



Australia's National
Science Agency

Strengthening Australia's Cyber Security Regulations and Incentives discussion paper

CSIRO Submission 21/760

August 2021

Main Submission Author(s):

[REDACTED]

Enquiries should be addressed to:

Ms Liz Yuncken

CSIRO Government Relations

GPO Box 1700 Canberra 2601

T [REDACTED]

E [REDACTED]

Contents

Introduction	2
CSIRO response	3
Q1: What are the factors preventing the adoption of cyber security best practice in Australia?	3
Q3: What are the strengths and limitations of Australia’s current regulatory framework for cyber security?	4
Q6: What cyber security support, if any, should be provided to directors of small and medium companies?	6
Q8: Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?	7
Q9: What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?	8
Q23: Would a cyber security health check program improve Australia’s cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?	9

Introduction

CSIRO welcomes the opportunity to provide comment on the Strengthening Australia's Cyber Security Regulations and Incentives discussion paper. CSIRO supports the strengthening of cyber security regulations to promote a growing digital economy and recognises the importance of the ongoing reforms required to outpace the complex threat environment.

This submission addresses selected questions in the discussion paper that relate to CSIRO's scientific and technological expertise.

As Australia's national science agency, CSIRO is at the centre of solving Australia's greatest challenges through innovative science and technology. CSIRO contributes to building trust and confidence in Australia's digital economy and critical infrastructure through mission-driven cyber security research in areas such as the Internet of Things (IoT) security, human-centred security, Artificial Intelligence (AI) security, post-quantum cyber security, and information and privacy security. CSIRO is responsible for operating research infrastructure in a high security environment to deliver outcomes across multiple sectors within Australia and overseas, including government, research institutions, commercial and other non-government sectors.

CSIRO welcomes the opportunity to discuss these matters in more depth with the Department of Home Affairs.

CSIRO response

Q1: What are the factors preventing the adoption of cyber security best practice in Australia?

CSIRO has been working on technologies and tools¹ to help mitigate factors that prevent the adoption of cyber security best practice by government and industry in Australia. For example, CSIRO has developed Data Airlock, a tool to learn and share insights without sharing the underlying data. Other tools developed by CSIRO, such as R4 and Personal Information Factor (PIF) tool, can help evaluate the risk of sensitive information leakage, while CSIRO's Regulation Technology (RegTech) helps reduce compliance cost via automation.

Based on our research and interactions with industry, CSIRO suggests the following factors be considered.

1. Lack of technologies and tools to:

- **accurately estimate cyber risks across a supply chain.** Risks include the likelihood and consequence of security and privacy incidents to a business itself and the business' downstream supply chain, customers, and end-users.
- **accurately attribute the cost of a cyber incident to the right parties.** Attribution is not simply about attributing responsibility to attackers but is also about attributing some responsibility to various entities along the supply chain, especially upstream suppliers, who have not adequately adopted cyber security best practices.
- **share cyber threats and learnings without revealing commercial or security-sensitive information.** Adopting best practices requires not only understanding general best practices but also timely learning from peers about specific threats and how they were handled. However, sharing such information with peers may reveal sensitive information regarding security posture, system configuration, commercial details and reputation. Tools and technologies are required that can desensitise threat and incident handling information or enable anonymised sharing with low re-identification risks.

2. **A lack of research translation and adoption support – The lack of technology can be addressed by turning cyber security best practices and technologies into competitive product features to increase value and export intensity to the traditional industry.** Cybersecurity is not just about protection but increasingly about resilience and trust being the competitive advantage of products and organisations. This highlights the importance of efficient translation of cybersecurity practices and technologies into product features.

¹ <https://www.csiro.au/en/research/technology-space/cyber>

3. **Lack of understanding on interactions of cyber security and other critical or emerging technologies.** For example, AI and quantum technologies need cyber security best practices and new solutions to mitigate the risks of being compromised and misused by adversaries. On the other hand, AI and quantum technologies can also make adopting cyber security best practices easier. Businesses, especially SMEs, will struggle to appreciate the interactions of these technologies.
4. **High cost for SME adoption of cyber security best practices.** While large corporations usually have the human and capital resources to adopt cyber security best practices, SMEs lack the same means. Some technology-based approaches can lower the adoption cost in a scaled-up manner. For example, CSIRO is working on: 1) reusable reference implementations and exemplars (of standards and best practices) for specific sectors; and 2) technology-based automated compliance via machine-understandable and enforceable standards and regulations.
5. **Lack of understanding of the inter-dependency among critical infrastructures:** Though we have seen an increased focus on critical infrastructure security, there is a lack of research and understanding of the inter-dependencies among critical infrastructure from a cyber-security perspective. For example, critical infrastructure delivering services such as water supply, health care, and transport are dependent on the reliable supply of energy. With the expanding definition of critical infrastructures, the corporations, private or public, responsible for the critical infrastructures struggle to apply best practice cyber security. To do so they require a much deeper understanding of the inter-dependencies and cyber risk emanating from such dependencies.
6. **Lack of appropriately skilled, readily available and more affordable cyber security human resources.** Cyber security is a specialised field that requires subject matter experts to interpret and translate issues in a way that can be understood and acted upon by organisations. As the myriad of best practice frameworks grows, the cross organisational support required to implement these best practice frameworks also increases, with a relatively small pool of resources to currently draw on, especially in SME.

Q3: What are the strengths and limitations of Australia's current regulatory framework for cyber security?

The strength of the current regulatory framework is that regulation is focused on risk (e.g. privacy, corporations, national security), rather than the mitigation techniques of cyber security. The limitation of this approach is that mitigation techniques are left to those seeking to be compliant. Although it provides flexibility, choice and variety across the economy, poorly understood or implemented solutions might not mitigate risk to the extent required by law. Additionally, most (if not all) of the legislation has limited reach and does not cover all entities.

This limitation is not specific to Australia. The process of establishing or changing legislation and the regulatory framework is slow compared to the pace of technological advances and cyber security landscape changes. For example, advances in machine learning have created a new

modality for data, changing the way data confidentiality should be interpreted and implemented. Accordingly, legislation and regulatory frameworks must use abstract language, resulting in poor interpretation and implementation. This gap can be closed with constantly evolving standards, guidelines and tools, in which Australia would require greater progress.

Q4: How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

The cyber security guidelines for vendors along with standards and legislative changes, have improved clarity, coverage and enforcement of cyber security requirements in some sectors, such as the medical device domain. For example, the Therapeutic Goods Administration (TGA) recently published pre- and post- market cyber security guidelines for vendors and consumers, which improved clarity, coverage and enforcement. This guidance is for manufacturers and sponsors of medical devices that include software or electronic components. The TGA was the first to publish both pre- and post-market cyber security guidelines issued to all domestic and international vendors. The purpose of this guidance is to help manufacturers and sponsors understand how the TGA interprets regulations, and thus indicate how to comply. The goal being that this will improve patient safety through safer product development.

It is important that Australia's regulatory environment evolves with sector-specific regulations. For example, the TGA model can be expanded to financial services through security profiles of the Consumer Data Right (CDR), and could involve all domains that are preparing for a CDR uptake. Like the medical device domain, a well-linked chain of legislation, regulation, standards, guidelines and supportive tools targeting pre- and post-market for both vendors and consumers would improve clarity, coverage and enforcement in respective sectors.

Q5: What is the best approach to strengthening corporate governance of cyber security risk? Why?

CSIRO's view on each of the three options presented in the discussion paper to address the issue of strengthening corporate governance is outlined below. Regardless of whether a voluntary or mandatory framework is adopted, cyber security and cyber resilience should become a fundamental part of the risk management practices of boards and company directors. This could result in boards and directors coming under more scrutiny and pressure to ensure that they are using effective data management frameworks and processes.

1. Status quo (no action)

The status quo is not robust enough to protect the Australian economy, as demonstrated by several recent incidences. These include the recent Federal Court case between ASIC

and RI Advice where an Australian Financial Services Licence holder is alleged to have failed to implement cyber security and cyber resilience measures.

2. Voluntary cyber security governance standard for larger businesses

CSIRO suggests that a voluntary framework may provide a low-cost option for positive progress, which will be particularly important as businesses recover from the COVID-19 pandemic. There are concerns that a voluntary framework may not increase compliance and strengthen corporate governance measures. However, the possibility that the voluntary framework will become the standard that company directors will be held to in civil proceedings or ASIC prosecutions, will provide the necessary incentive to enforce the voluntary code.

A voluntary regime would be strengthened by including cyber security guidelines and reporting in the ASX'S Corporate Governance Rules and Practices. In turn, ASX listed companies would be required to report their compliance with cyber security practices into their "if not why not" reporting framework. This would provide greater transparency of cyber security practices to ASX shareholders and the market.

3. Mandatory standard for cyber security governance for larger businesses

A mandatory standard would impose considerable cost and compliance concerns for businesses. It is anticipated that the introduction of a voluntary code would become the default standard required for business and company directors' standard of care requirements and, thus, become mandatory-like in practice.

Q6: What cyber security support, if any, should be provided to directors of small and medium companies?

Small-to-medium enterprises (SMEs) are often targeted as they generally have lower cyber security maturity levels and are potential weak links in the Australian business cyber ecosystem, potentially acting as gateways to large-scale attacks.

CSIRO suggests that three main streams of cyber security support be provided to directors of SMEs to increase their overall cyber resilience and equip them with the tools to thrive in the digital domain:

- **Targeted training and awareness** - there needs to be an improved focus on leveraging business knowledge with an application in the cyber domain, to better enable directors to make executive decisions that will guide their organisations and maintain financial and economic viability. Executives are often time poor and may not have an interest or the necessary background in cyber security. By providing targeted training and awareness, these executives can be upskilled to better develop their cyber security awareness and technical understanding, contextualised to make informed strategic investment decisions to protect their business, by mitigating the potential risk of cyber security attacks. Examples of targeted training include CSIRO's work with the Australian Institute of

Company Directors (on 'Cyber for Directors' course material), with the Cyber Security Cooperative Research Centre (on executive cyber security gamification, cyber common operating picture, and SME cyber pilot project in South Australia), as well as initiatives such as CSIRO's Innovate to Grow – Cyber. All of these initiatives are aimed at upskilling executives with workable cyber knowledge.

- **Cyber security blueprints and implementation / compliance support** – it is imperative that SMEs are appropriately guided to increase cyber security resilience. The development of a cyber security blueprint could provide SMEs with guided and step-by-step support to enable the minimum baseline cyber security requirement. These organisations could be supported and motivated to comply with requirements to build their cyber defence. By supporting all organisations to level up to a safe minimum requirement, a supportive circle of trust could be developed. The Australian Signals Directorate's 'Essential 8' could be the focus of compliance support, however, compliance with international cyber security standards, such as the ISO/IEC 27000 series, would improve the international competitiveness of Australian SMEs. By assisting SMEs with automated compliance, simple measures that will significantly bolster cyber security can be established. This will help SMEs manage and maintain their cyber security posture at work and at home.
- **Opportunity to participate in broader government security services** - SMEs often need support as they do not have the resources or capacity to build their own cyber expertise. Furthermore, putting in place the connections and networks that these SMEs would need to directly work with research and academic partners will enable them to target their own specific problems, equip them to thrive within the cyber domain, and provide them with the opportunity to contribute actively to building the Australian cyber skills network. Providing SMEs with the opportunity and incentive to work with government and other research initiatives to target a specific problem, would further strengthen the Australian cyber security ecosystem.

Q8: Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

It is not clear that a cyber security code under the Privacy Act would effectively promote the uptake of cyber security standards in Australia. Acts such as the Privacy Act indicate some risks that ought to be controlled but are usually not prescriptive in how those risks should be controlled and mitigated. They also use "reasonableness" tests which may not be effective in a cyber security context. The Privacy Act may not be the best setting for a cyber security code. Having cyber security standards embedded in the Privacy Act may give the impression that cyber security is only an issue where privacy is of concern. Further, it is unlikely that any codifying will fully consider all possible circumstances in which the Act might apply. It seems that codifying minimum standards under this or any Act addressing specific risk and/or with a limited scope of application is not the best place, and rather a specific Act might be necessary.

More generally, as recognised in the discussion paper, codes are often slow to adapt and correct, yet cyber security responses need to be fast and agile. While the discussion paper lists the response times for patching systems, the response time for adjusting codes to new cyber threats could be longer. Furthermore, the existence of codes may lead to a “tick-a-box” mentality with a focus on compliance leading to an adoption of the lowest standard possible, rather than one that truly understands risk and seeks to best mitigate those risks. Lastly, CSIRO’s experience of conducting re-identification risk assessments in datasets has shown that risk can be peculiar to specific datasets. It is unlikely that codification can consider all possible risks that may arise. Therefore, in some situations codification could lead to inadequate mitigation of risk, while in other circumstances overreach and, at an extreme, prevent otherwise lawful and low risk use of data.

CSIRO suggests an evidence-based approach to understanding what risks materialise from cyber security breaches and in what settings. An environment of voluntary standards for use by those with no cyber security capabilities themselves could be a useful tool. Further, those standards could also be imposed (no longer voluntary) on select sectors of poor cyber security performance. CSIRO sees value in a system with an underlying point assessment like the Australasian New Car Assessment Program (ANCAP) ratings for new cars, allowing business and their customers to be better informed on the level of cyber security used. The challenges of keeping such a system up to date are clear.

Q9: What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

As outlined in the response to Question 8, several issues would limit the effectiveness of a cyber security code under the Privacy Act, some resulting from limitations in the Act itself and others from the potential regulatory code. Nonetheless, if a cyber security code were to be created under the Privacy Act, it should avoid giving specific standards or technical mechanisms due to the rapid pace of technology changes. Moreover, the relevance and effectiveness of cyber security risks and control mechanisms often depend on the data situation, the custodian entity, or the intrinsic characteristics of the data itself. These factors are difficult to capture in a comprehensive list of standards or techniques.

There is a wide range of evolving technical controls in cyber security. Thus, rather than focusing on specific technical controls, such a code could consider the aims or intents behind specific techniques. For example, a data custodian could be required to demonstrate an evidenced understanding of the privacy or confidentiality risks of data pertaining to individuals or businesses. This could be achieved by performing a systematic and repeatable quantification of re-identification risks on such data. However, the code would not mandate the use of a specific named technique or standard to do so. Rather the technical methods to perform such quantification could be left to industry-based best-practice or even standards (but not mandated), thus mitigating some of the shortcomings mentioned earlier.

Q10: What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

A multi-pronged approach is required to strengthen the cyber security of smart devices, ranging from developing awareness of device usage, to building a national blacklist, and providing free access to a 'sheep dip' (dedicated computers for testing smart devices for cybersecurity before they are allowed to be used).

As an overall consideration, all approaches should take into account the nature of smart devices (diversity, large scale) and the dynamic features of cyber security with the applications of smart devices. It is important to consider cyber security at design and manufacturing (supply chain security), the registration of smart devices into a network ensuring its integrity (device authentication), cyber security maintenance at operation time (updated patch and monitoring), and trusted data sharing, ensuring cyber security does not sacrifice business requirements and efficiency.

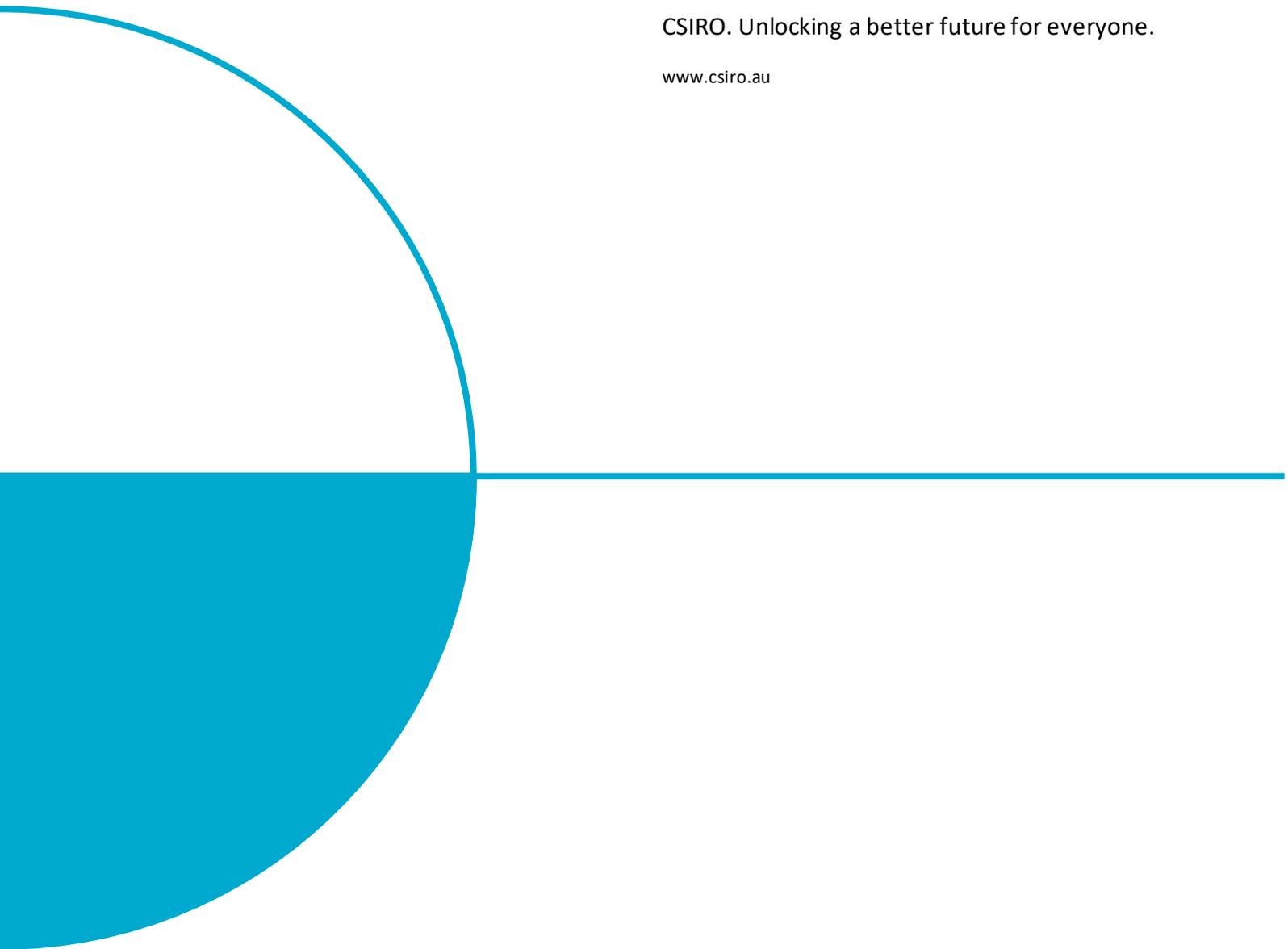
Two potential approaches to explore are:

1. Establish a regulatory framework that targets consumers and indirectly challenges vendors to supply secure devices, as is the case in the defence domain.
2. Regulate local or imported smart devices to ensure they follow certain standards for (machine) security assessability, such as, scan a QR code and receive a security report on the device. For example, a simple software bill of materials (SBOM) on a device can be used to check the device's security level based on the most recent exploits. This report may also advise the correct configuration for safe device use regardless of the vulnerabilities that it carries, such as, to disable a vulnerable feature or isolate.

Q23: Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

To improve supply chain management, one approach could be to introduce the concept of SBOM to software supply chains. The USA has introduced the Minimum Elements for SBOM recently via an executive order² to improve software supply chain security. SBOM helps to capture meta information about each component in a supply chain such as Supplier, Version, Dependency Relationship, Author, and Timestamp. SBOM also enables automation via automatic generation and machine-readability to allow for scaling across the software ecosystem.

² <https://www.ntia.doc.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials>



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