Sello Tech Pty Ltd
Securing your Digital World

14 April 2023

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

To whom it may concern,

Firstly, we at Sello Tech would like to express our strong support of the 2023-2030 Australian Cyber Security Strategy, and in particular our support of the great work done by the Expert Advisory Board in this Discussion Paper. We greatly appreciate the opportunity to provide this feedback, and specifically we appreciate that our voices are being heard. The vision for 2030 is well conceptualised and, we believe, very achievable. It is our hope that Sello Tech can support the Australian Government in becoming the most cyber secure country well in advance of the 2030 goalpost.

The recent bouts of cybercrime have shocked the world. The best word to describe it is *invasive*. At Sello Tech, we are finished with feeling *invaded* and are strong supporters of strengthened regulations to ensure these attacks stop happening. We recognise that finding the balance between flexibility and robust compliance is a challenging one. We hope to support the Government in enabling mobility and reactivity while still being a global leader in cyber resilience.

We provide the following feedback as a response to a selection of the questions provided in the Discussion Paper. Our aim was to be concise with our thoughts and suggestions, and we are more than happy to elaborate further on any of our comments if needed.

Warmest regards,

Molly Hall, Sello Tech Chief Operations Officer
[redacted]

Buti Sello, Sello Tech Chief Executive Officer
[redacted]

1 Executive Summary

The principal theme of this proposal is that Australia must change its mindset on what cyber security means. It is no longer solely the responsibility of those at the top of the food chain to worry about their security; it is a topic that impacts all industries and scale of organisation right down to the individual. It is our hope at Sello Tech that we can assist the government in promoting this mindset and encouraging good cyber hygiene amongst our clients and society as a whole. To that end, we have provided more detailed thoughts and suggestions across the following areas: improving regulatory compliance, growing the STEM pipeline, and enabling cyber security across all organisational scales. This summary provides a high-level overview of our vision, with detailed responses to specific Discussion questions in Section 3.

In alignment with the first Core Policy area of the Discussion Paper, we believe that enhancing regulatory frameworks is a critical component to improving the cyber resilience of Australian businesses and organisations. Regulations can be confusing to understand and implement correctly, and compliance can be burdensome to verify. We believe that a combination of a delegation scheme and enhanced knowledge sharing could enable better understanding and compliance to the existing and future regulations. The delegation model can expand the oversight capabilities of the regulators, while still allowing for sufficiently thorough work to be completed. Implementing a one-stop-shop set of knowledge sharing resources, such as a Playbook, can assist organisations in understanding the requirements they must meet and different ways in which they can meet them.

Our second priority is in expanding the cyber security workforce and integrating with academic institutions to develop more effective tools. By engaging with existing institutions, such as Science in Australia Gender Equity (SAGE), it is possible to promote cyber security as a national priority in a consistent and forceful message. Gender equity in STEM fields is a key area of concern, and Sello Tech strongly supports any efforts to balance the workforce within cyber security. Further, enabling

collaboration platforms such as the Trailblazers Universities Program can help bring academic institutions and industry together to develop the next generation of cyber security tools.

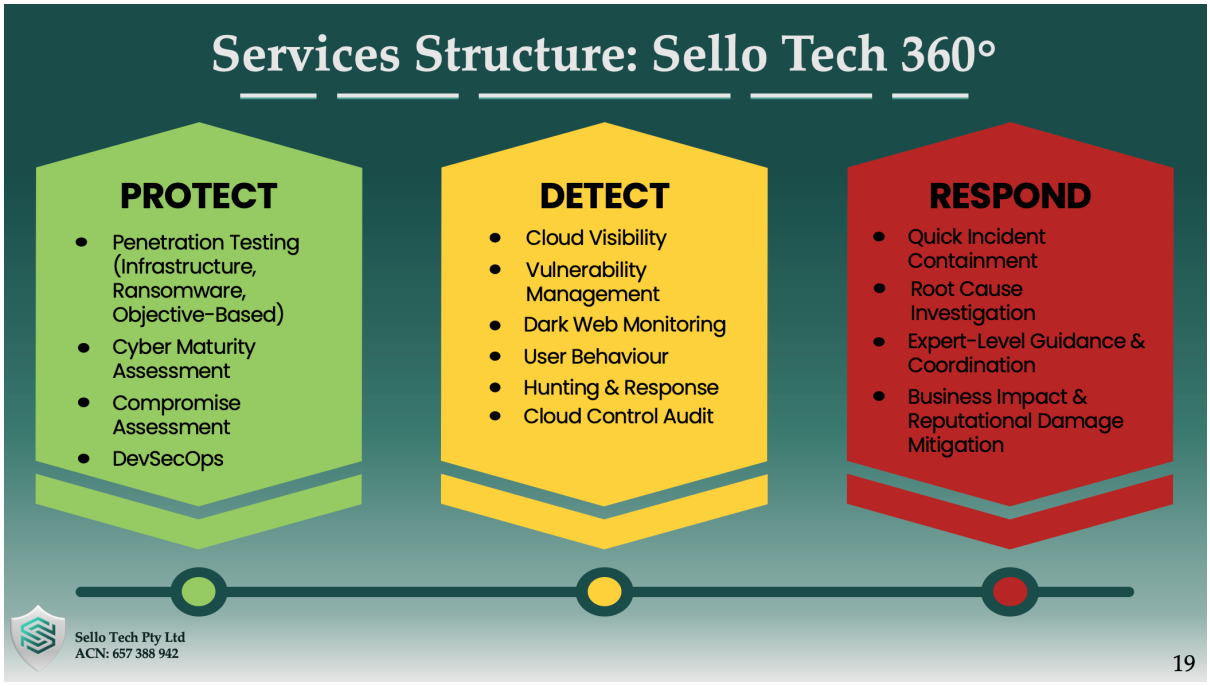
Finally, we believe that cyber security is a necessity for all scales of business and organisation and strongly support its accessibility to everyone regardless of size, industry, or location. However, the needs and capabilities of small business are different from those of a larger corporation. By providing guidance and financial support to small businesses, the government can help promote the mindset that cyber security is applicable and accessible to all of us.

In summary, Sello Tech is extremely supportive of the Australian Government's efforts to enhance our cyber security approach and become the global leaders of cyber security by 2030. We provide this proposal and feedback with the hopes that Sello Tech can be a part of this vision. Further details on our feedback to specific questions can be found in Section 3, and we are more than happy to elaborate further on any thoughts or suggestions.

2 Sello Tech Background

Sello Tech was founded in 2013 by Buti Sello (CEO) and Jessica Sello (CFO) as the arm of Sello Groups which is responsible for cyber technology. In early 2022 we shifted to focus specifically on cyber security and brought on a new team of directors to make this vision come to life. Our current Board of Directors has extensive experience across a range of industries and roles from cyber security R&D, academia and higher education, aerospace/defense, heath, government administration, mining, supply chain, and telecommunication.

Our corporate strategy is to provide a highly personal approach to the cyber security needs of any scale of business. We believe that one size does *not* fit all, and the best approach is usually a tailored one. We feel strongly about promoting the Essential Eight, however we also recognise that there are circumstances in which a client may need to go *beyond the Eight*. We see our role as assisting our customers in identifying what they need to do, and then helping them to execute it. To this end, we have developed the Sello Tech 360° approach. Our three pillars of services cover the **protection** against threats, **detection** of threats and attacks, and then **response** in case of attack.



3 Select Responses to Discussion Paper Questions

Question 1, regarding new ideas for the Strategy:

> We at Sello Tech believe that cyber security is a mindset, and one that we must all develop. Unfortunately, security is not just the responsibility of the "techos" who understand it, it is something that impacts all of us. To this point, we strongly feel that an overhaul is needed of how everyone approaches cyber security: government, industry, academia, and individuals. While many regulations and guidelines are provided for the first three, individual cyber security awareness is lacking. The average Australian has a number of household devices which can easily become vulnerable: from their cell phone, smart TV, Amazon Dot, or even their child's Barbie doll. While we by no means want the public to live in fear, there is a huge opening for building awareness and developing good cyber hygiene. We strongly encourage an information campaign or training resources to help educate the populace on reasonable measures that can and should be taken. When you enforce this mindset at the bottom level (the individual), the best practices and approaches will be carried upwards.

Question 2c, regarding obligation of company directors:

> Yes, we strongly believe that company directors must affirm that they are aware of their responsibilities surrounding cyber security. It is strongly suggested cyber security awareness and compliance be added to the ASIC list of Company officeholder duties, and strongly recommended that directors must sign or submit affirmative consent that they are undertaking this responsibility.

Question 2e, regarding the burden of regulatory compliance and enforcement:

It is anticipated that the responsibilities of the regulatory bodies will grow immensely in the coming months and years as both the scope of the regulations and the applicable audience is expanding. While expanding the regulatory workforce to provide oversight and verify compliance will be needed, it may be beneficial to implement a delegation scheme. For example, the delegation model implemented by the United States Federal Aviation Administration has had much success in addressing the regulatory burden of an industry that is growing more complex each year.

Some best practices for implementing a delegation process may include:

- Implementation of an overseeing body who would be responsible for the delegates.
- Standardised training of the delegates, including sign-off of satisfactory training by the overseeing body.
- Different levels of authorisation to perform certain tasks. For example, one delegate may be authorised to complete an Essential Eight compliance audit, yet another delegate would have the authority to review a specific aspect of the Eight.
- While the delegates may be responsible for much of the regulatory compliance checks, the overseeing body would likely have final sign-off authority. This helps ensure the integrity of the oversight process while applying minimal burden to the regulatory body itself.
- Implementation of Playbooks (see response to Questions 6 and 7) which would enable the regulations to be consistently enforced and executed across multiple levels of the delegation hierarchy. Internal-facing Playbooks would be critical to ensure delegates understand how to complete their jobs as an effective agent of the regulatory body.

Questions 6 and 7, regarding knowledge sharing and communication of best practices:

The existing methods of knowledge and information sharing are certainly effective, including reports, webinars, and infographics. However, we would like to propose a new format which Sello Tech is currently developing for both internal and external use: Playbooks. The principle of a playbook is that it is a single source of information on a contained topic that is easily digestible by the reader. Some key features include:

- It is a **one-stop-shop of guidelines and best practices** with the intention of *supplementing* existing requirements and regulations. A key delineation is that the regulations are the governing authority at all times and take precedence over Playbook content. The Playbook pairs with the laws and regulations to help communicate the meaning, intent, and provide examples of compliance.
- The Playbooks include **multiple information formats** such as text descriptions, video, checklists, embedded documents, examples, and case studies. The type of media used can be dependent on the content and the audience.
- The Playbooks can be outward facing (resources for the business or entity who must comply with the new regulations) or inward facing (resources for the regulatory bodies themselves). This allows for the **regulations to be applied and enforced consistently** no matter the organisation, scope, location, or responsible authority.

  or inward facing. It should be noted that inward facing Playbooks are a strong component of the delegation scheme proposed above.

Questions 11 and 12, regarding workforce growth and education:

Sello Tech thoroughly supports the expansion of the STEM pipeline and STEM workforce, as it pertains to cyber security and all other STEM related fields. In addition to being advocates for STEM, we are also advocates for enabling a gender-balanced STEM workforce. As such, we would encourage engagement with Science in Australia Gender Equity (SAGE) to raise the profile of cyber security as a key field and priority area.

On the topic of attracting foreign talent, Sello Tech is pleased to see that cyber security is a desired field of expertise as listed by the Department of Home Affairs within immigration resources. However, for non-citizens hoping to study cyber security or ICT-related fields within Australia the visa process can be challenging. In particular, the lack of an extension process for programs which extend outside of the original timeframe can necessitate students applying for a new visa, which is time and resource consuming. It is common for a program to change form as it progresses, and it is increasingly common for students to work during the duration of their program. Any improvement to the flexibility of visa arrangements may help raise Australia's profile as a desirable country to study in.

Question 15a, regarding the needs of small business:

Even though small business may not carry as much data as medium to large enterprises, they may still carry sensitive data about their clients/customers, their supply chains, interactions with government departments, etc. Data which if compromised, the repercussions thereof may be non-negligible. It is in this line of thinking that a scheme perhaps resembling the Small-scale Renewable Energy Scheme (SRES) implemented by the Department of Climate Change, Energy, the Environment and Water, could be introduced to assist small business with the cost of securing themselves.

This could facilitate a multi-pronged approach by then legislating the obligations of company directors to specifically address cyber security risks and consequences. This is not necessarily a carrot and stick approach, but rather an approach that would reduce regulatory burden to small business whilst bringing about compliance. The same scheme might be extended to Medium Enterprise should it not prove to be cost-prohibitive.

Question 19, regarding promotion of new technologies:

The Trailblazer Universities Program shows much promise for major growth across many key industries. Sello Tech would be very supportive of a similar initiative for collaborative research within the realm of cyber security and security related fields.