Nokia's response to Australian Government's 2023-2030 Australian Cyber Security Strategy Discussion Paper

April 2023

1 About Nokia

We create the technology to connect the world. We develop and deliver the industry's leading end-to-end portfolio of network equipment, software, services and licensing that is available globally. Our customers include communications service providers whose combined networks support 6.1 billion subscriptions, as well as enterprises in the private and public sector that use our network portfolio to increase productivity and enrich lives.

With an end-to-end portfolio that is unique in the industry, Nokia can work in partnership with operators to deliver "real 5G". Nokia's in house 5G mmWave Small Cells and AirScale BTS provide in-building and outdoor coverage, while our Microwave Anyhaul, Cloud native RAN, antennas, and 5G cloud-native core are part of approximately half of our agreements to date. Beyond our mobile networks' portfolio, Nokia has excellent FP5 network processor-based IP routers and PSE-6 chipset powered optical networking - our customers can use the Nokia Network Services Platform to make this into full-5G-strength software defined connectivity 'smart network fabric' secured by Nokia Security Orchestration, Analytics and Response (Nokia SOAR) to ensure resilient 5G. Globally Nokia has been selected by more than 230 operators to supply 5G networks.

Nokia is a global leader in 5G and 6G research, 5G and 5G Advanced standardisation, technology innovation and offers a world-class portfolio of 5G products and solutions with a strategy specifically designed to support and drive the Australian market. Nokia is proud to be a strong partner in the current roll-out of 5G in Australia, continuing our 120-year presence here. Nokia has been selected by both Optus and TPG Telecom as a key supplier for the network deployments of 5G, including the required radio modules, as well as a major supplier to the National Broadband Network for fixed network technology solutions.

Nokia is also a supplier to various enterprises and industries which have deployed private wireless networks deployed using apparatus licenses, including for example 27 mines with 10 customers in Australia.

Leveraging the work of our research teams in the world-renowned Nokia Bell Labs, Nokia's industrial research lab, we innovate with purpose, pursuing responsible, sustainable technologies that will have a demonstrable impact on society. We are leading and fostering the digital transformation of society and industries by building end-to-end 5G networks that are faster, more secure and energy efficient. Nokia adheres to the highest ethical business standards as we create technology with social purpose, quality, and integrity.

For more information: https://www.nokia.com/networks/5g/

Disclaimer: This response is based on Nokia's current understanding of the market dynamics and various standards bodies; these dynamics are changing and hence our views may update with these changes

2 Introduction and summary

Nokia welcomes the opportunity to respond to the Government's *2023-2030 Australian Cyber Security Strategy Discussion Paper*. Nokia is a worldwide market leader in telecommunication technology and a trusted and longstanding partner in Australian telecommunications, supporting landmark projects for more than a century.

Nokia is a major supplier to the National Broadband Network for its fixed network technology solutions and a strong partner in the roll-out of 5G in Australia. Our technology is also supporting digital growth in critical sectors and industries such as transport, energy and mining, agriculture, healthcare and smart cities.

The more connected we've become, and the more we depend on continuous real-time information and communication – that criticality has only just intensified. In many industries and sectors, networks have grown to be vital to safety, security and people's quality of life and experience. This will only increase as sectors are moving to next generation digital technologies.

Cybersecurity is also a critical issue for sectors like health, transport, and energy. These sectors are responsible for transmitting and storing vast amounts of sensitive data, including personal information, financial data, and intellectual property. They also rely on complex systems that are increasingly connected to the internet and other networks, and as a result, are a prime target for cyber-attacks.

By taking a proactive approach to security, including protecting network infrastructure, securing supply chains, monitoring network activity, training employees, and having the appropriate measures in place, networks can help protect themselves and their customers from cyber threats. The Australian government has made cybersecurity a priority, recognising the growing threat of cyber-attacks and the need to protect critical infrastructure, government systems, and personal data.

Therefore, Nokia supports the Australian Government's vision of becoming the most cyber secure country by 2030 and welcomes that the strategy will be developed in partnership with industry academia, state and territory governments and the Australian and international community. As part of this submission, Nokia will focus on priorities as follows:

1. Harmonising regulatory frameworks to avoid fragmentation
2. Investing in the cyber security ecosystem by establishing testing facilities
3. Sustaining security in new technologies through a "zero-trust" approach

Nokia looks forward to working with Government to ensure all stakeholders understand the strategic importance of digitalisation and connectivity and have confidence in its security, safety and use cases.

3 Harmonising regulatory frameworks

To respond to the growing threats posed by cyber-attacks in an increasingly connected world, countries are strengthening their focus on network security and associated requirements, addressing the security of supply chains, and streamlining reporting and information-sharing processes. Governments are increasing scrutiny and oversight of industry and imposing stricter enforcement measures.

Nokia acknowledges that the Australian Government is undergoing some of the most significant security reforms in Australia's history with the *Security of Critical Infrastructure Act* 2018 (the SOCI Act) now in force, review of the *Privacy Act* 1988 underway and of course development of the 2023-2030 National Cyber Security Strategy.

As part of these security reforms, Nokia welcomes the Government's opening remarks in the *Cyber Security Strategy Discussion Paper* which highlights that a "clear package of regulatory reform is necessary" which potentially includes further development of the SOCI Act. However, Government should seek to harmonise cybersecurity frameworks where possible to avoid geographic fragmentation by providing a consistent set of standards and best practices which can assist in improving overall cybersecurity.

Having multiple, conflicting cybersecurity frameworks can create confusion and complexity for businesses and governments. Harmonising these frameworks can help to simplify the cybersecurity landscape and make it easier for organisations to comply with regulations and best practices.

Government should support and adopt existing industry-led security frameworks Industry-led international security frameworks promote innovation and adapt more quickly to ever-changing threats than more cumbersome security regimes. For example, the adoption of international, industry led standards, such as GSMA's Network Equipment Security Assurance Scheme (NESAS), removes the need for security requirements that vary across nations. NESAS is an industry led and defined framework focused on Product Security Assurance for network equipment defined by the 3GPP standardisation organisation. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as test cases for the security evaluation of network equipment.

The NESAS scheme was designed to meet the needs of disparate stakeholders including mobile network operators, equipment vendors, and national security agencies and regulators. It serves as an international model that has been applied in whole or in part in several countries and sometimes made mandatory.

Another example includes the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework which is a voluntary framework that provides a common language for understanding, managing, and expressing cybersecurity risk both internally in an organisation and externally. It is intended to be a useful guide for the full range of organisations, from small businesses to the largest enterprises.

NIST issued its guidelines as voluntary, but it encourages the private sector to determine its conformity needs, and then develop appropriate conformity assessment programs to gauge appropriate implementation of the Framework. The Framework is a risk-based approach to cybersecurity, and is composed of three parts: Framework Core, Framework Implementation Tiers; and Framework Profile:

- The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors and provides a high-level strategic view of the lifecycle of an organisation's management of cybersecurity risk.
- The Framework Implementation Tiers describe the relative sophistication and maturity of an organisation's cybersecurity practices using the tiers set out in the Framework. This mechanism enables organisations to understand the characteristics of their approach to managing cybersecurity risk which can help them prioritize and achieve their cybersecurity goals.
- A Framework Profile is a representation of the outcomes that a particular organisation has selected from the Framework. By developing a 'Current' Profile and a 'Target' Profile, organisations can establish a roadmap for reducing cybersecurity risk.

Globally, telecommunication equipment vendors and service providers have developed a clear understanding of reference requirements which add a level of certainty and transparency to procurement processes that use these internationally recognised security frameworks. The cost of security is shared among vendors and operators and is cost-effective in delivering security gains. Government and industry should strive to harmonise security standards across regions and support voluntary security frameworks that can easily adapt to ever-changing threats and rapid changes in telecommunications software, networks, and services.

Government should also increase collaboration with trusted technology partners to allow further sharing of security research and expertise. For example, Nokia and Nokia Bell Labs, the world-renowned industrial research arm of Nokia, are leading the development of new network technologies with built-in security and privacy. We not only engage in a rigorous program to ensure our own product security, but we also work to improve the security of our entire ICT ecosystem by sharing our practical experience in numerous industry standards groups and by investing heavily in security testing and technical collaboration.

Here are a few examples of on Nokia's thought leadership in making communications networks more secure:

- Nokia is laying the foundations for 5G-Advanced in 3GPP Releases 18 and 19, which will further enhance 5G capabilities and security, and enable new verticals. These new capabilities include features like XR, super-accurate positioning, improved coverage, and AI/ML for the 5G-RAN. We ensure that every generation of communications technology is more secure than the last.
- Nokia is the project and consortium leader of the European 6G flagship initiative (HEXA-X and HEXA-X-II) with 44 organisations. This initiative is creating the pre-standardized platform and system view that will form the basis for many inputs into future 6G standardisation and strives to address the challenges of trustworthiness, sustainability, and inclusion ("connecting the unconnected") .
- Nokia leads 6G-ANNA, the German 6G lighthouse project, and has played an instrumental role in establishing the Horizon Europe Smart Network and Services Joint Undertaking (SNS-JU) for industrial leadership in 5G and 6G.
- Nokia contributes to several Working Groups in the U.S. Communications Security, Reliability, and Interoperability Council (CSRIC).
- Nokia is a leader in many industry openness initiatives, including the O-RAN Alliance and Open Networking Forum, driving global consensus and standards to maximize global adoption of new security technology.

Overall, harmonising cybersecurity frameworks globally can help to improve cybersecurity, reduce complexity, increase collaboration, and facilitate global trade.

4 Investing in the cyber security ecosystem

In the advanced digital era, the nature and scale of information networks are evolving, as are the nature and scale of security threats. Networks will link billions of new devices, empower new industries, and enable myriad new applications and use cases. In fact, it is anticipated that between 2021 to 2025 the proliferation of IoT devices will more than double; currently there is around 14 billion devices globally, therefore by 2025 there will be more than 30 billion devices[1]

As such, cybersecurity is also a critical issue for sectors like health, transport, and energy – in fact, all the sectors deemed now "critical" under the expanded remit of the SOCI Act. Critical infrastructure, such as power grids, transportation systems, and healthcare networks, are essential to the functioning of modern society. However, these sectors rely on complex systems that are increasingly connected to the internet and other networks, making them vulnerable to cyber-attacks.

For example, rail networks globally are looking for improved on-board monitoring systems, trains will be equipped with IoT connected sensors. Legacy communications technology for railways will be replaced by 5G and Future Railway Mobile Communication System (FRMCS). However, this also means more avenues of attack open to those looking to play havoc with critical communications infrastructure. The security of network components together with end-to-end-solution security are key to protecting applications from complex attacks.

Nokia itself not only invests heavily in future technologies like AI/ML that can further augment security capabilities but also in R&D centers and end-to-end testing labs. Such facilities use and develop cutting-edge tools and techniques to assess the security resilience of networks, as well as their associated software, hardware, and applications.

They also serve as a central repository for cybersecurity knowledge shared across vendors, operators, enterprise, and government customers. In addition, they can provide high-value jobs and help attract a highly skilled workforce to the country's tech ecosystem. In 2021 and 2022 alone, Nokia launched the following major security centers:

- In 2021, Nokia opened a new **European center of excellence in cybersecurity** to support the development of 5G and network virtualization. The new center, located in Lannion, France, will support Nokia's global security intelligence and operations management centers (SIOCs).
- In 2022, Nokia opened our **ASTaR (Advanced Security Testing and Research) lab** in Dallas, Texas. It is the first end-to-end 5G testing lab in the U.S. focused solely on cybersecurity. ASTaR uses and develops cutting-edge tools and techniques to

[1] Nishant Batra at TechAccord Davos 2023 event #WEF23 - YouTube

assess the security resilience of 5G networks, as well as their associated software, hardware, and applications. ASTaR will use these assessments to address emerging security threats, and lab researchers will engage with the cybersecurity community to identify emerging threat vectors and potential vulnerabilities. Furthermore, the ASTaR lab will become a central repository for cybersecurity knowledge that will be shared across Nokia and with its communication-service-provider, enterprise and government customers.[2]

- Most recently in 2022, Nokia announced with the Government of Canada, the Government of Ontario, and the City of Ottawa a **new R&D hub to expand Nokia Canada's capacity** in next-generation ICT, and cyber security innovation. The new facility will be set on a 26-acre campus, and construction will begin in 2023. Government funding for this project includes up to CAD 40 million via the Canada Strategic Innovation Fund (SIF) and CAD 30 million from the Government of Ontario, through Invest Ontario. These contributions will support the long-term capability of Nokia, Canada and Ontario in cyber security, R&D, and next-gen technology, including 6G, while delivering high-paying jobs in construction and technology.[3]

While Nokia recognises the urgent need for security innovation, there is always more that can be done to counter the relentless pace of those seeking to infiltrate our networks. As such, there are also several examples were Nokia alongside other vendors, operators and software companies are supporting security and cyber security programs and initiatives for critical industries. For example:

4.1 U.S National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence 5G Cybersecurity

Nokia was selected to work with the National Cybersecurity Center of Excellence (NCCoE) and other key vendors, including members from government and industry to form part of the 5G Cybersecurity Project. NCCoE initiated the industry collaboration effort centered on 5G cyber security (with emphasis on 5G core). Other collaborators include AT&T, T-Mobile, Cisco, Palo Alto, Dell, Intel, CableLabs, Redhat, MITAC, Keysight and AMI[4]

The 5G Cybersecurity Project identifies several 5G use cases and demonstrate how the components of the 5G system can provide security capabilities and mitigate identified risks and meet industry sectors' compliance requirements. The scope of this project is to

[2] Nokia launches groundbreaking cybersecurity-focused testing lab in the U.S. | Nokia
[3] Nokia chooses Ottawa, ON, tech cluster to build world-leading, sustainable ICT and cyber security R&D hub | Nokia
[4] https://www.nccoe.nist.gov/5g-cybersecurity

leverage 5G standardised security features which are defined in 3GPP standards to provide enhanced cybersecurity capabilities built into network equipment and end user devices.

Nokia solutions deployed for this project include software, 5G RAN and core solutions, and IP-Backhaul, as well as innovations from Nokia Standards and Bell Labs.

4.2 MITRE Open Generation Consortium (Open Gen)

MITRE Open Generation Consortium (Open Gen) brought together numerous organisations to drive collaboration and breakthrough innovation with 5G technology. This collaborative effort aims to design, develop, demonstrate, and validate solutions that may be uniquely enabled by 5G capabilities to unlock massive economic value. Areas of impact include uncrewed aerial systems (UAS), public safety, remote healthcare, smart cities, and autonomous vehicles.

The consortium offers an opportunity to work closely with technology leaders, innovative startups, industry associations, academics, and government liaisons. Open Gen will complement existing groups in the U.S. by testing 5G standards and use cases.

There are three working groups: 1. Use Cases and Devices, 2. Architecture and Solutions, 3. Implementation, Testbeds, and Experiments (ITE). There are 3 testbeds planned: NUAIR (Syracuse, NY), Virginia Tech, and Northeastern University.

Members at launch include full members Ericsson, Nokia, and Verizon; startup members Altiostar, FIRST iZ, HUSH Aerospace, and Kittyhawk; academic members Northeastern University and Virginia Tech; and non-profit member CTIA – The Wireless Association. Nokia is a founding member of the Open Generation Consortium (website, white paper).[5]

4.3 Australian Government's proposed "Secure G" facility

Nokia suggests similar investments in security, cyber facilities and industry testing labs in Australia given allocated funding for the "Secure G" initiative. Further utilisation of existing facilities should also be considered.

Nokia has been pleased to support the Government's $31.7M "Secure G" connectivity initiative which is primarily focused on enabling businesses to test measures, protocols, standards and software that underpin transparent and secure 5G connectivity. Nokia along with the University of Technology Sydney and other industry partners and academia are members of the Lab's Expert Advisory Panel (EAP).

Given that connectivity is in place across a large percentage of the Australian population and the growing dependency of networks within critical industries, Nokia believes there is

[5] MITRE Engenuity Open Generation Position Paper (mitre-engenuity.org)

an opportunity to expand and scale the focus of the “Secure G” facility to allow critical sectors to test end-to-end security of their applications prior to deployment at scale.

Similar test labs globally, whether for 5G diversification or for 5G testing across industry, have utilised existing facilities as they’re likely to have standard support structures including swipe cards, support personnel, meeting facilities, access to experts as well as relevant infrastructure such as power and physical security requirements.

For example, Nokia 5G Futures Lab is located at the world-class research facilities of University of Technology Sydney (UTS) Tech Lab in Botany NSW. The 5G Futures Lab is a place where Nokia, its partners and customers come together to explore the potential of 5G using our cutting-edge technology and solutions. The 5G Futures Lab supports 3 network lab test lines and 1 RF Chamber test line. Nokia is licensed to transmit mmWave spectrum for a 1km radius around the 5G Futures Lab and its engine room is home to more than $2.5M AUD worth of Nokia products. There are also four 8K TVs in the 5G Futures Lab and a MonitEM-Lab Detector to monitor electromagnetic radiation levels within the lab, ensuring a safe working environment. The lab has a full-time manager.

Nokia’s 5G Futures Lab is located at the UTS Tech Lab which is a world-class multidisciplinary research facility that supports bespoke industry-led partnerships designed to drive innovation and growth in engineering and IT. UTS Tech Lab have significant investment in the largest RF Antenna and EMC chambers in Australia and significant investment in 5G/6G RF (up to 60Ghz) test tools (such as network analyzers) and processes that can be leveraged for physical testing and data collection. These facilities are managed by a Senior RF engineer and research RF engineer delivering commercial testing and services.

In addition, Nokia’s also has a 5G Industrial Incubation Lab in South Australia which in partnership with the South Australian Government, received $1.9 million in funding from the Australian Government to establish the facility as well as the localised 5G network. The 5G network at the University of Adelaide, was placed inside a shielded room (Faraday cage) to ensure there is no interference with the public 5G network. Nokia also hired two full-time engineers to work on the lab over a 12-month period.

At the Incubation Centre, Adelaide Airport is focusing on the introduction of 5G and AR/VR for the purposes of remote inspection and safety monitoring, incorporating real-time, high-quality and interference-free video streaming. The Airport Control Centre (ACC) and Airport Operations Officers (AOOs) who provide 24/7 numerous safety and emergency response coordination will look to utlise 360-degree cameras on the AOO vehicles to reduce the number of trips by support personnel to assess and diagnose problems.[6]

[6] Nokia opens 5G Industrial | Department for Trade and Investment (dti.sa.gov.au)

Governance could be undertaken through the continuation of an expert advisory council consisting of representatives from government, industry and academia to ensure standardised testing and reporting as well as building and leveraging relationships with similar labs and facilities worldwide. There would also be opportunities for training and development of work staff and users of the facility especially given cybersecurity breaches are usually linked to technical security protocols being subverted by human error, including fishing scams, infected memory sticks etc.

Finally, it should be noted that as the Government's "Secure G" facility is also anticipated to be linked to a 6G security including a development program for foundational research and future connectivity technologies, the facility would also support the Government's critical technologies in the national interest program. Nokia believes it is important programs such as the "Secure G" initiative, critical technologies in the national interest and ongoing regulatory reform do not operate in isolation and are viewed as part of the broader packages of Government agendas.

Overall, cyber security testing facilities available can aid to help businesses, organisations and critical sectors and industries test their technology and systems against cyber threats. These facilities can help businesses to identify and address vulnerabilities in their systems and improve their overall cyber security posture.

5 Designing and sustaining security in new technologies

Nokia supports the Government's commitment to supporting critical and emerging technologies to promote Australia as a secure nation of excellence, accelerate productivity growth through fostering innovation and research and creating digital skills of the future while ensuring secure supply chains.

In the context of the Cyber Strategy development, consideration should be given to how these critical emerging technologies of national interest converge and how other ongoing Government critical sector reforms can significantly benefit from advanced optical and radiofrequency communications.

As identified earlier, underpinning digital transformation of society and industries is some form of connectivity such as Passive Optical Networks (such as 25GPON) and 5G. For example, but not limited to, advanced materials and manufacturing, sensing, timing and navigation and transportation, robotics and space. Rail networks globally for example, are looking for improved on-board monitoring systems, trains equipped with IoT connected sensors. Legacy communications technology for railways, will be replaced by 5G and FRMCS.

Impact from technology such as 5G-Advanced in major critical industries such as agriculture, energy, smart cities, transport is expected to contribute up to $8 trillion in global GDP in 2030. Real-life use cases here in Australia include:

Mining and energy

TPG Telecom signed a Memorandum of Understanding (MoU) with Nokia in a partnership to develop mobile private network (MPN) innovations for the mining and energy sectors. The agreement describes collaboration across both companies' extensive portfolios to provide flexible technology solutions and encourage digital and operational technology transformation in mining.

It is expected new innovations will come from the partnership, specifically in productivity and worker safety, as 5G terminals will connect machinery and sensor assets to an internet of things (IoT) or operations platform to monitor productivity and safety of workers.

Agriculture and on-farm connectivity

TPG worked with Nokia to demonstrate how 5G networks can complement image processing, computer vision and edge computing technologies to deliver benefits and improve efficiencies to the agricultural sector. Livestock counting is a critical component of livestock management.

Livestock including sheep are manually counted at exchanges and ports, with the potential for errors and inconsistencies. The project uses 5G to enable multiple high quality 4K video streams to count livestock at regional exchanges, automating the process and removing human error. A supporting 5G edge network process the counting on-site and relay the data in real time back to farmers on a tablet or mobile device. By minimising counting errors, especially during unfavourable conditions, will directly contribute over $13.2 million to the livestock industry each year.[7]

Smart and sustainable cities

Nokia and the City of Melbourne conducted trials using Nokia Scene Analytics artificial intelligence (AI) technology to develop a deeper understanding of waste disposal behaviour. This allows the City to tackle the issue of waste dumping more efficiently and keep laneways – the busy and narrow city streets and pedestrian areas – even more clean, safe and free of garbage.

Under its 'emerging technology testbed' initiative, the City of Melbourne worked with Nokia to leverage an existing network of installed cameras as internet of things (IoT) sensors to monitor one of the compactors. The Nokia Scene Analytics solution employed an AI-powered algorithm to filter and collate data from the cameras, while also combining other data sources, such as operational data on the compactor itself, to create real-time alerts and produce reports. Initial trial results demonstrate that Scene Analytics can support the City's objectives for better, safer citizen experiences while simultaneously lowering maintenance and down time costs for waste management services.[8]

Transport

In Perth, Western Australia Nokia was selected by the Public Transport Authority of Western Australia to modernise rail communications with private wireless and mission critical IP/MPLS covering 250 km of railway track and tunnels. The project includes designing and building and 5 years of maintenance for the PTA's communications system, with options for two additional lots of 5 years of maintenance. [9]

[7] Media release_5G and AI make counting cattle easy as 1 2 3 for smart farms of the future.pdf (tpgtelecom.com.au)
[8] Nokia and City of Melbourne trial AI technology to keep city streets safe and clean | Nokia

[9] Nokia selected by The Public Transport Authority of Western Australia to modernize rail communications in Perth with private wireless and IP/MPLS technologies | Nokia

Robotics

The '5G Connected Cobot' project located at the University of Technology, Sydney demonstrates how the higher speeds and lower latencies made possible by 5G technologies can enable cobots to interact with their surroundings – including nearby humans – in real-time.

Initial testing has shown that utilising Nokia's 5G capabilities to offload the processing required from the cobot to a computer "at the edge" extended its battery life as well as enhanced its performance. This approach can lead to significant power and cost savings, all while increasing the capabilities of the cobot.

During the testing phase of the project, the team added a variety of sensors measuring the world around the cobot. Multiple lidars were used to view the world as a dense collection of 3D points, like how autonomous cars operate. This allowed the robot to easily measure the distance and direction to people and objects around it with high accuracy.

Early findings suggest that fitting the cobot with a 5G modem to allow off board processing of its data marks a significant step towards ensuring collaborative robots can be the co-workers we want them to be in the future.[10]

5.1 Supporting emerging technology through a "zero-trust" approach

As society becomes increasingly dependent on telecom networks, and digitalisation progresses, expectations on network security continue to grow. Cybersecurity in the IoT and metaverse era will require close cooperation between regulators, governments and industries.

To promote national security, maintain uninterrupted functioning of critical infrastructure and industries, ensure network resiliency, and prevent and mitigate cyber-attacks, governments globally should consider and adopt principles that define both trusted suppliers and trusted supply chains. Trust is essential as 5G and fiber networks enable automation and digitalisation of many processes and services.

The infrastructure must ensure reliability, resiliency, and security to promote trust. This requires trust in both the suppliers (their behavior, compliance, capability) and the supply chain (ability to deter, detect, and mitigate risks to the equipment and software).

A "zero trust" approach to security does not remove the need to work with suppliers that are trustworthy and ethical. The main objective of zero trust is to increase the security posture of organisations and their assets (infrastructure and data) against threats and security risks. In an environment with networks under constant attack, customers should ensure that the

[10] Next-gen robotics advanced by Nokia 5G technologies - UTS Tech Lab

products and services incorporated into their networks are not provided by potential bad actors seeking to exploit vulnerabilities, today or in the future. In short, while a zero-trust architecture is more likely to detect and defend against a security breach, it does not supersede in any way to the requirement to choose only trusted products and services.

Governments are responding by enacting new laws and regulations, such as the EU toolbox for 5G security, the Indian Telecommunication Security Assurance Requirements (ITSAR), or the US President's executive order to improve cybersecurity and integrity of software supply chains.

Because the security of our technology is integral, Nokia has always undertaken extensive monitoring and testing (including independent validation) of our products, at all stages from inception and during development, manufacturing, deployment and maintenance.

All Nokia products and our supplies are subject to the same security verification procedures to ensure their integrity, regardless of their place of development, manufacture or operation. For example:

- Nokia imposes security by design throughout our value chain. Our comprehensive, industry-leading Design For Security (DFSEC) process ensures that security is embedded into every product from the start, undergoing rigorous security testing prior to commercial release.
- At Nokia, we continuously review our operations and supply chains to mitigate against potential disruption to our customers caused by natural disasters, transportation capacity and political risks. We have a supply and sourcing strategy that is not dependent on one facility, one manufacturer or one location.
- Like most electronics, telecommunications, and IT companies, we source products and components from various countries as part of a worldwide network managed by Nokia Global Supply Chain, which ensures the diversity and security of our production capabilities and enables us to manage potential disruption to supply.
- No matter where our equipment and components of our equipment are developed, manufactured or sourced, it is subject to the same strict protocols to ensure quality, security and integrity.
- Our supply chains are multiple test and assurance points where any interference or manipulation can be identified and traced. The depth and breadth of our security procedures makes interference with our products next to impossible.
- Nokia's commitment to promoting global security means we will provide passive lawful interception capabilities to customers who have a legal obligation to provide such capabilities. We will not engage in any activity relating to active lawful interception technologies, such as storing, post-processing or analyzing of intercepted data gathered by the network operator.

- We will not knowingly provide technology or services for the purpose of limiting free speech, political discourse or otherwise contributing to activities that are not consistent with internationally recognised human rights standards. You can read more about Nokia's commitment to human rights here - Human_rights_policy.pdf (nokia.com).

Nokia notes several Australian Government programs and initiatives are either completed, underway or up for review including and not limited the review of the Critical Technology Supply Chain Principles and ongoing requirements under the SOCI Act.

In particular, the regulation of critical infrastructure under the SOCI Act which expanded sectors deemed critical – from four to 11 – to ensure protection of Australia's interests and Part 2A which requires responsible entities to adopt and maintain a critical infrastructure risk management program. This positive obligation focuses on physical security, personnel security and supply chain security in addition to cyber security which should give consideration to the aforementioned. Nokia supports these programs and regulatory reforms to protect and educate Australian Government, businesses and organisations on security and supply chains with regards to critical sectors of the Australian economy.

Nokia also recommends that Governments adopt frameworks that go beyond technical product security, to also evaluate suppliers' strengths/weaknesses in the areas of business continuity, transparency of corporate governance, and track-record in delivering and maintain secure products. Nokia DFSEC, which incorporates international models for best practices, and promotes a culture of security throughout the entirety of the product lifecycle, serves as an excellent baseline for such a framework.