26 August 2025

Department of Home Affairs
PO Box 25
Belconnen ACT 2616
Australia
Via upload at: homeaffairs.gov.au

Dear Sirs

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy – CREST (International)

CREST (International) is pleased to contribute to the Australian Government's development of Horizon 2 of the 2023-2023 Australian Cyber Security Strategy. We further welcome the government's desire to harness the efficiencies and capabilities that are offered through technological advances while continuing to protect Australia's data and technology assets from malicious actors.

As Australia faces an evolving cyber security landscape, both in terms of the threats facing the community and economy, CREST (International) is ready to work with government to leverage its global experience to deliver sector-aligned frameworks targeting financial services, telecommunications and critical national infrastructure.

With respect to the questions asked in the discussion paper we offer the following:

Shield 1: Strong businesses and citizens

In the cyber security market, there is all too often misalignment of expectations and outcomes when procuring services from a market that has 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, intelligence-led testing, incident response, threat intelligence and Security Operations Centres.

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

Recommendation: Government signal to the market the need to purchase technical cyber security services from a CREST (International) member company.

Registered Office: CREST (International), [redacted]
Company Number 09805375

Shield 3: World-class threat sharing and blocking

Cyber Threat Intelligence (CTI) is increasingly becoming established and continues to develop at a fast pace. Using an intelligence-led approach has long been accepted as best practice in the realm of conventional security and this needs to be parlayed into information security. Without it, organisations will invariably defend against too little, because they do not understand the threats they face.

This approach informs the uptake – and the government leadership – of a range of global intelligence-led cyber security testing frameworks such as:

- CBEST – for financial institutions in the UK
- STAR-FS – for smaller financial institutions in the UK
- GBEST – for UK government departments
- STAR* – a generic framework applicable in any sector
- TIBER-EU – for financial institutions in Europe
- iCAST – for financial institutions in Hong Kong
- AASE – for financial institutions in Singapore
- FEER – for financial institutions in Saudi Arabia
- CORIE – for financial institutions in Australia

** STAR: Simulated Targeted Attack and Response*

CTI products and services are likely to see deeper integration with other cyber security and broader business functions. Government should have an increasing influence on domestic consumption of CTI by declassifying and publishing intelligence, whilst promoting a broad array of commoditised tools and services - particularly to organisations that would otherwise lack the resources to adopt an intelligence-led approach. CREST would be pleased to work with government to create a framework which allows for automated threat indicator sharing across all sectors.

Recommendation: Government engage with the CREST Threat Intelligence Focus Group to create sector-specific frameworks to ensure intelligence-led security testing is the gold standard for improving an organisation's cyber resilience.

Shield 5: Sovereign Capabilities

Governments have a pivotal role to play in shaping the development, growth and professionalisation of the global cyber workforce. By establishing a coherent national framework, government can support workforce professionalisation, recognise transferable skills, and foster pathways into cyber careers. If designed with global alignment in mind, a national framework has the potential to be recognised worldwide. This is an area of active engagement for us at CREST, where we are contributing to efforts that promote professional standards and global interoperability.

There is an opportunity to diversify and strengthen the cyber workforce through the recognition of transferrable skills and global interoperability. Valuable, transferable skills include analytical thinking, risk management and systems-level problem solving, and can be adapted and built upon for cyber related roles. Supporting these transitions not only helps address immediate capability gaps, but also contributes to long-term workforce resilience.

To drive innovation and align research priorities with strategic national interests, a trilateral collaboration model between industry, academia, and government is essential. Think-tanks and professional bodies can play a role in convening a coalition of expert individuals and panels, facilitating knowledge exchange, and translating research into policy. At CREST, we are actively engaged in global research efforts with regional partners to better understand and map these transferable capabilities, ensuring that workforce strategies are informed by robust, evidence-based insights. We would welcome an opportunity to further this work with the Australian Government.

Recommendation: Government deepen collaboration with key global partners to enhance professional standards, strengthen security practices, and accelerate workforce development by investing in a national framework and shared global alignment.

Shield 6: Strong region and global leadership

CREST, with funding from the Department of foreign Affairs and Trade, has undertaken capacity building in the form or company mentoring (Vietnam and Indonesia) and training activities (Thailand), under the CREST Cyber Accelerated Maturity Programme (CREST CAMP). Broader international CREST CAMP activities have also been funded by the United Kingdom Foreign, Commonwealth & Development Office and the European Bank for Reconstruction and Development. This is the first and only international initiative to focus on developing cyber service providers and the skilled professionals they rely on. It is a pathway to accelerate cyber capability in countries that have identified the need to improve the maturity of their cyber ecosystem.

At its core, CREST CAMP fosters collaboration bringing together governments, private-sector organisations, educational institutions, and national authorities to strengthen local cyber security resilience. By uniting those seeking to build their cyber ecosystems with global experts, CREST CAMP contributes to a safer, more unified digital landscape.

Recommendation: Government provide funding to support the delivery of more CREST CAMP activities in Southeast Asia and the Pacific.

About CREST (International)

CREST (International) is an international not-for-profit, membership body representing the global cyber security industry. Since 2006 we have been leading the cyber security community to collectively raise the standards of cyber service providers and professionals, quality assuring the sector and in turn providing confidence to the buying community, governments and regulators. We work with industry, governments, regulators and academic institutions to fulfil our mission of building capability, capacity, consistency and collaboration in the cyber security industry.

CREST (International) has over 500 accredited member companies who are assessed against a rigorous standard, operating across dozens of countries. CREST accredits its member companies against one or more disciplines, including Penetration Testing, Vulnerability Assessment, Intelligence-Led Penetration Testing (CREST STAR), Threat Intelligence (CREST STAR), Incident Response, and Security Operations Centres.

We also certify thousands of professionals worldwide putting them through their paces in industry leading examinations. Through our elected Regional Councils, we actively engage with authorities in each of our five regions: North Americas, Asia, Australasia, EMEA and the UK.

If you would like to discuss this matter further, please contact [redacted]

Yours faithfully
CREST (International)

[redacted]