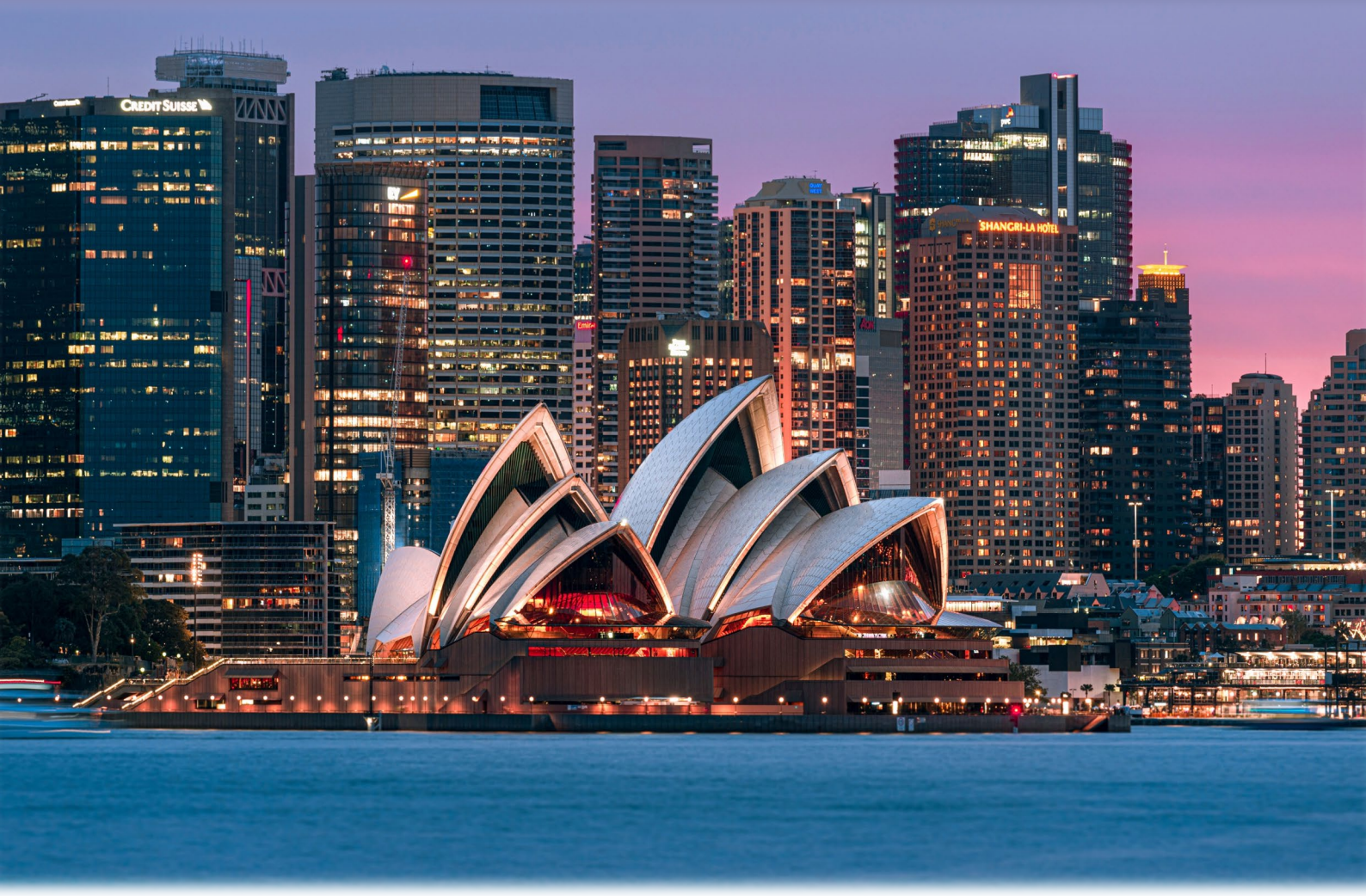
CYBERTRACE

1300 669 711
info@cybertrace.com.au
www.cybertrace.com.au



FORMAL REPLY

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

Without Prejudice

CYBERTRACE PTY LTD
ABN: 47 605 834 697
CAPI: 411710138 (NSW)

CYBERTRACE:V4 – 2023

A BRAND YOU CAN TRUST, A SERVICE YOU CAN RELY ON

Date: 11 April 2023

Our Ref: R20230411

Attention: Home Affairs

Authorised by: Mr. Dan Halpin

Role: Chief Executive Officer

Formal Reply

The Australian government has recognised the importance of cybersecurity and the need to combat cybercrime in collaboration with industry. As part of its efforts, an expert advisory board was established to provide advice and guidance on cybersecurity issues.

Based on our review of the discussion paper, we understand that the primary focus is the federal government's response to higher-level cybersecurity matters. However, we firmly believe that until the smaller issues surrounding state-level cybercrime reporting and investigation are solved, there is a limited chance that higher-level planning and response will be effective; especially if the model below it is broken. Instead of starting the planning from a high level, a bottom-up approach is needed.

Based on our experience with combatting cybercrime, meaningful change will not be realised until state and federal governments seriously address the regular inaction of state police and the role of industry (small and large) in combatting cybercrime.

For example, when reporting cybercrime, the majority of victims who contact our company, Cybertrace, report a negative experience with state police departments. Unfortunately, there appears to be a general reluctance from police station-based, generalist police to investigate cybercrime. In our view, this appears to be caused by a lack of training, a lack of formalised policy and procedure for investigating cybercrime, and negative police culture.

In frustration, many victims turn to specialist private investigators, such as Cybertrace, to investigate and capture time-sensitive evidence. However, in turn, police often refuse to accept evidence and intelligence provided by private investigation firms despite being licensed to provide these services, and in our case, subject matter experts.

In my view, there is no legal or procedural reason why police cannot or should not actively collaborate with private industry to combat cybercrime and provide higher-level support and service to victims of cybercrime. Public-private collaboration facilitates the sharing of knowledge, intelligence, and

unique investigative methodology. As industry traditionally leads the way with innovation, the advancement of investigative technologies will benefit the community as a whole. It is unlikely that this level of technical innovation would come from government departments which is a demonstration of why public-private collaboration is crucial.

Although this discussion paper does recognise the importance of industry for combatting cybercrime, we note the three individuals appointed to the board do not appear to have specific 'expertise' in cybercrime.

For future appointments, we recommend that board members hold demonstrated expertise in cybercrime and include industry representation from all areas of industry, not just major industries. Likewise, other board members could include CEOs of companies that have a demonstrated capability to develop and apply innovative technologies and academics who are theoretical experts in both cybersecurity and cybercrime.

Any failure to appoint sufficient expertise to an oversighting board, authority, think tank, or fusion centre may prevent government from effectively meeting its overall objective of combatting cybersecurity threats, specifically organised cybercrime operations.

To overcome a potential initial shortfall, we recommend the currently nominated board consider directing engagement with various areas of industry. This should involve a range of industry types and sizes including companies that hold significant expertise in combatting cybercrime.

Likewise, the board should focus its attention on improving the current processes and responses to cybercrime by state police organisations. In lieu of these recommendations, we foresee that any alternate and higher-level response will be deficient and fail to meet the government objectives, and the expectations of the Australian public to be protected from cybercrime.

If you have any further questions in relation to this matter, please contact our office on [redacted].

Kind Regards,

[redacted]

Dan Halpin
CEO
Cybertrace

W.cybertrace.com.au
E: contact@cybertrace.com.au
Ph. Australia: 1300 669 711