.805² as the framework for Cyber Security Architecture.
17. Since the supply chain for all vendors has been globalised, this presents many challenges in developing processes and procedures to address the global nature of sourcing components from many countries. The Open Group (a vendor and technology-neutral industry consortium) which has over 400 members has developed and published guidelines “Open Trusted Technology Provider Standard” (O-TTPS) which identifies best practice for vendors in delivering products with a globalised supply chain to ensure that products are not maliciously tainted or counterfeit.
18. We cannot ignore the human and organisational factor - all companies required to deliver products and services for Critical National Infrastructure projects should be audited yearly based on ISO standards 27001.
19. Indeed we currently operate according to a rigorous set of assurance standards, for example:
 - (a) We adhere to a globally accepted “Common Criteria” international standard and support the implementation of the next revision of Common Criteria;
 - (b) We have independent auditing of our cyber security assurance systems (and New Zealand government could engage in this process);
 - (c) We have independent auditing of our business processes (and the New Zealand government could engage in this process);
 - (d) Security verification provided by an independent third party.

¹ ITU-T Cyber Security Strategy Guide - <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>

² ITU-T X.805 Standard Security architecture for systems providing end-to-end communications-
<http://www.itu.int/rec/T-REC-X.805-200310-I/en>

20. To the extent possible, it is far more efficient for all concerned if an accord can be reached around independent testing at source because a second round of testing in another jurisdiction tends to add significant extra costs. It can also delay the deployment of equipment to the extent that by the time it has passed the test phase, a new generation of equipment has already been developed. Arguably the potential to delay is a more significant issue with respect to competitiveness than the cost.
21. We would be happy to work with Government agencies to discuss the level of assurance that could be provided through such processes.

Huawei's Cyber Security Global Corporate Policy

22. Huawei has established and implemented an end-to-end global cyber security assurance system. 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.
23. Designing security from within – “built-in” not “bolted-on”
 - (a) 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.
 - (b) 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.
 - (c) 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.
 - (d) Individual personal accountability is 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.

An industry funded New Zealand based testing lab

24. If Government requires further testing in New Zealand, Huawei proposes the creation of a New Zealand Security Evaluated Products Register (NZSEPR). This would be

developed in consultation with government departments by industry bodies such as the TCF and be overseen by GCSB. We envisage that this facility would be an independent testing facility and the TCF and other industry bodies would work with network operators to define a framework for testing of equipment in various areas of an operator's network. The testing facility will provide security assurance testing of software, hardware, system integration and network assurance testing to ensure that every aspect of the implementation and operation of infrastructure and systems complies with a minimum set of security requirements.

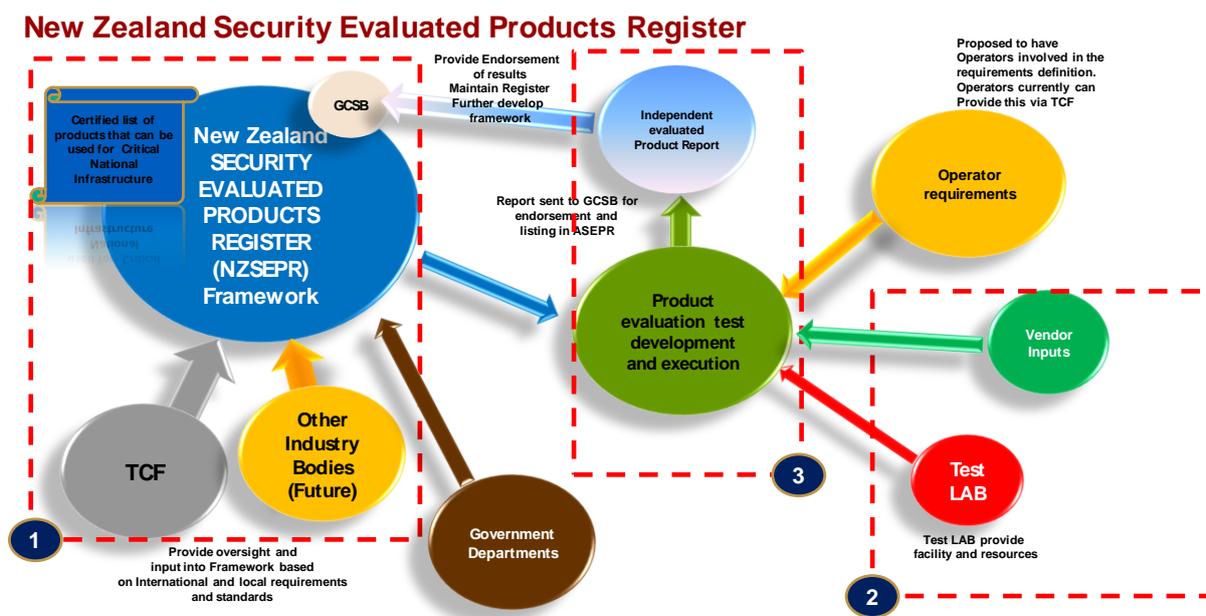
25. Huawei believes that protecting network security is a dynamic process – it needs to be flexible and allow industry players to quickly respond to new and unanticipated types of security threats.
26. Hence a flexible, outcomes-based regulation will be more effective. Detailed and prescriptive regulation 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.”³

27. In Huawei's view, a dynamic, outcomes-based approach has the following advantages:
 - (a) Network operators are best placed to identify appropriate compliance strategies.
 - (b) In our view, network operators themselves will be best placed to identify the most effective and efficient way to achieve compliance rather than Government dictating particular technical solutions to be adopted.
 - (c) In our experience as an equipment vendor, network operators can comply with an obligation to exercise “competent supervision” and “effective control” over their networks 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.

³ Telecommunications Industry Association, *Innovation White Paper: Securing the Network* (24 July 2012) available at <http://www.tiaonline.org/policy/white-papers>.

28. Furthermore, network operators' typical contractual arrangements with vendors will normally include significant technical and security requirements which apply to the vendor's equipment and will provide the network operators with a full suite of indemnities, suspension and termination rights in the event of a breach by the vendor.
29. 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 network operators to adopt the solutions which are most appropriate for their networks.
30. Network operators will have increased regulatory certainty, more autonomy over compliance and greater ability to manage costs with an outcomes-based approach enabling them flexibility to achieve the Government's desired outcomes in the most efficient way possible.
31. The following diagram provides a conceptual model of the New Zealand Security Evaluated Products Register:



32. This framework will also take into consideration the overall threat models based on the overall network architecture.
33. We envisage that this would be industry funded and that the requirements from operators during the procurement process will be clear and that all vendors will submit their equipment for assessment based on a framework which identifies the particular risk associated with the network architecture to be deployed. This will provide clear direction to the industry.
34. Such a testing facility would bring about a number of additional benefits to New Zealand that could also help fund its cost:

- (a) It could provide similar assurance for network build projects taking place in Australia;
 - (b) It could potentially evolve to provide a centre of expertise to assist network operators that are struggling to bring effective lawful interception capability in-house; and
 - (c) By providing a venue for equipment testing for Australasia and other countries.
35. One possible legislative mechanism for implementing this scheme would be to:
- (a) Require stakeholders (network operators and vendors) who wish to carry on business in New Zealand to purchase a license for a fixed fee based on the level of risk proportionate to the national security risk, this will allow smaller stakeholders who do not intend to participate in the national security risk environment to purchase a license based on their requirements. The fixed fees from the existing stakeholders should be sufficient to establish the lab in the first instance, but not so great as to prohibit the entrance of smaller players.
 - (b) When any new stakeholder then buys in, that share would be distributed to the existing stakeholder, so that all contributions are proportionate; and
 - (c) To the extent the testing facility generates profits, those should be invested in developing future cyber security models with the academic environment. To the extent that the testing facility suffers losses, the stakeholder could be required to make further contributions to cover those operating expenses.

PROPOSED AMENDMENTS

Making the network security regime even-handed

36. As noted above, we seek to make amendments to the regime to ensure that obligations fall on all vendors in an objective and non market distorting way, while still enabling the GCSB to ensure that the security of networks are maintained.
37. If the regime is implemented in such a way as to exclude certain vendors from projects which is not based on objective security criteria, a market distorting approach will have significant second and third order consequences:
- (a) It will impede the ability of network operators to run an effective tender process for major projects or to source the best technology if one of the most dynamic competitors is at a practical level removed from consideration due to increased delays, cost and complexity to deal with. (We note that for any given major project there will likely only be two to three of the overall pool of vendors in New Zealand in a position to compete vigorously to win the tender. Thus removing one player from the mix is a very significant impact from a network operator perspective and from a market competition perspective); and

- (b) As a result of impeding a certain vendor’s ability to compete relative to any other vendor, the outcome may be second best network design, technology deployed at an inflated price, and possibly sub-standard cyber security systems, which would then flow through to loss of benefit for end-users. Without genuine competition amongst vendors, there is no incentive for remaining vendors to maintain and drive higher standards in technology and cyber security systems.

38. In that context our proposed amendments are:

- (a) Insert a new section 8(1)(d) requiring the Director and each network operator to address any security risk identified by putting in place mitigations and processes that would apply equally to all suppliers of equipment and services. (It is worth noting that all obligations in section 8 are subject to the words “as far as practicable”, so this would not be an absolute restriction.)
- (b) Insert a new section 8(5) requiring the Director and network operators to work with vendors to establish common, objective processes and standards for ensuring security assurance as a means of addressing security concerns to the extent practicable.

A more targeted definition for “areas of specified security interest”

39. The current drafting in sections 46(1)(c) and 46(1)(d) is uncertain and needs further amendment.

Section 46(1) (c)

40. Section 46 (1) (c) currently blurs two concepts; it attempts to capture both aggregated information and sensitive information (authentication credentials etc). However, section 46 would be more coherent overall if section 46(1)(c) focused on capturing the places where data of a sensitive nature was stored and then 46(1) (d) was then left to capture places where large volumes of data aggregated.

41. Accordingly we suggest that section 46(1)(c) should refer to “sensitive information”, rather than “aggregated customer information” .

42. We also suggest a further, clarification to section 46 (1)(c) (ii) as most vendor equipment will be equipped with an operator console that in some senses might be regarded as providing “privileged access”. We believe that there needs to be some greater clarification around information that gives privileged access across a network generally otherwise too much of the network would be caught by section 46(1)(c) .

Section 46(1)(d)

43. The term in section 46(1)(d) “Any place in a network where data aggregates in large volumes...” is an uncertain subjective phrase. In our view it should be possible to list a small number of aggregation points within the core network that raise concerns, rather than retain such broad wording.

44. Further we question whether there is a need for an aggregation limb to the definition of areas of specified areas of interest at all. The reason is that any place that does genuinely aggregate very large amounts of data will also contain at least some sensitive data and so would be an area of specified security interest in any event by virtue of containing sensitive data.
45. Overall sections 46 - 54 should be drafted to be objective and give effect to section 8(3) and (4), such that Security Risks are addressed in a way that is proportionate to the risk and focussed on more targeted areas. In considering this, guidelines should be defined and published based on risks within the network and a self auditing regime allowed for risks identified as medium and low and do not support "Sensitive Information transmission" so as to reduce the burden on the government agencies, vendors and network operators alike.

Timing discipline

46. To date the industry has found that the focus of agencies has (understandably) been on their law enforcement and broader security activities. Resolving network build issues or resolving other issues affecting industry has ranked lower in their list of priorities.
47. While this outcome is understandable, it has resulted in very significant delays in the deployment of infrastructure that could be benefitting all New Zealanders.
48. Because technology moves so fast, there is a risk that another generation of technology will be developed before an existing set of technology has passed testing, if there are significant delays.
49. Accordingly, if agencies are now being given a much greater mandate to intercede in private commercial processes, there needs to be better, more efficient and more timely engagement, otherwise the situation will become unworkable.
50. We note that at section 74 of the TICS Bill it is expected that network operators will respond to information request within 20 working days, as per the Official Information Act. We propose that the same discipline should be imposed on the Director for resolving network security issues. If there is cause to extend that timeframe, written reasons should be provided for seeking the extension.
51. Finally agencies should also be resourced with the staff and the technical experts necessary to carry out these new functions expeditiously.

Miscellaneous observations for improving drafting

52. We suggest that the following miscellaneous changes should be made to improve the operation of the regime
 - (a) The definition of "wholesale network services" should specifically exclude/carve out "infrastructure-level services", otherwise the two phrases overlap;

- (b) The definition of “security risk” includes “economic well-being”. In the final analysis, that term adds nothing to the definition in that we cannot conceive of a meaningful scenario where New Zealand’s economic interests may be impeded under this regime, without it constituting a security risk.
- (c) The requirement in section 32(2) that “primacy” must be given to national security or law enforcement interests when considering an exemption application is problematic. Using that word would potentially have the effect of making the most minor impact on national security or law enforcement trump any other issue however significant. As a consequence, it may be difficult in practice to ever issue an exemption if that term is used and applied properly. It may be better to rephrase to “give greater weight to section 32(1)(a) considerations”.
- (d) There may be some activities that should be carved out of the obligation in section 47 to notify the Director when working on areas of specified security interest, for example:
 - (i) Minor day to day maintenance/repairs to maintain the status quo (otherwise the Director may be overwhelmed by applications of a trivial nature and network operators would be unreasonably impeded); and
 - (ii) Emergency/unscheduled fault restoration work necessary to maintain the efficient operation of the network which cannot be planned in advance. (The Director should be informed as soon as practicable after the event.)