UNSW submission to the 2023-30 Australian Cyber Security Strategy Discussion Paper

UNSW Sydney welcomes the opportunity to provide input to the development of the 2023-30 Australian Cyber Security Strategy.

UNSW is one of Australia's leading research and teaching universities and is currently ranked 43th in the world (2022 QS World University Rankings). Through its *2025 Strategy*, UNSW is committed to research including cyber security that addresses some of the most significant challenges facing Australia and the world, as well as educating students to become highly employable skilled professionals.

UNSW looks forward to working together with the Government to improve Australia's cyber resilience and to ensure that the *2023-30 Australian Cyber Security Strategy* best delivers its intended outcomes for the nation.

Key Messages

Universities have a significant role to play in supporting the Government's cyber security agenda including:

- Educating both cyber technical professionals and other professionals who operate in the cyber environment (for example in critical infrastructure businesses) to address the cyber skills shortage and building resilience.
- Cutting-edge cyber research addressing both the general challenges and the specific problems of government and industry across the cyber security ecosystem.
- Continuous Industry engagement – leveraging the current best practice.
- Improve cyber resilience by educating the public about cyber threats.
- Supporting Government agencies and industry with cyber professional education.
- Improving cyber security within the tertiary system as a critical infrastructure asset.
- Thought leadership and policy making decision support.
- Building sovereign cyber capabilities.

Universities and cyber security

Universities are important stakeholders in addressing the cyber skills shortage in Australia. Our world-leading cyber academics and experts contribute regularly to policy discussions on current best practice both directly to government and industry and through the media. Universities work closely with industry to develop new knowledge in cyber and to innovate new technologies, practices and systems. Universities themselves are also institutions of critical infrastructure that have been the target of malicious cyber activity.

UNSW's own cyber security continues to be one of the University's highest priorities, and we are working closely with relevant government agencies to build on existing safeguards against foreign interference, and to maintain and improve cyber resilience through a collaborative process.

Through our UNSW Canberra faculty, located on the Australian Defence Force Academy base, UNSW provides a unique contribution to the national cyber ecosystem, educating all of the Australian Defence Force training officers, included dedicated undergraduate and postgraduate courses in cyber security provided only to Defence and government agencies. This education underpins much of Australia's cybersecurity Defence and National Security workforce. We seek to grow this commitment, noting we also face challenges in recruiting and retaining sufficient high-quality educators to provide this education.

UNSW Institute for Cyber Security (IFCYBER)

UNSW is currently ranked 26th in the world for Telecommunications Engineering (2022 Academic Ranking of World Universities Subject Ranking), supporting our leadership position in cyber security research and education. We are a founding partner of the Cyber Security Cooperative Research Centre, and in 2019 hosted the inaugural Australian Cybersecurity Education Summit which brought together leading cyber educators, industry and government professionals.

Since our last submission on the federal 2019 Cyber Security Strategy, UNSW has invested in the establishment of the Institute for Cyber Security (IFCYBER), bringing together efforts in all seven faculties, across both education and research in one of the largest centres of expertise outside of Government.

In the intervening period, many of the core challenges in Cyber Security have grown, while maintaining the defining characteristics of what are known academically as complex socio-technical problems. Aspects of these challenges impact across society and the economy in Australia, and worldwide.

From a cross-disciplinary perspective, the complexity of challenges in Cyber Security include:

- evolving threat capabilities and approaches;
- the fast pace of change in how Cyber Security is applied by industry practitioners;
- changes in applicable legislation and policy; and
- keeping research and education current and relevant.

Addressing these challenges requires a combined effort – sharing insights between the research, education and application domains and their relevance to society. Through IFCYBER UNSW seeks to

operate at this nexus point – generating close collaboration between researchers, educators and practitioners benefiting all stakeholders.

Across the seven UNSW Faculties, there are approximately 140 members of IFCYBER delivering Cyber Security in undergraduate courses, Professional Education, post graduate programs and conducting research funded through competitive schemes and direct contract research.

Supporting the national cyber agenda

UNSW supports the national cyber agenda in several key functions;

- **Education and Training**: UNSW is committed to educating the next generation of cybersecurity professionals. We offer a range of undergraduate and postgraduate programs in cybersecurity and have recently launched a new Master of Cybersecurity and Data Science program. We work with government to develop cybersecurity training programs for existing professionals and provide training to government personnel including at the Australian Defence Force Academy in Canberra.
- **Cybersecurity Research**: UNSW has a strong track record of conducting world-class research in cybersecurity. Our research covers a broad range of critical technology areas, including quantum cryptography (and the underlying quantum computing sciences), secure software engineering, and cybercrime. We collaborate with the government and industry to conduct research to understand and mitigate cyber threats.
- **Thought leadership:** UNSW has a team of experts who specialize in cybersecurity policy and law development, maintaining a database of relevant legislation and policy. We can work with the government to develop policies and regulations that are effective in improving cybersecurity in Australia.
- **Industry Engagement:** UNSW has strong connections with the cybersecurity industry in Australia and globally. Through IFCYBER we are extending our established collaborative research consortia models to cyber security. This lies outside the strict procurement rules of government allowing government to access development and test environments as occurs in other countries. We can thus work with the government to facilitate industry engagement and encourage the adoption of best practices in cybersecurity.
- **Cybersecurity Awareness:** UNSW can work with the government to raise awareness about cybersecurity among the general public. We can develop educational programs and campaigns that focus on promoting cybersecurity best practices and increasing awareness about cyber threats.

Tackling the cyber skills shortage

Beyond our bespoke Defence and national security enterprise offerings referenced above, UNSW is a leading provider of cyber security education, offering cutting-edge technical courses as well as ones that are designed to produce well-rounded cyber graduates skilled in strategy, ethics and diplomacy. UNSW also offers a range of professional education courses catering to industry professionals. As our expertise in the field has demonstrated, the best education combines theory with integrated, practical learning and cutting-edge research. Furthermore, universities such as UNSW are uniquely placed to collaborate on research efforts to ensure that cyber resilience keeps pace with the changing nature of cyber threats.

As well as education for cyber professionals, another important way to improve cyber resilience is to improve general community awareness around cyber risks, and easy actions to protect or mitigate against those risks (that is provision of cyber literacy as part of a broader digital literacy effort). Meeting this need is particularly important with everyday consumer items that are increasingly connected, becoming a risk, such as: smart phones, smart speakers, and other interconnected appliances. UNSW acknowledges the work of state and federal agencies towards this end, but nevertheless recommends that a broader public awareness and cyber literacy campaign would be beneficial, in combination with specific warnings relating to risky products. Consideration should be given to initiatives such as product labeling requirements, standards, warnings (for example, product ratings using a star system as occurs with energy efficiency) and enforcement of these rules by NSW Fair Trading.)

Responses to consultation questions

Question 1: What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

The Strategy should be broadly future challenge focused, rather than addressing contemporary challenges in data and infrastructure security alone. These aspects, while important are only the leading edge for cyber security challenges that we will face in the short space to 2030. The strategy might address this with some essential definitions as a foundation for common inclusive ground in discussion and action. Specifically:

a. Defining cyber security as a socio-technical problem, or system, requiring a broad range of actions and remediations beyond "technology" or "legislation". Internationally recognised elements of this socio-technical system include: Human, Organisational & Regulatory Aspects; Infrastructure Security; Systems Security (including underlying sciences like cryptography); Software & Platform Security and systems for Attacks & Defences[1]. From an academic standpoint these elements rest on foundations of critical mathematics, sciences and engineering, including, but not limited to quantum computing and cryptography. We see this level of detail as important because rapidly maturing technology such as quantum computing is assessed as *likely* to significantly challenge basic cybersecurity principles such as encryption in the time-frame of this strategy (i.e. by around 2030). This type of "break through" risk driver might be addressed in the strategy.

b. Noting that the UK has moved to a comprehensive national cyber strategy, the Australian strategy might consider adopting and adapting an earlier UK definition (2016[2]): ***Cyber security*** *refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.*

c. Further, noting that the strategy should be broader than data and infrastructure security, the strategy might helpfully define compromises to:

    i. data confidentiality – for example as actions, measures and systems to provide protection of data from unauthorized access and disclosure, including means for

[1] Adapted from: https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf

[2] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

protecting personal privacy and proprietary information.

ii. data availability – for example as actions, measures and systems to ensure that "your data" is available to the data owner (you) – and trusted agents and not subject to "ransom" or other delays

iii. data integrity – or trusted data – for example as actions, measures and systems to ensure that "your data" is not altered except by the data owner (you) – and trusted agents

However, while the data compromises of the recent attacks in Australia are front of mind, a strategy that limits the Australian response to data and information security will have serious deficiencies. Thus, we recommend that these definitions be extended to "layers" covering the cyber security definition, as cybersecurity action stands or falls on this type of bedrock definition.

To support action and implementation, whether in terms of legislation or investment, the Strategy might usefully recognise the scope of responsibility, and vulnerabilities (or "threat surfaces") for: individuals (e.g. but not limited to personal data, privacy etc); industry covered under SOCI act; industry not considered critical, but bound explicitly or implicitly through privacy legislation in data handling (e.g. trades peoples) and government(s) of all levels and the relationships between one another. The strategy might seek to describe future state (and gaps) for each of these groupings – perhaps in terms of the data (compromise) definitions above.

This is particularly important because individuals do not have complete agency over the confidentiality, availability or integrity of personal data, after it is required to be provided to second and third parties for legitimate reasons – social and economic. Nor do companies have agency over all cyber systems reported to and share with governments. This interaction "pools data" and creates a threat surface and "data" risk.

The Strategy might recognise at least three types of threat or breach and responsibilities for responding to that type of threat:

a. a cybersecurity breach that comprises individual's data – typically through a cyber criminal act;
b. threats which mass or aggregate data from one or more sources that might represent a systemic economic or social compromise; and
c. threats which directly compromise a connected system

While the present day focus tends to be on type a) breaches above (e.g. Medibank and Optus), the security of these are the essential responsibility of the data holders. Type b. and c. threats are more likely to be associated with state actors and risk a broader compromise and this risk are the exclusive preserve of government.

The Strategy might also usefully consider investment in research and other investment in fast moving underlying sciences and technology that is required within the strategy timeframe. This includes Zero Trust Architectures (ZTA), "Safe to market" software development and integration and quantum computing and associated cryptography. This dedicated investment is required in addition to the current competitively funded research mechanisms to keep pace with the technologies being developed by allies as dictated in 2021 for example in the US federal system[3].

Question 2: What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

[3]See https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

UNSW notes that there is a plethora of interacting legislation – covering many aspects including privacy, data retention times and a host of others – across all levels of government and industry. These time data is held and interactions between data repositories generates the target data pool, (or threat surface) that may pose an unnecessary risk. A comprehensive study of the risks that each of these pieces of legislation, regulation and policy introduce to the threat surface is required before reform. This work might build on and fund some recent work: the Cyber Law Mapping Project[4]

Question 2 (a): What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

A comprehensive study of the risks that each of these pieces of legislation, regulation and policy introduce to the threat surface is required before reforms should be considered.

Question 2 (b): Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Yes – this might include reforms across legislation and if the SOCI act is to be broadened beyond infrastructure, the reforms might usefully address compromise definitions (above) and in risk terms to individual data types, the company operations and risk to cascade failure if certain types of data with broader societal or economic implications are comprised, held unavailable, or the data integrity altered.

Question 2 (d): Should Australia consider a Cyber Security Act, and what should this include?

Any new Act should be considered in concert with a review of the significant overlaps in legislation, policy etc.

Question 3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Australia has a strong track record of implementing robust cyber frameworks and promoting cyber education to enhance its own cybersecurity posture. This expertise could be exported to improve regional cyber resilience, particularly in the Asia-Pacific region, which is experiencing an increasing number of cyber threats. One opportunity for Australia is to provide training and capacity-building programs for developing countries in the region. This could include cyber education programs for government officials, businesses, and the general public, as well as technical training for cybersecurity professionals. By sharing its best practices, Australia can help these countries develop their own cyber frameworks and improve their cybersecurity posture.

Question 4: What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

This needs to be considered as a question within government and within CI sectors. Australian (Govt) should leverage existing and developing partnerships. For example, UNSW is working with AUKUS partners under the Plus Alliance, with University of Maryland (ARLIS) and partners in the US and through Mitre Corp and large cyber Primes to leverage bi and multilateral higher ed cybersecurity partnerships.

[4] See https://austlii.community/wiki/CyberLaw/.

Question 11: Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Yes – UNSW recognizes cyber security as a "socio-technical issue" … skills uplift in both the workforce and the general public need to address the whole social and technical system – as described for example by the UK CyBOK. Importantly, we recognise at least three meta families of skills – those required by "cyber technical operators" – those skills commonly found in employees of cyber security agencies and companies and requiring a deep technical basis; "cyber policy workers" – typified by those in other parts of government, but requiring non STEM skills; and lastly the advanced cyber literacy skills of everyone employed in for example critical infrastructure roles. Without the whole system, the cyber technical skills are used reactively.

Question 12: What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

As outlined in our introduction, UNSW is a primary education provider for the "landed" cyber security workforce. Noting that many roles will require background checks to clearances, government could assist by:

1. Considering fee waivers for Australian Citizens in identified cyber security courses – and at the same time commencing clearance process early for eligible students;
2. Providing migration assistance for foreign nationals from certain countries, and clearance initiation while study is undertaken. Considering a three year degree and some postgraduate study, such migrants would be available for sensitive roles not long after the conclusion of their education.

Accreditation might be addressed through two avenues:

1. accreditation of courses or topics in courses: this is difficult as the course content is necessarily very dynamic beyond introductory courses in cyber security
2. accreditation courses for individuals to an agreed industry standard across job families. This work might leverage the initial steps taken by the Digital Skills Organisation (Dept of Education), but to be useful must extend up the Australian Quality Framework from the current VET training system focus across a few job families.

Question 13: How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

Government should begin to take risk analysis and "red team" approaches and respond accordingly. … Some major cyber security incidents (such as cyber crime) impact a large number of individuals … Govt supports them with identity / financial recovery … However, these and others should be red teamed and analysed to determine how the major information loss could be used by mal-actors to compromise other parts of the critical infrastructure

Question 13a: Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The Government may consider adopting best practice (no fault reporting) models such as those employed in aviation for example by the Civil Aviation Safety Authority (CASA). The no-fault reporting model is a reporting system that encourages aviation professionals to report safety incidents and near-misses without fear of punitive action or blame. This reporting system is designed to create a culture of safety by encouraging open communication about safety issues, which helps to identify and

address potential safety hazards before they cause harm. This also means that aviation professionals are more likely to report safety incidents and near-misses, which helps CASA to identify potential safety hazards and take steps to mitigate them.

A similar model would work for reporting of cyber incidents.

Question 15: How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Improving cyber security best practice and knowledge and behaviours is a shared responsibility of government and industry best achieved by working in partnership with Australian education providers. UNSW works with industry practitioners to structure courses that deliver the latest in cyber literacy knowledge and best practice.

Question 15 (a): What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Like many others, we have identified a need for small businesses (and larger) to be provided with cyber security education and training at the "C-suite" level (Cyber literacy for management). This education is role specific. Importantly, it differs from the "technical cyber security education" required by the "cyber security workforce" and the foundational "cyber literacy" skills that should be a progressive system of education from some point in schooling – much the same as language, maths and digital literacy. Cyber literacy education for managers must address the applicable law policy and risk frameworks and their interaction.

Question 16: What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Supporting collaborations between universities, industry and government, is a key opportunity for government to enhance the uptake of cyber security services and technologies in Australia.

UNSW advocates for Government to extend our IFCYBER research and education framework to involve research with practitioners and our partner companies to conduct on-going assessment and development of new technologies with cyber security practitioners. This approach acknowledges that a good fraction of the new "emerging technologies" (for example Zero Trust Architecture systems) will need to be tested and integrated into the Australian cyber eco-system. This can and should happen outside government as well as inside.

Question 17: How should we approach future proofing for cyber security technologies out to 2030?

UNSW advocates for Govt to use the IFCYBER framework to involve research with practitioners and our partner companies to conduct on-going assessment and development of new technologies with cyber security practitioners. This approach acknowledges that a good fraction of the new "emerging technologies" (for example Zero Trust Architecture systems) will need to be tested and integrated into the AS system. This can and should happen outside government as well as inside

Question 19: How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

UNSW advocates for Govt to use the IFCYBER framework to involve research with practitioners and our partner companies to conduct on-going assessment and development of new technologies with cyber security practitioners. This approach acknowledges that a good fraction of the new "emerging

technologies" (for example Zero Trust Architecture systems) will need to be tested and integrated into the AS system. This can and should happen outside government as well as inside

Question 20: How should government measure its impact in uplifting national cyber resilience?

If the strategy is framed in capability and risk terms the measures would be reduction in both the "operational risk" – the day-to-day likelihood and consequence measures for attacks in various categories and in reductions in "capability risks" – such as workforce. The strategy might then consider adopting a measures approach similar to that described in the UK National Cyber Strategy 2022[5], wherein two evaluation mechanisms are discussed – a sensitive evaluation against a performance framework, guiding detailed evolution of strategy and a public annual report, guiding public policy and action. Aspects of the sensitive evaluation might be shared with entities identified in Acts such as the Security of Critical Infrastructure.

Question 21: What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

If the measures approach similar to the UK National Cyber Strategy 2022 is adopted as noted above, public transparency could be achieved through an annual report, preserving the sensitive evaluation information separately. Where the sensitive evaluation information is shared that should be accompanied by a co-commitment for input to address critical gaps.

Conclusion

If you would like any further information, please do not hesitate to contact the Director, UNSW Institute for Cyber Security at ifcyber@unsw.edu.au.

[5] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf