Submission to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*

April 2023

The Australian Government has announced its ambition for Australia to become the most cyber secure country by 2030, with the upcoming *2023-2030 Australian Cyber Security Strategy* ("the Strategy") to present a vision for how government, industry and the community can work together to achieve this goal.

This is a highly ambitious, but highly necessary undertaking; Australia's cyber security maturity has lost pace with much the developed world. Costly cyberattacks are currently pervasive across our society, from personally devasting scams targeting individuals to the recent high-profile data breaches which exposed the personal information of millions of Australians.

The *2023-2030 Australian Cyber Security Strategy Discussion Paper* ("the Discussion Paper") notes that even in the government's vision of Australia in 2030, where it is the world's most cyber secure nation, cyber-attacks will remain prevalent. It is, of course, an unrealistic ambition to seek to eliminate cyber-attacks entirely by 2030; as the Minister for Home Affairs has noted, we can't reduce our cyber risk as a nation to zero.

However, if Australia is to compete for the status of the world's most cyber secure country by 2030, we need to reduce and minimise the prevalence of high-impact cyber-attacks, and in particular those in which large Australian organisations entrusted with sensitive personal information are breached and lose control of that data. We also need to ensure that disruptive attacks on critical infrastructure providers, such as those seen in the United States in 2021 at Colonial Pipeline, continue to remain elusive in Australia. We view the recent *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act)*, and the *Security of Critical Infrastructure Act 2018 (SOCI Act)* which it amends, as highly positive steps to achieve this ongoing success.

To achieve a significant and permanent reduction in high-impact cyber-attacks impacting Australian enterprises, we will need to address a longstanding problem across the Australian economy and cybersecurity landscape: inconsistency in cybersecurity maturity. It is currently commonplace for organisations of similar size and function in the same sector to have vastly different levels of cybersecurity. To reach our shared vision, Australia will need to identify effective methods of assisting organisations, in particular those with contextually low maturity levels, to uplift their cybersecurity posture and capabilities such than a shared, common level of acceptable maturity can be reached across the board.

Further, if we are to become a world leader in our national cybersecurity posture, this uplift will also need to extend beyond critical infrastructure providers to all organisations which store or process large amounts of sensitive data – in effect, most Australian businesses, government agencies and not-for-profits. Recent critical infrastructure-focused initiatives such as the SOCI Act, while highly positive steps, are unlikely to cast a net wide enough for a national cybersecurity maturity uplift of sufficient magnitude to make us a true global leader in cyber posture. Maturity target levels for SOCI Act CIRMP cybersecurity frameworks are still set relatively low at this stage to become the world's most cyber secure country by the year 2030, requiring organisations to meet initial baseline requirements by August 2024. The following phases of maturity uplift are harder and will take longer than those currently in scope.

FTI Consulting is a global leading provider of independent cyber and risk management advisory services with a core offering focused on cyber readiness, incident response, and complex investigations & litigation. As external advisors, we have deep expertise and extensive experience in advising clients across all sectors of the Australian economy on

navigating complex cybersecurity issues and uplifting their cybersecurity maturity and resilience; we are fortunate enough to have insight into the key challenges that Australian organisations of all sizes and sectors face when undertaking those tasks, and the success factors required to achieve positive results.

On the basis of that experience and insight, we foresee **three key challenges** in uplifting organisational cyber security maturity across the Australian economy such that a common level of acceptable maturity can be reached, and by extension achieving a significant and permanent reduction in high-impact cyber-attacks.

1. Insufficient internal support from within the organisation

In all Australian organisations, cybersecurity must inevitably compete with other organisational priorities for resources and support. In Australian organisations with contextually low maturity, we must overcome resistance to cybersecurity investment by incentivising and in some cases mandating progress towards baseline levels of cybersecurity maturity. This could include, for example, recommended or required metrics for senior management.

Many organisations with contextually low cybersecurity maturity are aware of what their shortcomings are. The cybersecurity, IT and risk teams of these organisations often also know what needs to be done to uplift maturity. Often, however, it is not possible due to competing organisational priorities or insufficient support from management. It is still common, for example, for mid to large size Australian healthcare providers to not use multi-factor authentication at all, or only use it from administrators, because of fear of user disruption and pushback from within the organisation.

In these organisations, a meaningful uplift in cybersecurity maturity often only comes in the wake of a serious cyber incident, or not at all. If cybersecurity is to be uplifted in organisations with contextually low maturity, across the board, we must make cyber improvement a "must".

One way that this might be accomplished is for mandated metrics on senior management to consider cyber risk as part of each business undertaking.

By setting requirements for strong cybersecurity posture before a cybersecurity incident occurs, we may be able to shift organisations' mindsets from "reactive" to "preventative" and overcome internal resistance or apathy to cybersecurity by making it a "must".

2. Insufficient cybersecurity direction

Australian organisations with contextually low cybersecurity maturity often take a reactive approach to cybersecurity, without a proactive plan or strategy on how to uplift their maturity or capabilities over time. To increase the consistency of cybersecurity maturity across Australian organisations, we must assist, encourage, and possibly mandate that Australian organisations with contextually low maturity to recognise the gaps in their capabilities and adopt a defined strategy for increasing their maturity.

Cybersecurity maturity is closely linked to proactivity; organisations with low cybersecurity are often focused solely on the "now", responding to incidents and implementing short-term technical initiatives, whereas mature organisations, in addition to conducting necessary reactive practices, also usually have long term plans and initiatives to ensure that their cybersecurity function and capabilities are growing over time and will be fit for purpose in the future.

These "plans" can take many different forms, but two basic examples are a cybersecurity risk management plan and a cybersecurity strategy. Both documents involve comparing the current and desired future state of cybersecurity and developing practical plans for how to move from A to B to either reduce cybersecurity risk or strengthen cybersecurity capabilities.

To increase the consistency of cybersecurity maturity across Australian organisations, we must assist, encourage,

and possibly mandate that Australian organisations, at least those with contextually low maturity develop and implement such plans, such that their cybersecurity functions begin to move from reactive to proactive.

The SOCI Act is a good first step here; critical infrastructure providers are being required to develop and implement Critical Infrastructure Risk Management Plans (CIRMPs), which must be aligned with industry-recognised cybersecurity frameworks such as NIST and the Essential Eight. The Australian Government should consider casting a wider net and applying the same requirement to a greater proportion of Australian organisations.

To set organisations up for success, the Australian Government could assist organisations developing these plans by providing instructional content and templates for any plans that are mandated. Insufficient clarity on what exactly "CIRMP" documents should look like has been early feedback directed at the new SOCI requirements by some critical infrastructure providers.

3. The cybersecurity skills shortage

Australian organisations with contextually low maturity often face difficulty in attracting and retaining high quality cybersecurity professionals. To increase the consistency of cybersecurity maturity across Australian organisations, we must increase the overall supply of cybersecurity professionals and work towards defined baselines for skill development across core cybersecurity competences.

Much has been written about the shortage of skilled cybersecurity professionals in Australia; the Discussion Paper notes that there is no one silver bullet to address the problem.

In considering our approach, we should look to countries where a relative abundance of cybersecurity professionals has contributed to comparatively high national cybersecurity maturity. One such example is Israel, which is often touted as a world leader in both the innovation of its cybersecurity industry and the strength of its overall cybersecurity posture. Israel's comparatively plentiful supply of cybersecurity talent is largely due to its policy of conscription; young adults are required to complete mandatory military service, and many join the Israeli Defence Forces' signals intelligence and cyberwarfare units. After they complete their national service, these young Israelis enter the workforce with word-class, military-grade cybersecurity training.

We do not suggest that national service is an appropriate solution to Australia's cybersecurity skills shortage, but in addition to existing and future initiatives to increase the number of Australian STEM and cybersecurity graduates, the Australian Government should consider increasing the number of trained cybersecurity personnel across the Australian Defence Force (ADF) and Australian Public Service (APS), such that expertise developed inside government will "trickle down" into the wider cybersecurity industry as some personnel leave to the private sector over time. The Australian Signals Directorate's (ASD's) REDSPICE initiative, although having other primary objectives, is a positive step in this space.

In addition to having an overall shortage of cybersecurity professionals, development pathways across core cybersecurity competencies (for example, cybersecurity architecture, cybersecurity engineering, detection and response, governance, risk and compliance (GRC), cybersecurity leadership) are often unclear. The level of cybersecurity talent is varied across the Australian economy, in part, because it is not always clear what "good" looks like for a specific competency area, what knowledge and skills should be attained for each core competency over time, and what development actions should be taken to get to the next level of proficiency.

This is another strength of the Israeli model; cybersecurity professionals leave the military having experienced uniform, standardised training, with defined models for development and competence.

This can leave Australian cybersecurity professionals, and particularly those who are new to the industry or in small teams, without clarity on how to work towards proficiency in their specific area of responsibility. It can also

leave cybersecurity leaders without clarity on how to set development targets to grow the overall talent of their team over time, and unsure of how the skills and capabilities of their professionals compare to the rest of their sector and Australian cybersecurity industry.

Comprehensive certifications and development frameworks exist for most core cybersecurity competencies; (ISC)^2, the SABSA Institute, SANS Institute, Offensive Security and major cloud providers such as Microsoft and Amazon Web Services (AWS) are all examples of providers with industry-leading courses and certifications. In some cases, specific individual certifications from these organisations are now required to deliver certain professional services through Australian cybersecurity regulations such the Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework.

We believe that there is an opportunity for the Australian Government to standardise and benchmark skills development across the cybersecurity industry. For example, key bodies such as the Australian Cyber Security Centre (ACSC) should consider providing recommended, "standardised" development pathways for core cybersecurity competency areas, which cybersecurity practitioners and leaders could look to when planning and benchmarking the skills development of themselves and their teams respectively. These pathways could offer multiple certification alternatives at each stage so as to not favour specific certification providers and could be supplemented with the ACSC's own practitioner training material as required.

We of course note that certifications and third-party courses are not the only measures of competence in cybersecurity; they are meant to supplement the experience and expertise that professionals develop through performing their primary duties. They also become less relevant at more senior levels. However, we believe that there is value in recommending a national baseline for cybersecurity skills development and qualifications across core cybersecurity competencies.

Ultimately, of course, it is for individual Australian enterprises to determine what their desired level of cybersecurity maturity is and how they intend to get there, including their approach to these challenges. The Strategy should prioritise assisting and incentivising them to do so with a degree of ambition that reflects Australia's goal of becoming a global leader in national cyber security posture.

We hope that our submission to the Discussion Paper has provided some small benefit and insight to those charged with developing Australia's next cyber security strategy and look forward to the opportunity to contribute to our shared vision of Australia being the world's most cyber secure country by the year 2030.

WOUTER VEUGELEN
Senior Managing Director,
Head of Cybersecurity, Australia
+61 [redacted]