Australia's National
Science Agency

CSIRO Submission to 2023-2030 Australian Cyber Security Strategy Discussion Paper

CSIRO Submission 23/820

April 2023

Main Submission Author(s):
Liming Zhu and Surya Nepal

Enquiries should be addressed to:

E GovernmentRelations@csiro.au

Contents

Executive Summary

In this submission, CSIRO suggests several key ideas for consideration as part of the 2023-2030 Australian Cyber Security Strategy to uplift Australia's cyber security posture, protect Australia's critical infrastructure, reduce cyber security risk management and compliance cost, improve cyber resilience, and support exports and regional leadership. These ideas include:

- Focus on the intersection of cyber security with other emerging technologies;
- Connect cyber security risks with other organisational risks;
- An integrated approach for critical infrastructure sectors;
- Foster collaboration at scale and speed;
- Tackle challenges in software and digital aspects of supply chains;
- Understand the security of emerging platform technologies, e.g., Digital Twins, Augmented Reality (AR)/Virtual Reality (VR)/Extended Reality (ER);
- A focus on metrics, measurement, and Testing, Evaluation, Verification and Validation beyond documentation standards;
- Create a better understanding of the costs associated with implementing governance and technical controls within the organisational context;
- Use science and technology to inform policies regarding liability shifts and market incentives;
- A national initiative for the development and operation of meta-security techniques to promote innovation, adoption, and commercialisation of cyber security research outcomes from local Australian universities and research organisations;
- Cyber security by-design in the context of energy transition, environment, and climate change; and
- Human-centric cyber-defence at scale.

Introduction

CSIRO welcomes the opportunity to provide input to the 2023-2030 Australian Cyber Security Strategy discussion paper.

CSIRO is Australia's national science agency, with a crucial role in solving the country's biggest challenges through innovative science and technology. One of these challenges is to "Secure Australia and its region". To accomplish this, CSIRO conducts mission-driven cyber security research, such as through its Critical Infrastructure Protection and Resilience mission. Missions are large-scale scientific and collaborative research initiatives aimed at making significant breakthroughs. This cyber security research covers a range of areas, including critical infrastructure security, 5G/6G security, governance and technical controls of cyber security, automated compliance, software supply chain security, Internet of Things security, human-centred security, Artificial Intelligence (AI) security, post-quantum cyber security, and privacy.

CSIRO actively contributes to the development of multiple security-related international standards and conducts research on their implementation and adoption. It operates research infrastructure securely to deliver cross sector outcomes across within Australia and overseas, including government, research institutions, commercial entities, and other non-governmental sectors. Through its work, CSIRO contributes to building trust and confidence in Australia's digital economy and critical infrastructure.

This submission addresses selected questions in the discussion paper that relate to CSIRO's scientific and technological expertise. CSIRO welcomes the opportunity to discuss these matters in more depth with the Department of Home Affairs. Please refer to enquiries details on cover page.

CSIRO Responses to the Terms of Reference (ToR) & Questions

Q1: What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

CSIRO would like to suggest the following ideas for consideration as part of the 2023-2030 Australian Cyber Security Strategy:

Idea 1: Focus on the intersection of cyber security with other emerging technologies.

Emerging technologies, such as Artificial Intelligence (AI), Quantum, 5G/6G, distributed ledgers, and clean energies, have significant implications on cyber security threat vectors, policy levers, governance, and technical solutions. Due to their rapid development, continuous analysis and experimentation are essential to keep up with the implications. This requires deep sovereign science and technology capabilities in a semi-open environment that supports judicious international collaboration.

The program of work required goes significantly beyond desktop research on technology trends and potentials. It requires testbeds, experimentation, and applied research and development from an integrated team of experts in both cyber security and emerging technologies. For example, the Department of Home Affairs has established a 3-year research and development program on 6G security with CSIRO, where cyber security implications of 6G, including its intersection with AI and Quantum, are systematically investigated.

One area of particular importance in the emerging technology landscape is the quantum threat to cyber security systems. This demands diligent work on testing, benchmarking, and implementing both post-quantum and classical cryptography algorithms and quantum key distribution-based systems to ensure a smooth transition of cyber security infrastructure to the post-quantum era. CSIRO's Quantum Technology Future Science Platform has started work in this area.

Idea 2: Connect cyber security risks with other organisational risks.

An increased focus on the fiduciary obligations of board members and executives, connecting their business objectives with the cyber security requirements, is needed to ensure that good cyber security governance and management are in place and supports the primary business objectives.

Under the Australian critical infrastructure regulatory regime, directors must execute their non-fiduciary obligations to protect entities from cyber compromise reasonably. Organisations, especially at the board and executive level, are facing an increasing list of cyber security risks. Despite their prominence and regulatory pressures, cyber security risks must compete with other risks, including privacy risks, AI risks, supply chain risks, ethics and license to operate risks, and environmental, social, and governance risks. The existence of various applicable standards and frameworks complicates the perception of cyber security risks across sectors, particularly in terms of the information directors need to make informed decisions about cyber risks. These risks are often managed in silos, with each responsible unit competing for resources.

When an integrated risk approach is discussed, it usually focuses on how different parts of the organisation can be marshalled into a coherent plan to address a single risk. However, this approach fails to recognise that other risk areas are also asking for similar solutions, resulting in multiple “coherent” plans competing and overlapping with each other.

Despite these challenges, many governance and technical controls for different risks are similar or even the same. For example, provenance and system integrity technologies create trustworthy registries and integrity-assured links between data, code, model/AI components, predictions, decisions, and actions. Such controls, once put in place, can have positive impacts on all risk areas, significantly reducing costs and complexity compared to each risk area devising its own solutions. We need to address the need identified to translate threat information (such as the information obtained from a malware information sharing platform or from cyber threat intelligence) to impact opportunities. This can be done by assessing how organisational risk appetite changes and how different adversaries impact directors’ ability to make cyber security related decisions.

Another example from an adjacent field is an approach to managing AI risks (including the security and privacy of AI), where the responsible AI pattern catalogue connects risk mitigation approaches across teams, organisations, and industry levels, different stakeholders, and different technological concerns. It also integrates with the “social” and “governance” risks. Multiple approaches can be taken to break down the risk silos and allow governance and technical controls in cyber security to contribute to other risk areas and vice versa.

Idea 3: An integrated approach for critical infrastructure sectors.

The Security of Critical Infrastructure Act 2018 (SOCI Act) was amended in 2022 to strengthen the security and resilience of critical infrastructure by expanding the sectors and asset classes. This amendment presents an opportunity to:

1. Focus on an all-hazard integrated approach across cyber security, physical security, and (software) supply chain security and their resilience;
2. Tackle challenges in intra/inter-sector dependencies and system of systems; and
3. Reveal shared system vulnerabilities and consequences analysis (including unintended mitigation consequences) beyond siloed single-hazard analysis.

To respond to the science and technology challenges presented by these new opportunities, we need to take an integrated approach to threats, system vulnerabilities, and governance and technical controls. The aim is to significantly reduce the cost of regulatory compliance while revealing previously unknown unknowns. The science and technology developed will benefit both critical infrastructure operators and sovereign critical infrastructure solution providers, enabling them to leverage trust and science and technology differentiators to export to the region and other allied countries.

CSIRO’s new Critical Infrastructure Protection and Resilience mission is an example initiative in this area. The science and technology-focused Critical Infrastructure Protection and Resilience mission has started with the following priority sectors: energy (power grids and distributed/consumer energy resources), supply chains (e.g., critical minerals, manufacturing, transport, and software), telecommunication, and financial services.

Idea 4: Foster collaboration at scale and speed.

Collaboration is crucial for achieving cyber security and resilience, especially when it comes to critical infrastructure. To do this effectively requires science and technology that enables owners/operators of critical infrastructure, governments, product vendors and service providers, and other stakeholders to collaborate at speed and scale. However, many barriers exist to such collaboration, as highlighted in the US National Cyber Security Strategy. These barriers include limited willingness to share organisational-confidential information with regulators or national security agencies, trust issues in decentralised approaches for defending critical infrastructure in a zero-trust environment, data sensitivity issues, and technical challenges in machine-to-machine and human-to-machine teaming. These challenges can be addressed using the following approaches:

- By building trusted cyber security data sharing platforms, cyber security data can be shared between industry, regulators, operational security agencies and researchers. This can occur in international collaborations as well. One good example of such platforms is the US Department of Homeland Security's Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT) program for cyber security data sharing for research. CSIRO has been Australia's coordinator for the IMPACT program. CSIRO also routinely undertakes research using industry sectors' data or government data with appropriate firewalls in between.
- By leveraging distributed trust technologies and federated machine learning and analytics, collective trust can be achieved even with untrustworthy individual nodes and organisations. There is a need to explore threat intelligence sharing and coordinated cyber security response using distributed trust technologies assuming a zero-trust architecture.
- Sensitive data is often an issue in cyber security and resilience, ranging from privacy sensitivity to commercial and national security sensitivity. There is a need to develop a range of technologies for sensitive data sharing, such as treating data before release, federated data analytics without copy-sharing data, and secure enclave technologies that enable analytics/models to travel to data (rather than the other way). The secure enclave technology includes preventing certain analysts from viewing the data but with an informed response and auto examining the output to prevent piggybacking. The secure enclave technology goes beyond the current state-of-practice of a highly secured virtual environment for remote analysts to log in, view the data and conduct analysis.

Idea 5: Tackle challenges in software and digital aspects of supply chains.

Software plays a critical role in modern equipment, factories, and critical infrastructure. However, it is rarely written from scratch by contracting suppliers, instead containing components from dozens, if not hundreds, of the third and fourth party and open-source systems contributed by individuals and organisations globally. In addition, due to talent shortages and insights gained from deploying the same system in various settings, suppliers often provide remote diagnosis and control outside of Australia's jurisdiction, particularly during times of crisis.

The integrity of the software and remote-control operation process/context has become a significant challenge. In many supply chains, the most overlooked and pernicious issues stem not from supplier entity or equipment diversification but from the software inside. Even seemingly diverse suppliers and very different equipment can share the same software base and software suppliers, including open source. Therefore, the Biden Administration's Executive Order (14028) on Improving the Nation's cyber security requires software vendors to provide a software bill of materials. This vendor requirement will have significant implications for Australian companies exporting to the US and other regions.

CSIRO has started to look into this area by conducting deep research into software supply integrity in collaboration with the US's national research, standard institutes, and major tech vendors. The focus is on software related to critical infrastructure and sovereign capabilities, as well as trusted knowledge and component repositories. This research aims to identify potential vulnerabilities and improve the integrity of software supply chains.

Idea 6: Understand the security of emerging platform technologies, e.g., Digital Twins, Augmented Reality (AR)/Virtual Reality (VR)/Extended Reality (ER).

As the digitalisation of our world progresses, advanced sensing, data analytics, AI, and simulation are being integrated to create connected digital twins of the physical world. These digital twins are designed to help plan, monitor, diagnose, and actuate with greater efficiency and intelligence. Digital twins can potentially revolutionise critical infrastructure industries, such as digital manufacturing automation, by enabling collaboration between workers and objects on machine tools, processes, factory capacity, and staffing.

The digital twin market size is projected to reach US$73.5 billion by 2027[1] and is being promoted as a software platform by companies and labs, such as IBM's Digital Twins for Ports and Siemens' Digital Twins for the energy grid.

However, these emerging assets also expose new classes of threats, such as model and decision integrity, data and intellectual property theft. For example, an attacker can steal and manipulate the digital twin of a piece of critical infrastructure to perform an attack on the physical infrastructure. Furthermore, most of these digital twins can only maximise their value by connecting with the external world to receive up-to-date data from suppliers, sensors, and other digital twins. As such, there is a strong need to develop and adopt technologies that ensure the trust and security of connected digital twins.

Digital twins are also vulnerable to cyber-attacks, including impersonation and clone attacks, and this is a major challenge to their widespread adoption. Examples of cyber-attacks have been demonstrated, such as impersonating controllers in a digital twin scenario to inject malicious messages and execute operations on the control logic.

[1] https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html?gclid=Cj0KCQjw8qmhBhClARIsANAtbofV4ztufgJsuXup9LjcUsV8DHp5WqiaWu8Qe1oyCo_VS9whUR-iZkgaAsZEEALw_wcB

Extended reality technologies, including Extended Reality (XR), Augmented Reality (AR) and Virtual Reality (VR), are seeing increased adoption across a range of critical industries and applications. Digital manufacturing applications, such as assembly instructions and maintenance, education and training, military and defence, architecture and construction planning and management, as well as smart cities and infrastructure, entertainment and gaming, and retail and e-commerce, are among those that are currently leveraging these technologies. However, the adoption of these technologies also brings significant cyber security risks. Denial-of-service attacks can disrupt critical real-time services, while digital identity fraud through deepfake technology poses a challenge for identity verification. Furthermore, data privacy risks are a major concern due to the sensitive information these devices collect.

Idea 7: A focus on metrics, measurement, and Testing, Evaluation, Verification and Validation beyond documentation standards.

One commonly understood approach to achieving regulatory and policy harmonisation is to refer to the same standards or de-facto standards developed by standard-setting organisations, consortiums, or trusted research organisations. However, this approach is only a good first step.

Many well-known standards are “documentation” standards that stay at a high level with deliberate ambiguity to deal with the rapidly changing landscape and relatively slow update of standards. This creates a significant gap between standards and their implementation. A recent study, BASESPEC (Kim et al. 2021), compares vendor implementation and cellular specification through a systematic inspection of standardised message structures. By comparing extracted message structures with those in the specification, BASESPEC identifies mismatches and reports potential vulnerabilities or developer mistakes SMEs struggle to understand and produce high-quality implementations of the standards, and flaws in implementation are common even in large enterprises. Certification of standard conformance often relies on human-intensive consulting and auditing services, which are unaffordable to SMEs and have variable outcomes.

That’s why some standards organisations, such as the National Institute of Standards and Technologies in the US, pride themselves on going beyond “documentation” standards with a strong focus on machine-understandable standards, metrics/measurement, and associated Testing, Evaluation, Verification and Validation technologies. The National Institute of Standards and Technology also plans out roadmaps post-standard release. For example, in the AI risk management space, the post-standard roadmap, including the collaboration with CSIRO, includes Testing, Evaluation, Verification and Validation research and development and tools, automated compliance, sector and SME-specific risk profiles, and associated reference implementations for SMEs and well-known trade-offs between cyber security and other desirable outcomes. This is a good model to be applied to cyber security with the consideration of Australia’s local context, regulation, policy, and industry priorities.

Providing technology and research and development support beyond documentation and post-standard release is critical for enabling low-cost and high-quality adoption of standards that support associated policy and regulatory initiatives. Many organisations do not have in-house software development capability and depend heavily on procurement. Australia also does not have a large software house domestically. Therefore, we need to partner with a global software provider to deliver a realistic, practical solution for the diverse Australian market. This makes software security and compliance assessment a critical and regular operation that organisations have to perform.

The correct use of cryptography is the key to ensuring data security in modern software systems. As a result, several academic and commercial static analysis tools have been created to identify and address instances of crypto-API misuse (S. Fahl et al. (2012); S. Rahaman et al. (2019); D. Sounthiraraj et al. (2014)). Nevertheless, ensuring the appropriate application of cryptographic primitives has been historically challenging. Large Language Models can be used to address this challenge. CSIRO has investigated the use of transformer-based models to identify cryptography in source code, identify which cryptographic algorithms are used, and assess their compliance through compliance checks.

Idea 8: Create a better understanding of the costs associated with implementing governance and technical controls within the organisational context.

Every organisation has a unique cyber security risk appetite and tolerance based on its specific context. Therefore, the goal is not just to minimise cyber security risks, but to reduce them below the risk appetite level while considering other factors. These factors include adopting more user-friendly, cost-effective, and less restrictive governance and technical controls that do not slow down product releases or innovation cycles. However, the costs and security implications of these controls, especially in the context of each organisation, are not well understood.

For instance, organisations often receive threat intelligence about newly discovered vulnerabilities. However, there is a significant difference between a vulnerability and its context-dependent exploitability. Organisations need to understand not only if their components or service providers have vulnerable elements, but also the context in which they are deployed. For instance, whether they are in use, exposed in the attack surface, deeply hidden behind other security controls or critical to complex systems or not.

To reduce the costs of risk controls without increasing risks, Australia needs to collaborate with international tech vendors and local corporations on new science and technology that consider the exploitability of vulnerabilities in deployment contexts.

Idea 9: Use science and technology to inform policies regarding liability shifts and market incentives.

The US's National Cybersecurity Strategy 2023 proposes leveraging market mechanisms and reformed liability regulations to incentivise long-term investment in cyber security. However, to inform liability shift, responsibility sharing and incentives, it is necessary to have a thorough understanding of the cost of governance and technical controls in an organisation, supported by Testing, Evaluation, Verification and Validation. Achieving this requires a science and technology approach that includes the following:

- Understanding the context-dependent cost of different types of governance and technical controls, so that expectations for different types of organisations can be reasonable;
- Understanding the software supply chain and cross-organisational system dependencies to inform incentives and liability shift goals; and
- Using Testing, Evaluation, Verification and Validation to support the monitoring and enforcement of an organisation's governance and technology control.

Idea 10: A national initiative for the development and operation of meta-security techniques to promote innovation, adoption, and commercialisation of cyber security research outcomes from local Australian universities and research organisations.

Australian organisations routinely suffer from the threats of cyber-attacks, and they are always looking for innovative and effective ways to combat attackers. On the other hand, Australian research organisations, including CSIRO, produce every year many innovative cyber security techniques, but these techniques mostly remain restricted to paper publications or patents, and are not generally deployed to address cyber security problems encountered by Australian organisations.

Australia needs meta-security techniques that aim to enable a platform and ecosystem that consistently manage the new cyber security techniques developed in Australia at their early Technology Readiness Level stage. The meta-security techniques depend on multi-disciplinary knowledge (e.g., Cyber security, AI/machine learning, distributed systems, etc.) to ensure the correctness and reliability of new cyber security research outcomes by comprehensive evaluation, the management and storage of cyber security techniques with long-term accessibility to end users and repeatability, and consistent interfaces for better compatibility and composition.

The platform based on meta-security techniques will encourage Australian researchers to consider the impact of their research beyond paper publications. Meta-security techniques and its enabled platform will likely promote the innovation capability of Australian researchers and provide a new interaction channel among researchers and organisations. The platform enabled by meta-security techniques is complementary with other services that recommend mature commercial cyber security products.

It is desirable to have a national initiative to support the development and operation of meta-security techniques to keep Australian cyber security research outcomes reliable, accessible, and usable to the Australian organisation at the time they are needed.

Idea 11: Cyber security by-design in the context of energy transition, environment, and climate change.

As highlighted in the US National Cybersecurity Strategy 2023, ensuring cyber security during the transition to new energy ecosystems is crucial. This includes both distributed energy resources and consumer energy resources, such as electric vehicles and air conditioners. The transition provides an opportunity to incorporate security measures by design in a continuous manner.

Digital technologies, including satellite monitoring and digital twins, are also used for mitigation in the areas of environment and climate change. However, geospatial data, which is essential for climate adaptation, may contain sensitive information, especially combined with other data sources. As mentioned in Idea 6, the security of digital twins is another area of research that is gaining momentum in industry and academia.

Idea 12: Human-centric cyber-defence at scale.

As highlighted in the 2023-2030 Australian Cyber Security Strategy discussion paper, AI and quantum computing advances are shaping the cyber security threat (and defence) landscape. It is inevitable that in the future, most cyber offence and defence solutions will increasingly be AI-enabled. According to the US National Cybersecurity Strategy 2023, the burden of mitigating cyber risks primarily lies with the end-users, small businesses, and state and local governments with limited resources and competing priorities. Australia also faces a similar situation, in which the shortage of skilled cyber security professionals poses an immense challenge for cyber defence at scale. Addressing this requires a multi-pronged approach that includes the following:

1. **Developing science and technology for effective human-AI collaboration to enable cyber defence at scale:** Humans and AI have complementary skills that can be leveraged to strengthen cyber security at scale. Several fundamental science questions related to Human-AI collaboration need to be answered, including: (i) how should Human-AI collaborative systems be designed? (ii) how should humans and AI share situational awareness? (iii) how/when/what should humans and AI communicate when working on a shared objective? (iv) what skills will humans need to work in a collaborative environment? and (iv) what is the nature and function of human trust? There are some initiatives in this direction, including building augmented cyber defence capability by Cyber Security CRC and Collaborative Intelligence (CINTEL) Future Science Platform by CSIRO.

2. **Developing appropriate tooling to support the non-technical aspects of cyber security:** As identified in the 2023-2030 Australian Cyber Security Strategy Discussion Paper, it is equally important to consider both technical and non-technical elements of cyber security. Non-technical aspects include planning and governance, culture, and risk management. This includes (i) developing cyber security strategy tools to support boards and executive decision-makers, (ii) gamification of cyber security awareness training and digital upskilling for executive decision-makers and boards of directors, (iii) cyber security resilience and hardening through customised maturity framework development, and (iv) benchmarking cyber security capabilities across government agencies (with a particular focus on non-technical elements).

3. **Developing a national strategy to strengthen the cyber workforce:** Australia continues to face a critical skills shortage in the cyber security sector. This is reflected in the 2023-2030 Australian Cyber Security Strategy discussion paper, which identifies supporting Australia's cyber security workforce and skills pipeline as a key area for potential action. Any such initiative needs to be aligned with the development of an Australia-specific cyber security skills framework that (i) incorporates current initiatives and best practices to facilitate effective workforce planning and recruitment, (ii) enables training and development of individuals and teams, (iii) defines clear pathways for cyber security professionals, and (iv) provides means for recognising competencies and gaps in the cyber security workforce. Developing such a framework involves the participation of government, employers, education providers, and job seekers.

Q2: What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

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)?

As mentioned in Q1, Idea 7, a common approach to achieving regulatory and policy harmonisation is to refer to the same standards or de-facto standards developed by standard-setting organisations, consortiums, or trusted research organisations. However, learning from the National Institute of Standards and Technology's approach, it is crucial to:

1. Go beyond documentation standards.
2. Develop Testing, Evaluation, Verification and Validation technologies to reduce the cost of compliance while increasing the level of assurance, and
3. Have a roadmap for post-standard activities.

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?

As mentioned in Q1, Idea 8, it is crucial to have context-dependent and cost-effective cyber security controls on data and systems, as they have different values and sensitivity. In terms of data, it is essential to understand its intrinsic sensitivity and utility, as well as its potential sensitivity and utility when combined with other datasets. Deep science support using information theory or differential privacy is required for such assessments.

Once the sensitivity and utility of the data are understood, a spectrum of cost-efficient control technologies (as mentioned in point 3 of Idea 4) can be utilised for its use and sharing.

Software systems control all modern critical assets. As discussed in Idea 5, the software supply chain and remote-control process are among the most pressing challenges for critical infrastructure protection. In addition, the deployment-context-based assessment of the exploitability of vulnerability is crucial for reducing compliance costs without ignoring risks. CSIRO has started work on software systems related to critical infrastructure, aiming to create a trusted repository of critical components with associated guidance for its deployment-context-based assessment.

c) Should the obligations of company directors specifically address cyber security risks and consequences?

Cyber security governance, risk and compliance are critically important in the context of company director obligations. Directors could face civil or criminal charges for failing to ensure reasonable steps are taken to protect their organisations against cyber-attacks. As mentioned in Q1, Idea 2, there is a danger of introducing new risks as a separate to the already long list of risks that company directors have to manage. This may strain already limited risk management resources and result in the waste of risk-specific solutions without leveraging existing risk controls. Idea 2 outlines some approaches to solving this dilemma.

The ASX found that only 7% of directors understand the broader cyber security context in which the company operates, and only 37% understand IT security exposures (ASX, 2017). If cyber threats can impact a company's operations, leading to downtime or a complete shutdown, affecting a company's reputation and having flow on affects to their client base, causing financial losses and impacting the fiscal year's profit, then it should be the responsibility of company directors to ensure that their organisations are prepared to manage cyber security risks effectively. This includes implementing robust security measures, regularly assessing and testing systems for vulnerabilities, and providing training to employees on cyber security best practices.

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

Nil Response.

e) How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

In Q1, Ideas 7 and 8, we outlined several approaches for Testing, Evaluation, Verification and Validation-based monitoring and means of reducing regulatory costs, such as automated compliance, SME/sector-based profiles, reference implementations, and deployment-context-specific risk assessments with a focus on exploitability.

f) Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances? What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies, and insurers?

Nil Response.

g) Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Nil Response.

Q3: How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

As outlined in Q1, Idea 4, there are several barriers to coordinating cyber resilience across organisations and jurisdictions within Australia. However, the science and technology developed to overcome these barriers could also be extended to regional collaboration and response. As the trusted national science agency, CSIRO can initiate and facilitate such collaborations and help upskill participants. For example, CSIRO is planning to launch a cyber security and AI placement program for employees from Indonesian public services. Through this intensive 3-month program, public service employees from Indonesia will be exposed to the latest cyber resilience and collaboration technologies to appreciate their benefits.

CSIRO has also built a strong collaborative relationship with New Zealand. Along with Australian partners (Monash University, University of Queensland, Victoria University of Wellington, La Trobe University, Macquarie University, Swinburne University, The University of Melbourne, University of Central Queensland, and University of Technology Sydney) CSIRO formed a three-year Trans-Tasman Cyber Partnership program with New Zealand partners (at University of Waikato, Massey University, University of Otago, University of Canterbury, and University of Auckland). This partnership is focused on developing a coordinated national community for domestic cyber security research, increasing high-quality trans-Tasman cyber security research capability, and integrating the New Zealand and Australian cyber security research ecosystem.

The partnership is tasked with addressing science and technology challenges at the intersection of AI, quantum, and human factors. Specifically, to develop automated threat response methods with real-time situation awareness, AI-based response planning and a multi-level threat response with automation and self-evolving capabilities; to look at where AI can be used to automatically optimise cyber security tools to reduce the work needed to be done by human experts; and to determine the implications of quantum computing and post-quantum cryptography for current national security tools and systems, particularly in the New Zealand and Australian context.

As mentioned earlier in Idea 4, CSIRO has already served as Australia’s coordinator for cyber security data sharing for research with the US Department of Homeland Security via the IMPACT program. With this expertise, Australia could potentially become a regional coordinator.

Q4: What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

As mentioned throughout this submission, CSIRO is currently engaged in active collaborations with like-minded countries such as the US, United Kingdom, India, and New Zealand in the field of cyber security. There are several opportunities to elevate these collaborations.

Q5: How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

CSIRO provides experts to several cyber security-related standards committees and working groups, such as 5G/6G security, cyber security, quantum security, distributed ledger security, and AI trustworthiness/security. Most of these contributions are individual expert contributions and have limited capacity and remit to provide systematic inputs. A good example is CSIRO's research and development program with the Department of Home Affairs on 5G/6G security, which allows us to strategically influence international standards based on research and exploration with Australian context and interest in mind. Similar research and development programs on other strategic standard areas can significantly increase our level beyond individual expert representation.

As outlined in Q1, Idea 7, more attention should be directed beyond "documentation" standards, especially in collaboration with Testing, Evaluation, Verification and Validation-focused standards organisations like the National Institute of Standards and Technology. We need to consider not only a standard roadmap but also a roadmap post-standard release focusing on sector/SME profiles, Testing, Evaluation, Verification and Validation tools, and reference implementations.

Q6: How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

As outlined in Q1, Idea 7, communities need to move beyond documentation-based standards and implement Testing, Evaluation, Verification and Validation-supported best practices for best practice conformance. Furthermore, as the government is often accountable for critical infrastructure, it is advantageous to use it as a model area for adopting innovative technologies that can address the most pressing challenges, including cross-jurisdictional/entity collaboration at scale and speed, integrated cyber-physical and supply chain-aware risk and vulnerability assessment, and software supply chain integrity.

Currently, there is a lot of advice for government departments and agencies on how to incorporate cyber security within their operations, but there is not a one-size-fits-all approach to support all organisations, regardless of sector, size, cyber security background knowledge and available resources. Many government departments and agencies are tasked with gaining ISO 27001 compliance. Similar to other guidance documents, the language used in ISO 27001 can be too technical or verbose, making it difficult for staff, especially those without dedicated technical support, to effectively navigate cyber security maturity.

Adapting to a rapidly changing and increasingly complex cyber security landscape requires ongoing learning and support, which can be challenging for most organisations.

With most of the current solutions, organisations lose engagement and interest as cyber is not considered to be a business problem, but rather an IT or vendor problem. In some instances, organisations manage to successfully build their cyber security posture, but lose momentum in maintaining this maturity (whether as a result of change in staff, limited time available, or external factors).

What is needed is easy-to-use cyber security strategy development tools that departments and agencies can use in a guided process to define their strategic cyber security foundation, and then human-centric focused tools to guide them in the implementation thereof and engaging them as the technology and threat landscapes evolve. CSIRO, in collaboration with the Cyber Security CRC, is currently working on solutions in this space.

Q7: What can government do to improve information sharing with industry on cyber threats?

As outlined in Q1, Idea 4, the combination of a trusted non-regulatory/security agency and innovative technologies (e.g., Privacy Enhancing Technologies) can remove barriers to data sharing

Q8: During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

As outlined in Idea 4, the combination of a trusted non-regulatory/security agency and innovative technologies can remove barriers to data sharing. Organisations fear reputational harm and or financial losses as a result of cyber incidents, but guidance in managing the aftermath of cyber incidents is sought after. With a trusted relationship in place, where sectors can grow stronger by learning from each other and sharing data in a non-discriminatory manner, Australia's cyber security will likely mature more consistently.

The basis for useful research and development is the availability of accurate data. An explicit obligation of confidentiality could be extended to include an anonymised dataset generated through the cyber incidents in the IMPACT database (CSIRO is the national coordinator for the US-led repository). Not only would this (i) enable global researchers to use real-life data to develop and test new cyber security defensive controls, leading to enhanced global cyber innovation, but (ii) Australian organisations will benefit directly from the research based on true data on actual Australian sectors, and (iii) a true representation of the cyber state of the nation will assist the ASD/ACSC to better guide the cyber security of the nation.

Q9: Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Yes, as addressed in Q8, a true representation of the cyber state of the nation will assist the ASD/ACSC to better guide the cyber security of the nation. In addition, the availability of accurate and real cyber security incident data from the Australian landscape will significantly improve the public understanding of the cyber security threat landscape and help to streamline the recovery process when these events occur.

Q10: What best practice models are available for automated threat-blocking at scale?

Advances in AI play a significant role in automated threat blocking. Australia could consider developing an automated cyber defence capability. However, AI alone cannot deal with the problem. AI-Human teaming might be the right approach going forward (refer Q1, Idea 12 point 1). The following captures some of the activities relevant to the use of AI to solve relevant issues:

- **Threat Intelligence using Machine Learning**: To stay ahead of emerging threats and attack trends, organisations need to leverage threat intelligence. Machine Learning models can help in threat intelligence by analysing large data volumes and learning from patterns of normal and abnormal behaviour to proactively identify potential threats in real-time and implement measures to block them before they can cause harm. For example, developing Machine Learning models for automated threat detection and prioritisation at scale; developing an automated Malware triaging tool that aims to identify coordinated attacks at scale and help organisations eliminate threats at an early stage.
- **Continuous Intelligent Monitoring:** It is a vital component of an organisation’s security strategy, as it enables them to establish a monitoring system that tracks all network activities and identifies any anomalies in real time. This way, potential threats and vulnerabilities can be detected before attackers can exploit them, improving the organisation’s security posture. One effective method to achieve this is through the deployment of the Automated Cyber Deception Traps. By deploying such traps, the organisation can gain insights into the attackers' motives and tactics, which can be used to strengthen the existing defences. This proactive approach to security can help organisations stay ahead of potential threats and maintain a secure operating environment.
- **Intelligent Incident Response**: Incident response plans are crucial for organisations to respond quickly and effectively to security incidents. This includes identifying the source of the attack, containing the attack, and restoring normal operations as quickly as possible. To ensure the resilience of organisations under attack, it's ideal to find ways to automate the incident response life cycle at scale. This could involve utilising advanced technologies and intelligent automation tools to proactively speed up incident detection, investigation, and response, thereby reducing the impact of any potential security incidents.

Q11: Does Australia require a tailored approach to uplifting cyber skills beyond the Government’s broader STEM agenda?

Yes, cyber security is not a one-size-fits-all, nor an apply-one-and-done approach. Cyber security is an ongoing learning process where end users, decision makers and policy makers need to constantly re-assess the threat and technology landscape and reconsider their applied security measures, with potentially changing resources in mind. To support these challenges, a strict human-centric security approach should be taken to ensure the uplift of cyber skills is embedded in Australian culture and not just an add-on that is addressed when a cyber incident occurs or when cyber security features in the news.

Specific examples of where human-centric security strongly supports cyber security culture:

- Interactive game to present to executive decision makers that covers a variety of sectors and attack scenarios, guiding executives to better connect the organisational cyber security needs with the business needs. Cyber Security CRC has initiated such a program that focuses on the digital uplift of senior Australian executives in cyber security strategy development and implementation.
- Developing practical cyber security implementation and integration guidelines by identifying the common strengths and weaknesses of SMEs and establishing simple and cost-effective solutions to bolster cyber security.
- Offering programs with research and development expertise to support SMEs that are developing novel cyber security solutions. CSIRO’s Innovate to Grow program is one such example project; upon completion of the program, participants will be able to access support through CSIRO, connect to research expertise nationally, and tap into significant research and development funding.
- Organising events that are guided by experts and targeted at SMEs to connect and enable them with practical advice and directions on how to engage with, manage and strategise cyber security within their organisations.
- Organising the ‘Summer School’ aimed to connect the Australian cyber security ecosystem and enrich the pipeline of rising talents.

Q12: What more can Government do to support Australia’s cyber security workforce through education, immigration, and accreditation?

Nil Response.

Q13: How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Nil Response.

Q14: What would an effective post-incident review and consequence management model with industry involve?

As outlined in Q1, Idea 4, the combination of a trusted non-regulatory/security agency and innovative technologies can remove barriers to data sharing and post-mortem data analysis.

Q15: How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers’ data safe?

As outlined in Idea 7, significant effort is required beyond “documentation” standards, especially in collaboration with Testing, Evaluation, Verification and Validation-focused standards organisations like the National Institute of Standards and Technology. Tailored support to SMEs in the form of sector/SME profiles, Testing, Evaluation, Verification and Validation tools, and reference implementations will assist this.

When it comes to cyber security uplift, the SME sector faces a myriad of challenges. Namely, investment of money, time, and resources often present significant barriers to SME cyber uplift. In a recent joint report by Cyber Security CRC, CyberCX and CSIRO, we developed a state-wide blueprint for SMEs to uplift their cyber security posture. The pilot learnings have been analysed and formulated into a comprehensive analysis report and blueprint that will help inform the Government of South Australia, as well as other governments and government departments, in the implementation of scalable and practical initiatives to support SME cyber security uplift.

The blueprint is designed in a way that it can be implemented cross-jurisdictionally and is intended as a resource to help policy makers prioritise areas of importance for SME cyber security uplift. This blueprint provides specific recommendations for policy makers:

- Implement a co-designed approach to cyber security campaigns aimed at SMEs to support general awareness and the need for SME cyber security maturity. These might be co-designed with industry to ensure widespread industry uptake.
- Establishing new funding models and incentivisation packages to support SME cyber security uplift.
- Establishing new programs and initiatives to embed a cyber secure attitude across the economy and foster cyber maturity.
- Together with the business community, the co-design and development of a SME community engagement system to provide support and access to relevant cyber security information which will facilitate SME cyber maturity uplift.
- Ongoing, timely and clear guidance concerning specific legislative and policy requirements for SMEs.

Q16: 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?

Nil Response

Q17: How should we approach future proofing for cyber security technologies out to 2030?

Cyber security technologies and adversaries are in a constant state of evolution. Given this dynamic environment, there are a number of approaches to future-proofing cyber security technologies and systems, including:

- Moving beyond secure-by-design and implementing continuous improvement of security measures.
- Designing systems with adaptivity, transition, and agility in mind. For example, current systems need to be adaptable enough to accommodate the quantum transition. "Crypto agility" refers to the ability of a system to switch its cryptographic functions with minimal disruption.
- Investing in the intersection of cyber security technologies and other emerging technologies such as AI, Quantum and 6G, as many future-proofing measures require a deep understanding of these emerging technologies.

- Adopting proactive mode towards cyber security such as continuous monitoring and authentication (with usability and user-experiences considered), organisations can effectively reduce potential attack surface and can safeguard their digital assets. For example, considering a zero-trust policy, organisations can improve their security posture by verifying and validating all user and device identities, controlling access to resources, and monitoring activities within the network. This approach helps making it more challenging for cybercriminals to breach the network and exfiltrate data.
- Incorporating human factors and AI to build human-centric cyber security solutions. The combination of human factors and AI is a novel science area that can assist in targeting cyber security capacity building, enhancing cyber security experience, and enabling digital inclusion to allow humans and machines to work together in an efficient way.
- Using AI/Machine Learning to develop augmented cyber defence against adaptive and non-deterministic cyber-attacks and ensure software systems security. Traditionally, as new solutions are built and released, security is often considered later, giving attackers a sufficient window of opportunity to identify vulnerabilities and prepare and launch their attacks successfully. To address this challenge, the use of secure AI/Machine Learning-based automation and orchestration ensures that new cyber technologies and software systems, including AI systems, are adequately protected at all times.
- Making large-scale and heterogeneous intelligent Internet of Things systems in critical applications secure, agile, and cyber resilient. Intelligent (AI-enabled) Internet of Things systems in various critical applications need security measures in addition to the application of basic security protection (authentication, access control, and secure communication). This science challenge ensures that even if Internet of Things systems are compromised, the systems can still maintain their functionality and the data remains secure in terms of its integrity and confidentiality.
- Developing a hardware-agnostic quantum software and security solution to reduce the barrier for wider usability of secure and responsible use quantum technologies and help Australia transition smoothly to a post-quantum world. By developing a quantum software platform underpinned by the development of innovative quantum software engineering methods, tools, and platforms, we can provide a hardware-agnostic high-level software engineering environment for quantum application developers, alleviating the need for rigorous training in complex quantum physics. The platform will be used to develop hybrid classical/quantum security protocols to help in a smooth transition to a post-quantum world ensuring security, safety, and privacy of quantum technologies.

Q18: Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Procuring solutions from SMEs can be risky for the procurer. However, SMEs and start-ups tend to have more innovative technologies than large multinational incumbents. As outlined in Q1, Idea 10, we can build the meta-security program to support Australian cyber security firms. This is needed for Australian cyber security ecosystem.

Q19: How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

As outlined in Q1, Idea 1, continuous analysis and experimentation are essential to keep up with the implications of emerging technologies. This requires deep sovereign science and technology capabilities in a semi-open environment that supports judicious international collaboration. The program of work required goes significantly beyond desktop research on technology trends and potentials. It requires testbeds, experimentation, and applied research and development from an integrated team of experts in both cyber security and emerging technologies. For example, Department of Home Affairs has established a 3-year research and development program on 5G/6G security with CSIRO, where cyber security implications of 5G/6G, including its intersection with AI and Quantum, are systematically investigated

Q20: How should government measure its impact in uplifting national cyber resilience?

The US National Cybersecurity Strategy 2023 recommends that protecting the systems that make society function must be the responsibility of their owners, i.e., it is the government’s role to protect its own systems. It is encouraging to see that this view reflected in the 2023-2030 Australian Cyber Security Strategy Discussion Paper as well with Securing Government Systems identified as a core policy area. The Cyber Security CRC and CSIRO are developing a whole-of-government cyber benchmarking exercise that will help understand the cyber security needs of different agencies, organisations, and local government areas to focus resources and improve cyber security maturity across these entities well as to manage government-wide cyber risk more effectively.

Q21: What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy

Nil Response

References

E. Kim et al. (2021). BASESPEC: Comparative analysis of baseband software and cellular specifications for L3 protocols. In Proceedings of the Network and Distributed System Security Symposium (NDSS'21).

S. Fahl et al. (2012). Why Eve and Mallory Love Android: An Analysis of Android SSL (in)Security. In Proceedings of the ACM Conference on Computer and Communications Security (CCS '12).

S. Rahaman et al. (2019). CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '19).

D. Sounthiraraj et al. (2014). SMVHUNTER: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps. In Proceedings of the Network and Distributed System Security Symposium (NDSS'14).

ASX (2017). ASX 100: Cyber Health Check Report. Available from: https://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf?ecid=O~C~~~~asx-100-cyber-health-check-report~ASX~~201704~~#:~:text=Exchange%2C%20the%20Australian%20Securities%20and%20Investments%20Commission%20and,know-how%20threats%20can%20only%20be%20effective%20through%20increased (Accessed 21 March 2023).

As Australia’s national science agency and innovation catalyst, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Unlocking a better future for everyone.

www.csiro.au