MERCURY
INFORMATION SECURITY SERVICES

PO Box 6008, North Sydney, NSW, 2060
www.mercuryiss.com.au
info@mercuryiss.com.au
ABN: 70 603 857 585

20th of August 2025

Subject: Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

To whom it may concern:

The following letter is a submission to the consultation on the Australian Cyber Security Strategy. In addition to three of the questions we'd responded to, I have also provided general commentary on other domains and areas raised within the strategy.

Q9. What existing or developing cyber security standards could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting/endorsing SMB tailored standards?

Small and medium-sized businesses, as well as not-for-profits, remain vulnerable to cyber threats because they cannot realistically sustain the same level of protection as large enterprises. Whilst there is often discussion of creating tailored cyber security standards for these groups, especially for Australia, the reality is that bespoke services are prohibitively expensive and difficult to scale and represent an increased cost.

Current frameworks, such as the Essential Eight, are too often misapplied as compliance tick-boxes rather than as meaningful security outcomes. These frameworks are becoming increasingly ambiguous, with en emphasis on governing as opposed to address core issues. Compliance-driven approaches create bureaucracy but deliver little resilience. What is needed is a focus on practical, accessible measures that reduce risk without creating administrative overhead.

When it comes to cyber standards for devices, Australia should avoid duplicating effort by creating its own. Mature frameworks already exist internationally, such as those published by NIST in the United States and the Cybersecurity Agency of Singapore. By adopting these international standards, Australia can benefit from existing expertise, reduce compliance burdens for international businesses operating here, and ensure interoperability with global markets. Government's role should be to endorse, adapt, and guide implementation of these standards locally, not to reinvent them.

As an alternative, Australia should prioritise generic but relevant standards that are easy to adopt. Guiding principles behind this should incorporate:

1. Harmonisation with global standards, including the NIST Cyber security framework.
2. Emphasis on addressing the threat as opposed to compliance.
3. Relevance, ease of interpretation, assessment and implementation.

MERCURY
INFORMATION SECURITY SERVICES

PO Box 6008, North Sydney, NSW, 2060
www.mercuryiss.com.au
info@mercuryiss.com.au
ABN: 70 603 857 585

Q11. Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

Cyber insurance will remain a challenge in the absence of reliable data to provide actuarial measurements, as well as the reality of motivated threat actors. The products that do exist are expensive, poorly understood, and underpinned by an immature insurance market that lacks consistent, data-driven frameworks for assessing cyber risk. As a result, premiums are high and uptake is low, and the post insurance efficacy is limited. Furthermore, as the domain is dominated by threat and not more readily measured acts of nature or environment, the capacity to accurately measure and quantify becomes a challenge for Insurers and consumers.

The government could play a convening role in bringing together regulators, insurers, and small businesses to develop standardised models and baseline products that are both affordable and trustworthy, and focus on specific, targetable domains that can be insured against such as business email compromise. Unfortunately, in the absence of specificity and targeted focus, a conceptual "cyber insurance" can be misinterpreted and see limited resources consumed with no practical benefit.

Q15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? How can technology be used to support individuals in managing and recovering from identity crime?

Support services for victims of identity crime need a fundamental rethink. Current systems are fragmented, slow, and place too much burden on victims to navigate complex recovery processes. A lesson from Australia's financial services sector is that credit card fraud is a liability of the credit card company and not the victim. This has been evolutionary in Australia's adoption of more secure technologies in payment services that have lowered the cost to companies, impacts to victims and created a better system of services.

This response does not wish to provide a solution, however additional exploration that leverages a protective framework through commercial outcomes will see an enhanced response to this domain.

Errata

The following other points of feedback from the provided documents have been raised.

<u>Protecting Critical Infrastructure</u>
Protecting critical infrastructure requires moving beyond compliance checklists to focus on engineering resilience. A valuable model exists in the U.S. Department of Energy's 2008 work on consequence-informed engineering and threat modelling. Australia should adopt similar approaches, prioritising the ability of essential systems to withstand, adapt, and recover from attacks. By embedding consequence-based thinking, we can ensure that investment in critical systems strengthens their resilience in practice rather than just in theory.

[redacted]
www.mercuryiss.com.au
[redacted]
ABN: 70 603 857 585

Policy Evaluation Models: limitations of the presented model

The policy evaluation model presented in documentation is focused on cyber-crime and do not sufficiently account for non-criminal actors, particularly nation states or insider threats, which historically have a greater impact than many external criminal operations. By concentrating too narrowly on criminal activity, we risk leaving blind spots in our defences. A more holistic threat model—one that incorporates nation states, insiders, and systemic vulnerabilities, should be considered in framing any strategy and policy evaluation.

This is also a wider issue within cyber security, wherein a narrow framing of the issue to "white kids in hoodies" or a particular nation state fails to encompass the complexity of the domain, instead preferencing easy paradigms that are inconsistent with reality. This model should be re-evaluated to enable a more resilient strategy.

Cyber Awareness Messaging

Government cyber awareness campaigns also need rethinking. The current approach is dominated by alarmist messaging that amplifies fear, uncertainty, and doubt, which we often joke internally as "Instagram modelling". This has the unintended effect of making cyber security feel overwhelming and inaccessible to the public, and often an act of gratification or narcissism by individuals who, in the absence of any training or background in the domain, are overnight cyber security geniuses.

One such criticism from late last year was the messaging that "*you should do a black box.*" This was presented at an industry event by an individual who was otherwise experienced in another domain, however in context the statement made no sense, contributes to confusion and encumbers all stakeholders. This issue is regularly seen in messaging, reporting and even standards specification, where intent is overlooked. There is a need to improve clarity and come back to understanding the substance of need over style.

Government messaging should be made deliberately unremarkable—boring, even. Cyber safety should be framed as routine and practical, much like seatbelt use or sunscreen application. By normalising simple, repeatable behaviours rather than sensationalising threats in a choreographed routine, Government can improve awareness and adoption without creating panic or disengagement, or rewarding counterproductive behaviours by self-appointed cyber security experts.

[redacted]
www.mercuryiss.com.au
[redacted]
ABN: 70 603 857 585

Cyber Literacy and Workforce Development

Literacy and workforce development, including professionalisation, is a domain which I personally am still considering, however I would like to take the time to share some of my own thoughts and observations.

Improving cyber literacy cannot be achieved through universities and formal accreditation alone. From personal experience, attending informal learning environments such as Ruxcon from 2003, BSides since 2015 and a multitude of community events which have allowed our professionals to genuinely build skills. These community-driven spaces encourage experimentation, knowledge-sharing, and practical problem-solving in ways that formal institutions rarely replicate. Government should support grassroots cyber communities, conferences, and hackathons to build a pipeline of skilled practitioners. Investing in these informal ecosystems will deliver far greater dividends than focusing solely on academic pathways.

I have spoken at length about the need for professionalisation, the avoidance of “unregulated genius” and the risks associated with individuals unsuited to the domain online throughout 2025. A greater concern I am observing in professionalisation is the imposition of professional development through an unnecessarily complex framework that does not meet the needs of the industry. As part of any industry consultation, a balanced approach to formal structures alongside informal education must be evaluated. This is still a topic that is evolving within our domain and one which I do not believe we have the answers for yet.

I look forward to the ongoing development of the strategy and will be available for any subsequent consultation.

Regards,

[redacted]