PARA FLARE

Dear Mr Penn, Air Marshall (rtd) Hupfeld, and Ms Falk,

RE: ParaFlare submission to the 2023-2030 Australian Cyber Security Strategy discussion paper

ParaFlare, one of Australia's largest providers of Managed Detection and Response services, welcomes the opportunity to provide feedback on the development of the 2023-2030 Australian Cyber Security Strategy.

We applaud the Australian Government's proactive approach to addressing some of the nation's most complex and urgent cyber security challenges.

The work ParaFlare does to protect Australian businesses from increasing cyber threats provides us with valuable insights into some of those urgent challenges. As active cyber defence specialists – which involves hunting, containing, and eliminating cyber threats within networks and systems – we see the agility, adaptability and persistence of cyber threat actors every day. And while some threats are sophisticated and elaborate, the majority are known and avoidable threats that exploit simple security flaws with devastating effect.

Despite countless warnings following successive large-scale security breaches in 2022, too many Australian businesses remain naïve about the threats that seek to do them harm.

In responding to any cyber breach, speed and agility is of the utmost importance. The ability to recover quickly from a cyber attack is critical.

In the words of Cyber Security Minister, Clare O'Neil, "As a nation we have a unique opportunity to move cyber security beyond a niche technical field to a strategic national security capability that underpins our future prosperity."

We could not agree more.

With that in mind, we offer our recommendations to address three questions within the discussion paper and thank you for the opportunity to contribute to the development of the nation's cyber security strategy.

[redacted]

Adam McCarthy
ParaFlare Chief Executive Officer and Co-Founder

[redacted]

Major General (rtd) Dr Marcus Thompson
ParaFlare Board Chair

1300 292 946
LEVEL 1/44A FOVEAUX ST,
SURRY HILLS NSW 2010
PARAFLARE.COM

bsi ISO/IEC 27001 Information Security Management CERTIFIED

ABN 82 612 095 253

PARA FLARE

What opportunities are available for Government to enhance Australia's domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Our recommendation: Encourage 'Buy Australian' cyber *now* and adopt a sense of urgency.

On 25 January 2021, The White House announced President Biden would sign an Executive Order strengthening buy American provisions, ensuring the future of America is made in America by all of America's workers.

With this order, President Biden is ensuring that when the federal government spends taxpayer dollars, they are spent on American-made goods by American workers and with American-made component parts.

This announcement was made three days into President Biden's term, with instruction to deliver change within 180 days. This important inclusion set a necessary deadline for change, demonstrating a sense of urgency, and this is certainly an option the Australian Government could consider.

The Labor Government under Prime Minister Anthony Albanese has taken bold steps toward a similar model in Australia with the announcement of 'A Future Made in Australia' to bolster the manufacturing sector, and the Future Made in Australia Office, aimed at improving sovereign procurement.

The intent is admirable, and the overall thinking sound. What is missing is the sense of urgency that was part of the Biden announcement, and the need to quickly move from policy ideas and big picture thinking to real change.

"The Future Made in Australia Office has been established in the Department of Finance to support delivery of the *Buy Australian Plan* and actively support local industry take advantage of government purchasing opportunities" (Department of Finance website).

This statement gives little confidence to industry that change will happen quickly in Australia, if at all.

One of the major obstacles is the fact that the Future Made in Australia Office has been established within the Department of Finance. This is not an accessible, industry-friendly model. We encourage the Strategy to

1300 292 946
LEVEL 1/44A FOVEAUX ST,
SURRY HILLS NSW 2010
PARAFLARE.COM

ABN 82 612 095 253

consider how A Future Made in Australia Office at arms-length from the Department of Finance, and with genuine powers to enforce 'Buy Australian,' could benefit the technology and cyber security industry.

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

Our recommendation: Enable 'Buy Australian' cyber by empowering government decision makers.

Competition is a key element of the Australian Government's procurement framework, and rightly so. As stated in the *Commonwealth Procurement Rules (1 July 2022) "*Effective competition requires non-discrimination and the use of competitive procurement processes." While there is no question about the importance of the competitive procurement process, and the need to demonstrate value for money to taxpayers, the system lacks agility in times of urgency.

Small to medium Australian enterprises are at a significant disadvantage when attempting to sell products and services to government. In the cyber industry, these are the businesses that are addressing cyber workforce challenges through education and training, developing innovative technology, and protecting businesses from cyber threats. The current process – open tender, limited tender, or procurements from standing offers – favours foreign prime contractors (primes) who have decades of experience and knowledge working with Federal Government agencies and are already on government panels. However, primes are not always able to deliver on all of government's needs. While smaller businesses can subcontract to government through primes, this can be to the detriment of their Intellectual Property.

Senior government decision makers need to be trusted and empowered through the Commonwealth Procurement Rules to go directly to Australian businesses who offer technology or cyber security products and services that address national security challenges when they need them.

There are capabilities that exist within industry now that could give our warfighters in the Australian Defence Force a significant advantage over potential adversaries. However, the current procurement system makes it almost impossible for these companies to quickly get their products and services into the hands of the people who need them.

PARA FLARE

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

Our recommendation: Deliver training at scale to solve the national cyber security shortage.

One of the more significant constraints on the achievement of the 2023-2030 Australian Cyber Security Strategy is the availability of trained workforce. Anecdotally, we consider the Australian cyber security workforce to be 30-40% below current requirements, and that is before additional obligations are imposed upon Australian businesses.

The Strategy should consider how training can be delivered at scale. As a proud employer of a large number of veterans and former Australian Defence Force members, ParaFlare has an intimate understanding of the effectiveness of military-style training systems, and their ability to generate skills, including technical skills, at scale. Key to this is a common curriculum, or standard, to which vocational training can be delivered. However, no current standard exists in Australia, leaving the many cyber security training and education providers, in both the domestic and international markets, to train disparate and varying standards.

Mature professions such as engineering, law, medicine, and accounting each have a national body that accredits courses against agreed minimum standards; certifies individual skills and monitors the currency of those skills; and maintains and enforces a code of ethics for their respective profession. We advocate a similar approach to the cyber security industry as a means to accelerate its progression into a recognised mature profession. Such a national body could develop the standards that are essential if we are to quickly accelerate the development of the professional cyber security workforce that Australia needs to achieve the 2023-2030 Australian Cyber Security Strategy.

1300 292 946
LEVEL 1/44A FOVEAUX ST,
SURRY HILLS NSW 2010
PARAFLARE.COM

ABN 82 612 095 253