# Huawei Technologies (Australia) submission

# to the Department of Home Affairs Discussion Paper

# *Australia's 2020 Cyber Security Strategy*

1 November 2019

Huawei welcomes the opportunity to provide a submission to the Department of Home Affairs Discussion Paper Australia's 2020 Cyber Security Strategy.

Since the launch of the current national cybersecurity strategy [1], April 2016, the Australian government has placed significant effort to discharge the related actions.

For example:

- Opened the Australian Cyber Security Centre (ACSC).
- Established Joint Cyber Security Centres (JCSCs) in five capital cities.
- Launched cyber.gov.au
- Appointed an Ambassador for Cyber Affairs in Dr. Tobias Feakin.
- Publicly attributed cyber incidents to nation states.
- Supported domestic industry through the Australian Cyber Security Growth Network (AustCyber), Austrade's Landing Pad Program, and an AU$50 million investment in the Cyber Security Cooperative Research Centre (CSCRC).
- Invested in skills and education, including through Academic Centres of Cyber. Security Excellence at the University of Melbourne and Edith Cowan University.

Beyond that, in 2019, the Australian Signals Directorate (ASD) has put in place the following programs to evaluate products, protect systems and information against cyber threats:

- The Australasian Information Security Evaluation Program with evaluation activities certified by the Australasian Certification Authority (ACA).
- The ASD Cryptographic Evaluation Program, for software and ICT equipment that contains cryptographic functionality.
- The ASD High Assurance Evaluation Program, for ICT equipment protecting highly classified information.

The Australian Cyber Security Centre (ACSC) also certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria, as part of the Australasian Information Security Evaluation Program (AISEP).

This document consolidates Huawei's views in response to federal government public consultation [2] and discussion paper [3], seeking feedback from all organizations and individuals about how to grow Australia's cybersecurity, i.e. improve the security of business and communities, and, at the same time, ensure Australia's future prosperity.

## Executive summary

In order to improve the security of business and communities and, at the same time, ensure Australia's future prosperity, the Australian Government should:

1. Reduce the risk of national dependency on any one supplier, regardless its country of origin, to improve 5G and fibre networks resilience.
2. Ensure more competitive, sustainable and diverse Telecoms supply chain, to drive higher quality, innovation, and incentivise more investments in Cybersecurity.
3. Define network security and resilience requirements on 5G and fibre networks; contribute to unified standards; identify toolbox of appropriate, effective risk management measures; and enforce tailored and risk-based certification schemes.
4. Ensure that there are conformance programmes and independent product testing/certification in place for equipment, systems and software, and support specific evaluation arrangements. (The assessment and evaluation of products from different vendors shall be the same, as their supply chain has the same level of risk.)
5. Develop Australian industrial capacity in terms of software development, equipment manufacturing, laboratory testing, conformity evaluation, etc., looking at end-to-end cybersecurity system assurance; new architecture and business models; tools for risk mitigation and transparency, and greater interoperability and more open interfaces; and share results, in closed loop (3.)

New developments in all cloud, AI, IoT, and software-defined everything are posing unprecedented challenges to the cyber security of ICT infrastructure. The lack of consensus on cyber security, technical standards, verification systems, and legislative support further exacerbates these challenges. Safeguarding cyber security is considered to be a responsibility held by all industry players and society as a whole. Growing security risks are significant threats to future digital society.

To address these challenges, Huawei has opened a Cyber Security Transparency Centre in Brussels, aiming to offer government agencies, technical experts, industry associations, and standards organisations a platform, where they can communicate and collaborate to balance out security and development in the digital era [4].

Huawei takes this opportunity to show its interest to collaborate with the Australian Government, ASIO, ASD and other relevant public and private organizations to embed trust in all business processes, Telecoms supply chain, and enhance cybersecurity through research and innovation in Australia.

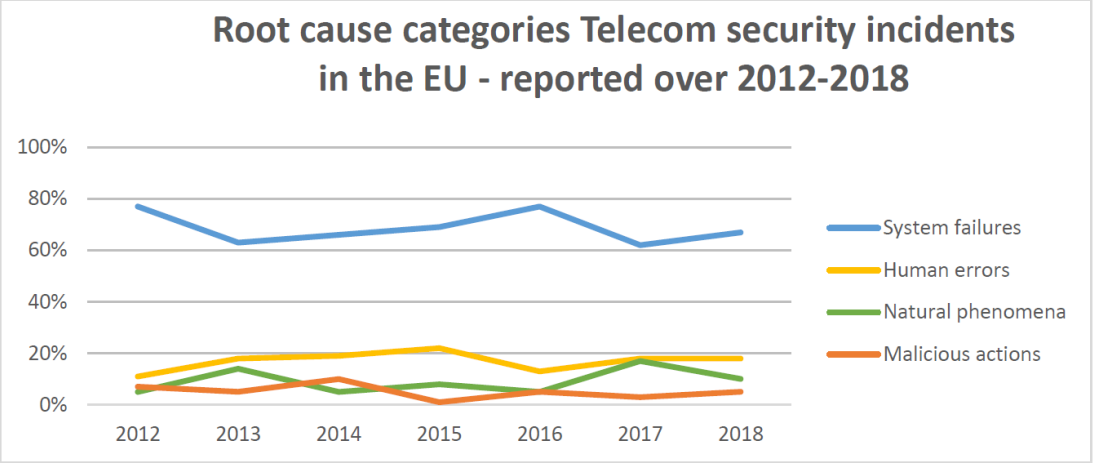
Trustworthy equipment (all supply chain), resilient system and verification shall be all based on standards. This must be a collaborative effort between private (Industry, SME, and Research) and public (Policy Makers, Regulators) parties, as no single vendor, operator or Government can do it alone.

1. What is your view of the cyber threat environment? What threats should Government be focusing on?

As a variety of industries go digital, cyber security risks are increasing. The rising number of mobile connections is creating a larger attack surface (security control zone) for every network. The increasing adoption of cloud platforms means that the geographical and legal boundaries are being expanded for cyber security. The Internet of Things (IoT), Industrial IoT (IIoT), Artificial Intelligence (AI) and big data help us to create and deliver much more value than ever before, but the risk of data breaches is also rising [5], [6], and [7].

In May 2019, the European Union Agency for Network and Information Security (ENISA) published the analysis of the incident reports that the organization has been collecting and aggregating since 2012 [8].

- System failures are the most common root cause, roughly two thirds every year. In total, system failures account for 636 of incident reports (68% of the total). For this root cause category, over the last 7 years, the most common causes were hardware failures (36%) and software bugs (29%).
- The second most common root cause over the 7 years of reporting is human errors with nearly a fifth of total incidents (17%, 162 incidents in total).
- Natural phenomena come third at just under a tenth of total incidents (9%, 89 incidents in total).
- Only 4% of the incidents are categorized as malicious actions. In the period 2012-2018 two thirds of the malicious actions consist of **Denial of Service (DoS) attacks**, and the rest are mainly **damage to physical infrastructure**.




Also, as recently reported by the UK's National Cyber Security Centre (NCSC), in the 1,200 or more significant cyber security incidents the NCSC has managed since it was set up, the

country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out... The techniques [...] were looking for weaknesses in how networks were architected and how they were run [9]. In addition, 90% of the significant security incidents reported to Ofcom in 2018 are attributed to system failure (including hardware or software failures, and systems, processes and procedures failures) [10].
From these findings, a few things become immediately clear. Firstly, it is clear that system failure and human error constitute the greatest risk, and should be the focus of risk evaluation. Secondly, and by extension, the potential risks inherent to any given product should be evaluated based on factors that have a material effect on security, such as: product security architecture, security mechanisms, and security features, regardless the country of origin of the corresponding suppliers [4].

High risk threats may be from trusted insiders and/or external organizations that may seek to exploit weaknesses in telecoms service equipment, and/or in how operators build and run their networks, in order to compromise security [11]. When dealing with cyber security threats, not only their technical nature but also specific to their political nature, economic or other behaviour of malicious actors which seek to exploit our dependency on communication technologies should be taken into account [12].

However, the "flag of origin" for telecommunications equipment is not the critical element in determining cyber security. This is logical: we know, for example, that Russia has carried out significant hostile cyber activity against UK telecommunications networks, and yet there is no Russian equipment in the UK's networks. See [13] and [14] for more information.

The UK National Cyber Security Centre (NCSC) has identified a number of key security risks associated with the telecoms supply chain [11]:

- National dependence on any one vendor, especially the ones deemed high risk.
- Faults or vulnerabilities in network equipment.
- The 'backdoor' threat – the embedding of malign functionality in vendor equipment.
- Vendor administrative access to provide equipment support or as part of a managed services contract.

Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions [12].

The EU coordinated action on 5G cybersecurity risk assessment has just drawn the following conclusions based on capabilities (resources) and intention/attempt (motivation) [15]:

- Integrity and availability of 5G is the major concern, on top of the existing

confidentiality and privacy requirements.

- Threats posed by Member State or State-backed actors, are perceived to be of highest relevance by exploiting undocumented functions or attacking interdependent critical infrastructures (e.g. power supply).
- Other more severe threats included compromised confidentiality and availability associated with an insider within a telecom operator/subcontractor, and associated with an organized crime group.
- Most critical 5G assets: **Core Network Functions**, **Network Function Virtualisation (NFV) and Management and Orchestration (MANO).**
- Most important vulnerability: **Dependency on any one supplier, i.e. lack of diversity in equipment or solutions used both within individual networks and nationally**, because it reduces system resiliency, dis-incentivises investments, increases the likelihood of systemic failure, hostile exploitation and business continuity risks.

In Europe, including the UK, the above findings will lead to:

- The definition of a toolbox of appropriate, effective and proportionate risk management measures to mitigate cybersecurity risks.
- Development of the European industrial capacity in terms of software development, equipment manufacturing, laboratory testing, conformity evaluation, etc.

The German rules [16] came after the EU report on 5G networks by state-backed actors had been published. Network operators Deutsche Telekom (DTEGn.DE), Vodafone (VOD.L) and Telefonica Deutschland (O2Dn.DE) would be required to identify and apply enhanced security standards to critical network elements. More broadly, vendors should be certified as trustworthy, giving customers the possibility of legal recourse to exclude them and seek damages if proof is found that equipment had been used for spying or sabotage. Certification of critical equipment would meanwhile have to be obtained from Germany's cybersecurity authority, the Federal Office for Information Security (BSI) [17].

Huawei welcomes the conclusions drawn by the **5 Eyes** in London, on July 29-30th 2019 [18]:

- Ensure supply chains are trusted and reliable to protect networks from unauthorized access or interference.
- Rigorous risk-based evaluation of a range of factors which may include, but not be limited to, control by foreign governments.
- Evidence-based risk assessment to support the implementation of agreed-upon principles for setting international standards for securing cyber networks.

Those requirements were in line with key ground rules set back in March 2019 ahead of the drafting of the full set of rules by the Federal Network Regulator (BNetzA) and the BSI [18].

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Cyber security involves many elements and stakeholders. An all-industry, full-society collaborative approach is essential to enhancing systematic cyber security governance for everyone. Shared responsibility of all stakeholders should drive the Telecoms supply chain security [12].

Telecoms operators are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks. Vendors must prioritized cyber security sufficiently (e.g. respect laws, regulations, and standards, certify their products, and ensure quality in their supply chains). The regulator is responsible for ensuring operators take appropriate measures to safeguard the general security and resilience of their networks and services. It is the responsibility of the government to take the necessary measures to ensure the protection of the national security interests [11]. Standardisation development organizations, and other stakeholders, ensure that there are conformance programmes and independent product testing/certification in place, as further explained in the following answers.

All stakeholders including industry should work together to promote security and resilience of national critical infrastructure networks, systems, and connected devices. Sharing experience and best practices, including assistance, as appropriate, with mitigation, investigation, response, and recovery from network attacks, compromises, or disruptions should be promoted [12].

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

Governments and industry organizations should work together on unified cyber security standards. These standards should be technology-neutral and apply equally to all companies and networks. Over many years, the telecom industry has made great strides in delivering continuity, reliability, and compatibility across telecom networks by developing shared, unified standards with clear responsibilities between Telecom operators and equipment suppliers, with use of contractual requirements and attestation requirements. As MIT Media Lab cofounder Nicholas Negroponte wrote in an article on Fast Company [19], "**Telecommunications policy should be based on objective standards, not geopolitical issues**."

Once clear unified cyber security standards are developed, we need independent, comprehensive verification processes that comply with these standards. As a global community, we need to establish third-party cyber security verification mechanisms – under the supervision of government, regulator and intelligent agencies – for all industries and companies so that trust and distrust are based on facts, not feelings. Verifiable facts and

unified verification standards will in turn lead to objective results enabling organizations to compare and choose products based on their security requirements [4].

Cyber security is and privacy preservation are the top priorities at Huawei. We are committed to supporting the secure and stable operations of customer networks, in compliance with laws, regulations, standards and best practices with maximal level of transparency. For the past three decades, Huawei has operated in more than 170 countries and regions, serving over three billion people around the world. Our equipment has never caused a large-scale network breakdown, and we have never experienced any serious cyber security breach. Huawei has never done anything to jeopardize the security of our customers' networks or devices, and thus no evidence of such actions exists [4].

## 4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

The Government should make sure that there is a comprehensive national program of risk (and resilience) management, customised for the critical infrastructure sectors, with independent conformance programs, work closely with industry (e.g., CA and IoTAA in Australia), international partners (e.g. 3GPP and GSMA), and, particularly, with cybersecurity agencies (e.g. UK NCSC in UK, BSI in Germany, and ENISA in Europe) to ensure there are recognised standards and best practices and conformance programs – relative to telecom operators and equipment suppliers – priority regulations, contractual/procurement requirements and disclosure requirements.

Furthermore, the Government should play a role to influence procurement decisions, encourage key sectors to identify recommended risk-informed procurement requirements for like-situated private companies – regulated and unregulated – through its collective buying power and power of direction to promote and enforce the use of a diverse and secure supplier base and those who buy from buyers should have risk-informed procurement requirements, in the private and public sectors [11]. (While the public sector currently does not procure telecoms infrastructure equipment on a large scale, this may increase, to some degree, as 5G technology allows for network slicing and custom networks.)

The Government should collaborate with key private sectors players, for each critical infrastructure (CI) sector, recommend best practices for key providers, especially Telecom operators and equipment vendors, risk related to ICT, generally, 5G risk, IoT risk, AI risk. First identify requirements, both those capable of being addressed now, and those that are priorities for R&D, and provide solutions to different levels of security within a carrier network, which should be built to be resilient to any attack, such that no single action could disable the system. In [13], [14], [15], this can be best achieved by diversifying suppliers:

- **Reducing over-dependence from a single vendor**. The network should not be

dependent on just one vendor, as this would render it less resilient.

- **Increasing competition**. Requiring operators to use equipment from more than one vendor increases competition between those vendors, which will force them to improve their security standards for each key node.

The Government, in collaboration with private parties, should play a fundamental role in raising the bar on cyber security standards across the board, together with objective conformance programs and disclosure requirements of conformance and gaps for key providers to government [14]. In the case of 5G, there are primarily only three potential suppliers of 5G Radio Access Network (RAN) in Australia to the four mobile service providers - Nokia, Ericsson and Huawei. (In Australia, Huawei had tendered for the RAN.) Limiting the field to just one or two RAN suppliers, on the basis of the above arguments, induces over-dependence and stifles competitive pressure to deliver the best practice network resilience and security. Including a third company (especially one with a very competitive market offering) would avoid seller's market syndrome and, counter-intuitively, deliver higher overall security [14].

Taken from [14]: this debate must not therefore be characterized as one between those who are "pro-China", and those who are "anti-China". China, with its dynamic economy and growing global influence, is – and will continue to be – a key economic and diplomatic partner for Australia, and one with which the Government must continue to deal with respect. Huawei itself is a remarkable company, which has achieved extraordinary technological advances, and brought radical innovation and competition to a sector that, without Huawei, might lack these attributes. The focus and effort should be placed on how to comprehensive manage real cyber security risk – objectively and with transparency. Competition is key to all this: for innovation, lower cost, offering greater security and providing greater resilience.

Strayer and Healey delivered what is now the standard litany of USG resistance to Huawei. It consists of four major allegations [20]:

- Huawei 5G equipment poses severe cybersecurity threats.
- Huawei steals intellectual property.
- Huawei gets government subsidies.
- Huawei is inseparable from and a tool of the Chinese government.

**Each argument is politically potent in U.S. political scenarios, but surprisingly weak when subjected to basic logical and empirical scrutiny**. In [20], the first of two articles deals with the first three parts of the litany. The second part takes on the last one, which is the core premise of the campaigners and the real source of the problem in Australia. Taken from [20]: "It's clear that this is part of an organized, government-led campaign. But the real issues underlying the U.S. challenge to Huawei are not being stated directly. Red flags are being waved and diversionary tactics used in the service of an objective that is not openly

stated." The same conclusions were drawn in [21] and in [22] for the Australian case.

Finally, in partnership with industry, including Huawei, the Government should play an important role in targeting investment in Testbeds and Trials Programme in a number of potential areas including, but not limited to, software-based innovation in core network functions, open architectures in access networks, and cyber security in small cell technologies [11].

## 5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

Over the last decade Australian electronic communications policies have failed in delivering more competition, lower prices and more choice for businesses and consumers, and the current regulatory framework has not systematically favoured deployment by all market actors of very high-capacity and resilient networks [23], [24]. And now the question is whether 5G will be another failed infrastructure project that Australia can ill afford. In [23], it looks worse, as it feels like we could end up with a repeat of the NBN. "Australia's NBN was national infrastructure product that was, at its inception, best described as a moonshot which would have delivered fibre internet to 90% of premises across the country. What it ultimately ended up as was a hodge-podge of second-rate technologies that provide second-rate internet connectivity to many".

In developed countries, such as Europe, China, South Korea, Singapore and Japan, significant changes have taken place within the ICT sector and patterns of consumption and needs have been radically shifting, demanding access to an ever-increasing array of digital services, which place an ever-increasing demand on the networks across which they are provided. And even more is needed in the years to come, as service applications based on the Internet of Things, cloud computing and virtual and augmented reality will further develop and grow [25], [26].

The full economic and social benefits of this digital transformation will only be achieved if the Australian Government can ensure widespread deployment and take-up of very high capacity networks, in rural as well as urban areas and across all of society. Since the telecoms sector today is an enabler for the entire digital economy and society, Australia needs to act quickly with new policies and regularity frameworks to secure its global competitiveness and prosperity in the near future. It is essential that policymakers get the new Cybersecurity strategy right and invest in developing skills and local industrial capacity if they want to provide opportunity for all in the era of the Fourth Industrial Revolution [25]. Ensuring cybersecurity and finding a balance between technology integration, human capital investments and the innovation ecosystem will be critical to enhancing productivity in the next decade.

The European Commission "Recommendation on Cybersecurity of 5G Networks" [27],

"Cybersecurity Certification Framework" [28], and "Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society" [26] are examples of actions to improve the security and ensure future prosperity of all member states (including UK) in Europe, and gain trust from people, homes and organizations within the Union.

Following the Commission Recommendation for a common European approach to the security of 5G networks, 24 EU Member States have now completed the first step and the EU-wide risk assessment was completed by 1 October 2019 [15]. Commissioner for the Security Union, Julian King, and Commissioner for the Digital Economy and Society, Mariya Gabriel, welcomed this important step forward and said: "… The "**national risk assessments**" are essential to make sure that Member States are adequately prepared for the deployment of the next generation of wireless connectivity that will soon form the backbone of our societies and economies. Close EU-wide cooperation is essential both for achieving strong cybersecurity and for reaping the full benefits, which 5G will have to offer for people and businesses. The completion of the risk assessments underlines the commitment of Member States not only to set high standards for security but also to make full use of this ground breaking technology… We need all key players, big and small, to accelerate their efforts and join us in building a common framework aimed at ensuring consistently high levels of security. We look forward to continuing our close cooperation with Member States … to develop a European approach to protecting the integrity of 5G."

As already introduced, based on the received information, Member States, together with the Commission and the EU Agency for Cybersecurity (ENISA), have prepared a coordinated EU-wide risk assessment [15]. In parallel, ENISA has analysed the 5G threat landscape as an additional input. By 31 December 2019, the Network and Information Systems (NIS) Cooperation Group that leads the cooperation efforts together with the Commission will develop and agree on a "**toolbox of mitigating measures**" to address the risks identified in the risk assessments at Member State and EU level.

Following the recent entry into force of the EU Cybersecurity Act [29] at the end of June, the Commission and the EU Agency for Cybersecurity will set up an **EU-wide certification framework** in collaboration with industry. Member States are encouraged to cooperate with the Commission and the EU Agency for Cybersecurity to prioritise a certification scheme covering 5G networks and equipment. The EU Cybersecurity Act establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes.
Certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU. But, without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers in the European Single Market.

The certification framework will provide EU-wide certification schemes as a **comprehensive set of rules, technical requirements, standards and procedures**. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. It will attest that ICT products and services which have been certified in accordance with such a scheme comply with specified requirements. In particular, each European scheme will specify:

- The categories of products and services covered.
- The cybersecurity requirements, for example by reference to standards or technical specifications.
- The type of evaluation (e.g. self-assessment or third party evaluation).
- The intended level of assurance (e.g. basic, substantial and/or high).

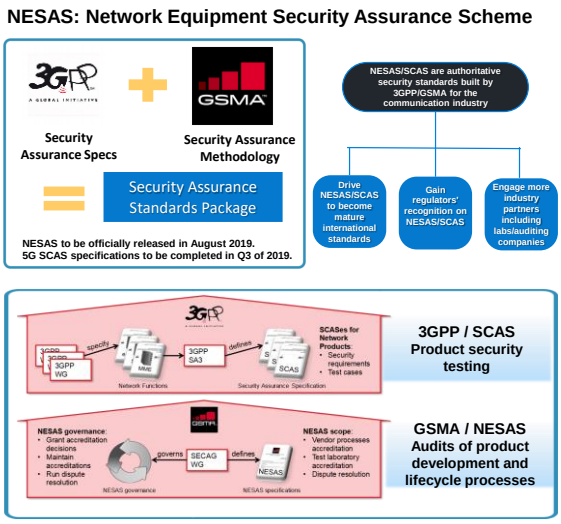
To express the cybersecurity risk, a certificate may refer to **three assurance levels (basic, substantial, high)** that are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. For example, a high assurance level means that the product that was certified has passed the highest security tests. The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service. In short:

- Step 1: Creation & Governance of a **new Certification Scheme at EU Level** – Voluntary scheme for the industry but mandatory that member states put it into place. (By 28 June 2020.)
- Step 2: **Enforcement** of the **new Certification Scheme** at the **national level** (e.g. Actors in France). (By 28 June 2024, and every five years thereafter.)
- Step 3: Introduction of **new Certification Schemes** (created in the Step 1) to make it **mandatory in the industry**, using the **sectorial regulation** from the different Directorate General (DG), e.g. FIMA, Home, Move, etc. (By 31 December 2023.)

At the same time the industry is actively contributing to integrate the **3GPP SeCurity Assurance Specifications (SCAS)** [30] and **Network Equipment Security Assurance Scheme (NESAS)**, jointly defined by 3GPP and GSMA [31], certification and accreditation frameworks with the upcoming EU toolbox and new Certification Schemes.

In particular, the German national cyber security authority (BSI) [17] is working together with ENISA to adapt the 3GPP SCAS-GSMA NESAS model to the new European Cyber Security Act, and setup an EU 5G regulatory framework (in cooperation with the industry).

A comprehensive review of the EU NIS Directive and cybersecurity/notification requirements it imposes on critical infrastructure companies and digital service provider's powers, and EU's march to take the global lead on cybersecurity with the EU Cybersecurity Act ("Act"), together with recommendations to U.S. companies offering an ICT product, service, or process within the EU, may be found in [32].


## 6. What customer protections should apply to the security of cyber goods and services?

Data privacy preservation and protection can be easily achieved by adopting and enforcing the EU General Data Protection Regulation (GDPR), which would harmonize data privacy laws across Australia, protect and empower all AU citizens' data privacy, and reshape the way organizations across the region approach data privacy [33].

Following a coordinated AU-wide risk assessment, the ACSC, e.g. in collaboration with UK NCSC and ENISA, should analyse the cyber goods and services threat landscape as an additional input. The Government, e.g. together with the European Commission delegation in Canberra and key industry players, should develop and agree on a toolbox of mitigating measures to address the risks identified in the risk assessments at State and National level. The Government should then set up an AU-wide certification, accreditation and assurance framework covering all relevant cyber goods and services, as done in the EU. Ideally, the AU Government could collaborate with EU to come up with global certification approach – like the Common Criteria – once tested equal good to go!

## 7. What role can Government and industry play in supporting the cyber security of consumers?

Data privacy preservation and protection of consumers can be easily achieved by adopting and enforcing the EU, which would harmonize data privacy laws across Australia, protect and empower all AU citizens' data privacy, and reshape the way organizations across the region approach data privacy [33].

As in Europe, Australia needs to establish an overarching security framework for the telecoms sector, covering operators and vendors of terminals, devices and ICT infrastructure.

Cybersecurity risks, following a coordinated AU-wide risk assessment, need to be clear with a mitigating program (toolbox of mitigating measures) and certification framework in place to provide three or more levels of assurance to consumers and auditable transparency regarding whether, how, and when equipment vendors access customer networks and data. Government needs to force the industry players to enhance governance, ICT infrastructure and device resilience, and incentivise them to proper manage the supply chain risk, in order to provide the requested level of assurance. One key incentive is the contractual requirements of the equipment vendors to the operators, part of pre-contract risk -informed procurement requirements.

## 8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

Security and risk assessments of vendors, network technologies, telecom operators, and their conformance to best practices [34] and regulations, should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges. Risk management framework in a manner that respects data protection principles to ensure privacy of citizens using network equipment and services should be implemented [12].

Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted [12].

Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law [12].

The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards to data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection [12]. We need open and transparent assurance against backdoors and ability of any country to force any company to turn over sensitive data, as bad guys can hack through anyone.

The Government and ACMA, in consultation with industry, should establish a new set of security and resilience requirements for 5G and full fibre networks. These requirements should be clear, targeted and actionable, providing clarity to industry on what is expected. The adoption of the requirements by operators (and through them, suppliers) will mitigate

network security and resilience risks, and ensure the protection of the Australian national security interests. By raising the security bar, the new Telecommunications Sector Security Reforms (TSSR) should make sure there are recognised standards with conformance programmes to ensure that there is compliance. Vendors that cannot meet these requirements should be excluded. That will increase the demand for those vendors who place a high value on security. Once determined what vendors should do, the Government should make that a requirement and have a programme in place to make sure they keep it up or they are hurt or cut out. Given the global nature of telecoms, there is also an opportunity for regulatory alignment with Europe and UK to sharpen the security incentives in these markets [11].

Measures to equalise cyber security standards across vendors should make it harder for a vendor to enjoy competitive advantage at the expense of security. Moreover, operators should be required to demonstrate to the ACMA and Government that they have comprehensive risk management and monitoring programme consistent with agreed-upon standards and other requirements, and that they have put in place appropriate architectural controls and other measures to address identified risks in their supply chain, regardless the country of origin of the deployed equipment [11].

Another critical way of applying the new TSSR should be through effective assurance testing and ongoing management of vendor equipment. Operators should work closely with vendors, supported by ACSC, to ensure:

i) A robust security development lifecycle process.
ii) Effective assurance in the context of that specific operator's deployment of designated equipment, systems and software.
iii) Ongoing verification arrangements to make sure that security requirements are met.

It is clear that operators should prioritise greater security assurance and whole-of-life costing in their vendor base and the new TSSR will help drive that. When taken together, these measures will create a robust and risk-based security regime for telecoms that will improve how the market works, without banning a carrier from accessing the best 5G technology. This new framework will allow the Government to respond to threats, risks and technology changes, including strengthening the controls if needed in the future [11].

Furthermore, the government should establish equivalent cyber security evaluation centres for all 5G equipment vendors in Australia, especially the ones supplying core networks [14]. In Australia, there is an industry need to create a more diverse and competitive supply base for telecoms networks. This will be critical to drive higher quality, innovation, reduce the risk of national dependency on individual suppliers, and attract more investments in the ICT field, especially on Cybersecurity.

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

The responsibility for the management of cyber security and privacy risks to Australian telecoms should be shared between the Government, ACMA and industry.

Telecoms operators should be responsible for managing the risk and assuring the resilience of their networks, including the risk from equipment and other suppliers. Government should make sure the operators are managing their networks in conformance with regulatory requirements and industry best practices in a manner that provides assurance and transparency. Government should make clear to operators that they should not compromise appropriate risk management practices to achieve commercial priorities. The business models of vendors should prioritize cyber security and privacy protection consistently with laws, regulations, standards, product certification requirements, and manage risk from suppliers. Moreover, the Government should demand for similar actions from all vendors, as with Huawei Cyber Security Evaluation Centre (HCSEC) in the UK. All flaws resulting from practices that may have achieved good commercial outcomes but have resulted in poor cyber security should be identified in all equipment, regardless the label placed on them.

After input from the private sector, the TSSR should provide clarity to industry on what is expected in terms of appropriate risk management practices for network operators. ACMA should engage industry to understand supply chain risks and the arrangements adopted by operators to mitigate them, and get regular updates on operators' major supplier arrangements and TSSR compliance plans.

10. Is the regulatory environment for cyber security appropriate? Why or why not?

As explained above, the current regulatory environment does not provide a risk assurance framework with a common understanding or methodology for identifying threats, assessing or managing risk, or promoting resilience. Nor have appropriate standards or best practices, or supporting conformance and testing protocols been developed, much less implemented, to facilitate ongoing assessment of the effectiveness of risk management and the state of network resilience. Specifically it does not provide guidance to address the fundamental questions to take the security of telecom networks extremely seriously in Australia, e.g. [11]:

- How to incentivise telecoms operators to improve security standards and practices in their networks.
- How to address the security challenges posed by all vendors.
- How to create sustainable diversity in the telecoms supply chain.

The Telecommunications Sector Security Reforms (TSSR) Act is in force with a ban on Huawei participating in 5G procurements. The Security of Critical Infrastructure Act (SCIA) is also in force with no clear directions on how to protect Gas, Water, Electricity and Ports infrastructures. The Assistance and Access (Decryption) Bill is also in force despite of the industry concerns, even making it very difficult for Australian based organisations to sell their cyber security services to the rest of the world [35].

Looking at mobile Telco infrastructure, currently, the TSSR (power of direction) makes the entire ICT infrastructure less secure by increasing the over-dependence from 1-2 vendors. It also makes the continent less prosperous by reducing competition and dis-incentivises investments in the ICT sector, especially on Cybersecurity [36].

In [37], the "Case study 4: 5G Policy" proves that authors had no understanding of 5G network architecture and its practical realisation and deployment, including its current state and evolution, and relationship with earlier mobile system generations. And, as a result, in [38], the consequent "Government Provides 5G Security Guidance To Australian Carriers" gives recommendations based on incorrect technical advice on 5G Architecture, interfaces, functions and protocols (see, e.g., [39], [40], [41]) and effects such as on Huawei due to Chinese laws [42].

## 11. What specific market incentives or regulatory changes should Government consider?

Government needs to force the industry players to enhance governance, ICT infrastructure and device resilience, and incentivise them to properly manage their supply chain risk, in order to provide the requested level of assurance. For example, the TSSR should incentivise all vendors to address systemic engineering failures, as well as incentivise telecom operators to improve security standards and practices in 5G.

Also, incentives to inform the Government due to regulatory requirements (e.g. TSSR, SCIA) need to be in place to ensure carriers are not threatened by coming forward and ask for support from ASD to take the security of telecom networks extremely seriously in Australia, instead of prioritising their commercial interests.

## 12. What needs to be done so that cyber security is 'built in' to digital goods and services?

Manufacturing, supply, and product development processes need to be consistent with, and be driven by, recognized industry standards and best practices. Equipment vendors should have objective requirements steeped in standards and other agreed requirements, with independent certification to assure conformance to requirements

A number of different security certification schemes for ICT products exist in Australia, using common criteria, see, e.g., the Australasian Information Security Evaluation Program, High

Assurance Evaluation Program and ASD Cryptographic Evaluation Program [43]. Yet, in close collaboration with the private sector, the Government should mandate an Australian cybersecurity certification framework that specifies technical requirements and creates a tailored and risk-based AU certification schemes for testing all critical products and components. Such certification would play a critical role in providing an objective basis for knowing which products and services are worthy of trust, which is crucial for the Australian digital market.

## 13. How could we approach instilling better trust in ICT supply chains?

Having a common standard and all players being subject to the same scrutiny to ensure a competitive, sustainable and diverse supply chain. In parallel, the Government should mandate an Australian cybersecurity certification framework that enables the creation of tailored and risk-based AU certification schemes, as done in Europe.

## 14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Private entities need to be prepared to invest in the ongoing education of cyber security professionals, through assisting staff in achieving and maintaining professional credentials, in order to embed trust in all end to end processes and enhance security through innovation.

The Government should invest in experimental programs to provide an opportunity to support architectural models that open-up network domains, allowing operators to use different vendors for different components of the network, and make sure that trustworthy equipment (all supply chain), resilient systems and verification are all based on standards.

The Government should also explore the need for a new national telecommunications lab, with the support of industry and academia. In addition to testing interoperability, the lab could also provide training facilities, de-risking functions for new entrants to the market, and capabilities for security researchers to work on new telecoms technologies, learn, adopt and improve Cybersecurity in a safe environment.

The Government could fund a series of projects that bring together operators, vendors, industry ‘verticals’ (e.g. manufacturing, healthcare and logistics) and universities, to explore new applications and business models for 5G [11], as new systems shall be able to mitigate (cyber) security threats of the communication system and any associated data.

This must be a collaborative effort between private (Industry, SME, and Research) and public (Policy Makers, Regulators) parties: No single vendor, operator, or Government can do it alone.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Needs to be more promotion of tools and technology that can provide safeguards on intrusion prevention and detection.

17. What changes can Government make to create a hostile environment for malicious cyber actors?

Review the current disciplinary actions to be in synch with the impact of the crime/act committed.

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Ensure a risk management framework is in place with relevant resourcing to provide proactive measures. We also need periodic refresh of threats and risk assessments and controls and even standards, as explained above.

19. What private networks should be considered critical systems that need stronger cyber defences?

Private network critical systems of some industry sectors (defence, energy, water) would clearly benefit from stronger cyber defences from a national security perspective. The minimised economic and social impacts to other private network systems (in government, health, manufacturing, education, transportation, finance) through improved cyber defences cannot be denied either.

20. What funding models should Government explore for any additional protections provided to the community?

Private and public partnerships and international collaborations with Europe (including the UK), China, Japan, Singapore, South Korea, USA.

Under the current multiannual financial framework (MFF) 2014-2020, EU funding for cybersecurity is channelled through a number of programmes and funds. For instance, the EU research programme Horizon 2020 has invested roughly €600 million in cybersecurity projects (an additional €450 million has been devoted to the public-private partnership on cybersecurity (cPPP1) over the 2017-2020 period); under the European structural and investment (ESI) funds, up to €400 million has been allocated for investment in trust and cybersecurity; the Connecting Europe Facility (CEF) invested about €30 million in cybersecurity measures in the 2014-2017 period [44].

The European Commission has just proposed, as a next step, the creation of a Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre to invest in stronger and pioneering cybersecurity capacity in the EU [45].

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Main constraints are in sharing information classified as sensitive, confidential, or having privacy concerns. Greater understanding of classification and transparency requirements is required.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Completely agree as the main focus is generally on price and business bottom line, and the customer is not in a position to know all about cyber risk and therefore needs assistance in proper understanding of business requirements and the potential threats that exist.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

If consumers are aware of the potential risk then they are more enabled to perform risk assessments and required mitigation.

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

Vendors should be subject to rigorous oversight through procurement and contract management. This involves operators requiring all their vendors to adhere to the existing legislation (TSSR; SCIA).

Require operators to work closely with vendors, supported by Government, to ensure effective assurance testing for equipment, systems and software, and support ongoing verification arrangements. As done in Europe, the Government should define and mandate an Australian cybersecurity certification framework that enables the creation of tailored and risk-based AU certification schemes.

25. Would you like to see cyber security features prioritized in products and services?

Yes, as stated above several times, this would provide a level playing field of requirements for any given vendor/supplier, and would also help with the risk assessments done by the customer.

## 26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

Ensure vendors and carriers build and operate secure and resilient networks, and manage their supply chains accordingly; and assess the risks posed by vendors, regardless of their country of origin, and apply proportionate and targeted controls to mitigate the risks, without banning operators and infrastructure owners from access to the best 5G technology. (Cyber supply chain includes the design, manufacture, delivery, deployment, support and decommissioning of equipment (hardware and software) or services that are utilised within an organisations cyber ecosystem. Supply chain must consider the whole lifecycle of an IT product or service in an organisation [46].)

The Government should be extremely cautious of making decisions solely based on nationality of a vendor. A vendor from a country whose laws are not likely contrary to Australian law, does lower the immediate elevation of risk associated with likely adverse extrajudicial control in nationally critical systems [46]:

- If the vendor is from a country of possible concern, and considered "high risk", that alone should not rule out the vendor. Instead, consider the actual role of the system under question relative to critical data and perform risk assessment and mitigation through complimentary security controls.
- Conversely, if a vendor is not from a country of concern with regard to extrajudicial influence, this should not immediately rule them as a lower risk option with regards to overall cyber supply chain risk. There are still cyber security vulnerabilities that must be considered and mitigated.
- Ask vendors for evidence of compliance with commonly known standards they would already have to comply with for the different regions they operate in. In the absence of that, ask for demonstration that the vendor has complied with best practice guidelines and evaluate their products, regardless the country of origin.

Seriously consider actions to address and mitigate Cybersecurity concerns similar to what is ongoing in the EU, see e.g. [27], [28], [29], and [45], especially on the EU-wide Cybersecurity Certification schemes, and the policy response for a new robust security framework in the UK [11].

In developing Australia's 2020 Cyber Security Strategy, the Government, in consultation with the industry, should consider:

- A new set of network security and resilience requirements on 5G and fibre networks for telecoms operators, overseen by ACMA and Government, to design and manage their networks, as well as their business and governance processes, with higher standards and best practices. The adoption of the requirements by operators (and through them, suppliers) will mitigate network security and resilience risks, and ensure

the protection of the Australia's national security interests. Building on these arrangements, it is important that improvements to the security practices of all vendors are secured. The effect should be to improve cyber security standards across all suppliers and, in doing so, help to level the playing-field between suppliers.

- Engage industry to understand Telecoms supply chain risks and the arrangements adopted by operators to mitigate them, and gain regular updates on operators' major supplier arrangements and TSSR compliance plans.

- Encourage providers to participate in threat intelligence-led penetration testing scheme and, subject to third party contract arrangements, test operators' vendor specific arrangements, and share thematic findings across the sector to support a culture of continuous improvement; and increase analysis and reporting on network security and resilience.

- Require operators to work closely with vendors, supported by Government, to ensure effective assurance testing for equipment, systems and software and support specific evaluation arrangements. The new approaches should increase understanding of areas, including engineering and design processes, ongoing product support and vulnerability remediation. The assessment and evaluation of products from different vendors should be the same, as their supply chain has the same level of risk.

- Develop a targeted diversification strategy in order to reduce the over-dependence from 1-2 vendors, and ensure there is a more competitive, sustainable and diverse supply chain. This is critical to drive higher quality, innovation and reduce the risk of national dependency on individual suppliers, regardless of where their HQ is located.

- The new strategy should incentivise entry and growth, including market design and R&D support, cybersecurity evaluation and innovation centres; promoting interoperability and demand stimulation; and attracting established players to Australian market.

- The Government should support market expansion in 5G – including improving access to spectrum, removing barriers to roll-out and promoting new infrastructure models, looking at the development of a more diverse supplier base over time.

- The Government should ensure that any public investment and support is targeted at those areas which can address market failures and yield the strongest security and prosperity benefits to Australia, such as: software-based innovation in core network functions, open architectures in all network domains, and cyber security in small cell technologies.

- The Government should invest on 5G Testbeds and Trials Programme, in partnership with the industry, looking at end-to-end cybersecurity assurance and compliance to law, standards and regulations; new architecture models allowing operators to use different vendors for difference components; tools for risk mitigation and transparency, and greater interoperability and more open interfaces.

- The Government should also explore the need for a new national telecommunications lab, with the support of industry and academia. The lab should bring together operators, vendors, industry 'verticals' (e.g. manufacturing, healthcare and logistics) and universities, to explore new applications and business models for 5G and beyond.

- Government could have a number of schemes in place to attract large businesses, including attractive tax incentives (e.g. the lowest corporation tax rate in the G7 and R&D tax credits), a stable regulatory regime and access to talent and labour. These opportunities should be further explored, working with international partners, such as, e.g., the EU and UK, where appropriate.

## References

[1] https://cybersecuritystrategy.homeaffairs.gov.au/

[2] Australia's 2020 Cyber Security Strategy - A call for views: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020

[3] Discussion paper: https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

[4] https://www.huawei.com/en/press-events/news/2019/3/huawei-cyber-security-transparency-centre-brussels

[5] https://www.auscert.org.au/resources/security-bulletins/

[6] Huawei, "Position Paper on Cyber Security", White Paper, September 2019. https://www-file.huawei.com/-/media/corp/facts/pdf/huaweis-position-paper-on-cyber-security-0918.pdf?la=en-us

[7] Huawei, "AI Security". White paper, October 2018. https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/ai-security-white-paper-en.pdf

[8] EU Cybersecurity Agency (ENISA), "Annual Report Telecom Security Incidents 2018", May 2019. https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2018

[9] https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels

[10] Connected Nations 2018, Ofcom, December 2018. https://www.ofcom.org.uk/research-and-data/multisector-research/infrastructure-research/connected-nations-2018/main-report

[11] UK Department for Digital, Culture, Media & Sport, "UK Telecoms Supply Chain Review Report", July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

[12] The Prague Proposals, "The Chairman Statement on cyber security of

communication networks in a globally digitalized world, Prague 5G Security Conference, May 2019. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

[13]The Intelligence and Security Committee of Parliament, "Statement on 5G suppliers", July 2019. http://isc.independent.gov.uk/news-archive/19july2019

[14] The Science and Technology Select Committee, "Letter to the Secretary of State for Digital, Culture, Media and Sport about Huawei's involvement in the UK's 5G network", July 2019. https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/chairs-comments-huawei-5g-network-17-19/

[15] EU coordinated risk assessment 5G cybersecurity, October 09th 2019. https://eu2019.fi/en/article/-/asset_publisher/member-states-publish-a-report-on-eu-coordinated-risk-assessment-of-5g-networks-security

[16] https://www.reuters.com/article/us-germany-telecoms-5g/new-german-rules-leave-5g-telecoms-door-open-to-huawei-idUSKBN1WT110

[17] https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

[18] http://telecoms.com/498852/five-eyes-align-security-objectives-but-where-does-this-leave-huawei/

[19] https://www.fastcompany.com/90344450/dont-ban-huawei-do-this-instead

[20]http://www.circleid.com/posts/20191016_lets_have_an_honest_conversation_about_huawei/

[21] https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

[22]https://www.innovationaus.com/2019/07/5g-a-decision-that-demands-scrutiny

[23]https://ausdroid.net/2019/10/17/opinion-australia-vs-the-world-and-why-our-5g-isnt-winning/

[24] https://www.afr.com/technology/nbn-catastrophe-means-new-plan-is-needed-

20190625-p5211z

[25] https://www.weforum.org/agenda/2019/10/global-competitiveness-report-2019-economic-trends-for-policymakers/#skills

[26] European Commission, “Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society”, September 2019. https://ec.europa.eu/digital-single-market/en/news/communication-connectivity-competitive-digital-single-market-towards-european-gigabit-society

[27] European Commission, “Commission Recommendation – Cybersecurity of 5G Networks”, March 2019. https://www.europeansources.info/record/recommendation-on-cybersecurity-of-5g-networks/

[28] EU Cybersecurity Act “ENISA and Cybersecurity Certification Framework”, June 2019. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

[29] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

[30] https://www.3gpp.org/DynaReport/33-series.htm

[31] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[32] https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/jodywestby/2019/10/21/eu-cybersecurity-certification-schemes-will-surprise-us-businesses/amp/

[33] https://eugdpr.org/

[34]https://nvd.nist.gov/800-53

[35] COMMUNICATIONS DAY, “Calls for federal government to work with industry on cyber security”, page 8-9, 14 October 2019.

[36] https://huaweihub.com.au/setting-the-facts-straight-on-cyber-security/

[37] ASD Annual Report 2018-2019. https://www.asd.gov.au/sites/default/files/2019-10/annual_report_2018-19.pdf

[38]https://www.minister.communications.gov.au/minister/mitch-

fifield/news/government-provides-5g-security-guidance-australian-carriers

[39] https://www.youtube.com/watch?v=WNpVaP2mRcw

[40] The Facts on 5G: https://huaweihub.com.au/the-facts-on-5g/

[41] https://www.youtube.com/watch?v=DeTASrRYalE

[42] https://www.youtube.com/watch?v=WVVjeq1F5ew

[43] https://www.cyber.gov.au/programs?page=0

[44]http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635518/EPRS_BRI(2019)635518_EN.pdf

[45] https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

[46] Australian Signals Directorate's Australian Cyber Security Centre (ACSC), "Cyber Supply Chain Risk Management - Practitioners guide", July 2019. https://www.cyber.gov.au/sites/default/files/2019-06/Supply%20Chain%20Risk%20Management%20-%20Practitioners%20guide.pdf