IONIZE

Suite 2.01
40 Cameron Avenue,
Belconnen ACT 2617

(02) 6162 1783
www.ionize.com.au
info@ionize.com.au

Re: Response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper

Dear Expert Advisory Board

We thank you for the opportunity to provide a response to the Australian Cyber Security Strategy Discussion Paper. Ionize believe that this is a time the opportunity for government and the private sector to work together to detect, prevent, and respond appropriately to cyber attacks from a range of highly sophisticated operators. Ionize is in a unique position to provide a response to the Discussion Paper, given that we have been operating in the Australian market for 15 years, supporting both tier one corporate clients, and a number of federal government departments. Ionize operates a 24x7 Security Operations Centre (SOC) in Canberra at the PROTECTED level, and is a Level 2 Member of the Defence Industry Security Program (DISP). As one of the very few fully sovereign cyber firms operating in the Australian market, we are pleased to provide our three recommended strategies, after reviewing those proposed in the Discussion Paper.

Strategy 1: Setting Clear Expectations

We believe that the government needs to set clear expectations to all companies that hold personal data of Australians. The recent spate of data breaches clearly indicates a lack of understanding or capacity to protect the private data of citizens from cyber-attacks. One way to achieve this is to consider *framework standardisation* alongside industry-defined and scientifically-validated *benchmarks*. This evidence base could then be used by a central cyber authority to assess and appraise the capacity of individual companies to protect the personal data that they hold. We believe that such a central authority must have additional powers to those currently held by the OAIC, and other coordinating entities such as the ACSC. Note that we are not proposing that new standards be created; there are already a proliferation of cyber security standards available in the marketplace. Our concern is that most Australian companies do not seem to understand that these standards apply to them, nor that the government expects compliance with any standard at all.

Strategy 2: Public-Private Collaboration

Ionize do not believe that the current level of information sharing between the public and private sector is sufficient to reduce the level of cyber risk that we face as a nation. We make this assertion based on our long-standing support of a number of federal government departments and large corporate clients. Implementing affective cyber security controls relies on having *adequate, reliable, and valid cyber risk data*. The only mechanism for this to be collected nationally is for the government to coordinate the activity. However, there is still an impression in the private sector that the government is not particularly forthcoming with the

level of cyber intelligence that is needed. The current level of cyber attacks and data breaches indicates to us that a further enhancement of intelligence sharing would be extraordinarily beneficial to our nation.

Strategy 3: Managing the Residual Cyber Risk

We believe that most companies do not invest anywhere near enough in cyber protections. This means that there is a very significant level of residual cyber risk in the Australian economy today. The only way to remedy this problem is for the government to regulate the active monitoring of all significant personal and private data holdings in Australia. For the avoidance of doubt, this means active monitoring through a Security Operations Centre (SOC) or equivalent. We say that all organisations in Australia must identify their most significant data holdings, and be required to have access to these holdings and the systems and networks that host them protected by a SOC. The data holdings most at risk are personal and private data, as well as any of the *critical technology* sectors or *critical infrastructure* that has been addressed by more recent legislation. We believe that the government must be more prescriptive about the actual level of protection and the standards that must be complied with in order to protect this data.

In summary, we hope that these three strategies will be considered by the government alongside the other elements of the Strategy Discussion Paper.

Yours Sincerely

Andrew Muller

Managing Director