CREST (International)
Seven Stars House
1 Wheler Road, Coventry
West Midlands UK

Response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper – CREST International

CREST (International) is pleased to respond to the discussion paper seeking views on how the Australian Government can achieve its vision under the 2023-2030 Australian Cyber Security Strategy.

CREST is an international not-for-profit membership and examination body representing the global cyber security industry. Our goal is to help secure a digital world for all by quality assuring our members and delivering professional certifications to the cyber security industry. We accredit over 300 member companies (with over 40 members operating in Australia) across dozens of countries and certify thousands of professionals worldwide. In addition, we work with governments, regulators, academia, training partners, professional bodies and other stakeholders around the world.

Our members undergo a rigorous quality assurance process and employ competent professionals. As a result, organisations buying their cyber security services from our members do so with confidence.

In response to questions presented in the discussion paper we offer the following responses:

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

We believe secure only makes a statement about a nation, an organisation, or a system as a snapshot of a point in time. The Strategy needs to focus more on resilience. Resilience encompasses becoming more secure but also recognises that it is important to be in a better position to deal with and withstand attacks when they happen. Because they will happen.

To achieve a more resilient cyber eco-system, it is essential to build greater awareness of different tools, techniques and services that a public or private sector organisation needs to protect itself and others.

In the cyber security market, there is misalignment of expectations and outcomes, when procuring services from a market with very little governance, oversight or regulation. For example, while buyers recognise that cyber security involves technical assurance, they may believe that vulnerability assessment, penetration testing and red teaming all mean the same thing. This results in some buyers procuring one type of service and receiving something different that doesn't meet their needs. This problem exists across the fields of penetration testing, incident response, threat Intelligence and (SOC) Security Operations Centres.

This issue is compounded by the difficulty in selecting the best service provider. Public and private organisations need assurance that they can trust them to do what is needed, to do it properly and ethically.

Standards that define the service itself and also provide assurance in the supplier would help all organisations in Australia to easily identify who is the right supplier for their specific (and their industry's) requirements and one that will improve their resilience. This is paramount to a more resilient nation.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism or reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

Cyber criminals are increasingly targeting Australia's critical infrastructure. Many factors have led to this but the growing digitisation of industry and people's reliance on mobile technologies is significant. When it comes to legislation, it is important to look at existing cybercrime laws and ensure there are defined laws on all cybercrimes.

As technology evolves and attacks increase it is essential that the regulatory framework does too. Regulation is necessary, and experience tells us that while something is optional, compliance will be low. Having a regulatory framework for an industry is also complicated by the increasingly complex and global digital supply chains most industries operate in. This is where taking advantage of global standards is important. It is also important to consider improving supply chain resilience when considering any new regulation, but also doing that without making it prohibitively difficult to conduct business.

But Government can only do this with the help and the support of industry collaboration to get it right. It also must consider global standards. Professional bodies like CREST also have an important part to play, working with its industry members to establish frameworks that do exactly what they need to do. And also, to monitor and report on compliance.

At CREST, we have worked with governments globally to establish and administer frameworks for several critical industries. There is no one size fits all solution. The level of regulation depends on the industry, whether it is part of critical national infrastructure and also the consequences of a cyber attack. And while regulatory frameworks will have many parts that are consistent across industries, it is important to ensure they are right for the specific market needs and the threats that the sector faces.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

It is trite to discuss the globalised nature of the internet and related digital technologies. As a result, it is in Australia's interest to support the immediate Indo-Pacific region to uplift those nations which are still developing whilst sharing threat intelligence, tools and techniques with those nations with a higher level of maturity.

CREST is comprised of regional and international Councils, discipline-specific Focus Groups made up of Members (service providers), each of which works with governments and regulators across the globe. We can draw on regional knowledge and expertise to ensure a local approach to solving the cyber threats facing the immediate region. CREST would be pleased to partner with the Australian Government to engage with and build the capacity and capability of our nearest neighbours.

CREST's standards, accreditation and certifications are recognised globally and by many entities the Commonwealth would benefit from partnerships with.

7. What can government do to improve information sharing with industry on cyber threats?

Private and public partnership is essential. A genuine collaboration between the government and industry is the only way to ensure a strong defence against cyber attacks. Along with its traditional sources of threat intelligence, government need to establish a cross government / industry sharing partnership. This will provide a platform for the government and the private sector to share threat intelligence quickly and confidentially.

Good threat intelligence is of course essential. And this needs to be a collaborative and bi-directional effort between government and industry. The government needs to provide a baseline intelligence for red teaming engagements such as threat intelligence providers adding more specific industry intelligence. But both government and industry must have assurance in the threat intelligence providers and the skills of analysts.

CREST offers a recognised career pathway – based on a suite of certifications – for those individuals within the threat intelligence arena. Additionally, CREST has several member companies accredited to deliver threat intelligence, the services of which can be located via the CREST 'buyers portal' on the CREST website. Additionally, CREST has a Focus Group dedicated to threat intelligence which has created guidance to help businesses find the right Cyber Threat Intelligence partner to meet their security challenges better. The report can be found at http://www.crest-approved.org/wp-content/uploads/2022/04/CTI-in-Business-Context_2021.pdf.

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

Absolutely. Cyber has a particular set of issues regarding cyber skills. For example, Gartner recently said by 2025, in Australia nearly half of cybersecurity leaders will change jobs, 25% of which will be for different roles due to multiple work-related stressors. There is also evidence that people at all levels in cyber leave cyber roles for the same reason. And when it comes to diverse groups, retention is also a big issue, often due to a lack of inclusiveness.

All the excellent work governments do to get more people into cyber from school-level or transition into cyber from other roles means nothing if they are entering an environment where they do not feel supported and included. More work needs to be done on this, alongside initiatives to encourage more people in.

When it comes to a tailored approach, particularly for diversity and inclusion, it is important to look at where the country is now in terms of both people's attitudes to cyber roles and the success of any work that has been done. Of course, changing mindsets and behaviour is the most difficult thing but perhaps when encouraging more diverse people into the industry is recognises as a potential way to alleviate the skills crisis and makes for better security teams, it is perhaps the most important element to look at.

CREST has recently launched a best-practise guide on fostering greater equity, inclusion and diversity as part of a national cyber security strategy. The report can be found at https://www.crest-approved.org/wp-content/uploads/2023/02/GATES-Inclusion-and-Diversity-Guide_FINAL.pdf

Additionally, CREST has formalised programs for supporting students into cyber security careers.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

CREST has created a range of research reports and best-practice guidance which inform governments and industry on the benefits of a close working relationship to solve cyber security challenges. CREST has a range of membership options, certification pathways and professional development opportunities, all designed to raise the standards in the global cyber security industry.

CREST has had a Chapter in Australia since 2012 and stands ready to work closely with all tiers of government to create more qualified and competent cyber security professionals.

We recommend the Australian government mandate all Commonwealth departments to use CREST accredited individuals working for CREST approved companies to solve their cyber security challenges. Additionally, we recommend the Australian government advocate industry to choose CREST member companies when procuring cyber security services. This is particularly important for those organisations which operate within dedicated critical infrastructure industries.

CREST's online buyer search facility provides easy access to information on which companies to choose, even where buyers need help determining what services they need.

CREST looks forward to partnering with the Australian Government to achieve the results set out in the next Cyber Security Strategy. More information on CREST can be found at: https://www.crest-approved.org.

Please direct all enquires to the Chair of the CREST Australasian Council, Nigel Phair via: [redacted]

Yours sincerely

[redacted]

Rowland Johnson
President
CREST (International)
April 2023