The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

25 May 2015

Dr Margot McCarthy
Associate Secretary, National Security and International Policy
Department of the Prime Minister and Cabinet
1 National Circuit Barton ACT 2600
margot.mccarthy@pmc.gov.au

Dear Dr McCarthy,

CYBER SECURITY REVIEW 2015

The Australian Industry Group (Ai Group) welcomes the Australian Government's review into cyber security.

We represent many Australian businesses across a wide range of sectors, including both the Information and Communications Technology (ICT) sector and other business users of ICT.

We understand that the Department of the Prime Minister and Cabinet will report to the Government on its findings and recommendations by mid-2015, with a new cyber security strategy to be released following this Review.

We are broadly supportive of the Government's leadership in following up from a previous cyber security review in 2011, and its direct consultation with Ai Group, our members and broader industry. We consider that this review is well overdue, especially given the Commonwealth's existing cyber security strategy was last released in 2009. With increasing penetration of digital technologies into the economy and society more broadly, now is an opportune time for an updated strategy.

Cyber security is a constantly evolving area whose importance is increasing in line with the use of rapidly changing digital technologies. Unless security is adequately managed through effective public and private action both independently and collaboratively, we will lag behind developing international standards and remain excessively vulnerable to security violations. Developing an effective cyber security framework will require ongoing and meaningful stakeholder engagement, especially with the business community.

This submission identifies particular areas of focus for designing a cyber security framework. They are:

- Improving data on the extent of cyber security issues and readiness to respond to such issues;
- Establishing and fostering an environment conducive to Government and business collaboration to respond to cyber security issues;
- Raising awareness of cyber security issues amongst the Australian public;

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

- Developing best practice and standards for managing cyber security for each business sector with proper stakeholder consultation; and
- Collaborating at an international level to develop best practice and standards to enable collaboration and information sharing with respect to cyber security.

Lack of data

We note that the review has been broad in its scope, which can be useful in taking a holistic approach to cyber security to assess where things are going well and where they are deficient in Australia. In the future, it would be more useful to narrow the issues further in order to consider more effective ways of addressing particular issues.

That being said, the broadness of the review suggests a fundamental issue with a lack of available data to inform government and businesses of the extent of cyber security issues, resilience and readiness across Australia. In our recent submission to the ABS's ICT Statistics Review, we emphasised the importance of having more statistical data to assist in identifying issues as they relate to Government, businesses and the broader community on cyber security risks and readiness to respond to such risks. Improving and sustaining the collection of such data should be a priority for the ABS, and will improve the capacity for evidence-based policy making and private sector responses.

Collaboration

We recognise that it is also important for Government, businesses and citizens to collaborate on tackling cyber security issues. Sharing of knowledge and experiences can be facilitated through coordinated engagement; a light-handed approach by Government that encourages (rather than penalises) an environment of open collaboration will play a vital role in this area. However, this should be accompanied by clear communication to businesses of what is expected in terms of best practice.

A collaborative environment can also be conducive to developing innovative solutions to counter cyber security. This is a positive side to the challenge of cyber security, which should be embraced.

Raising awareness of cyber security issues

We also recognise there is a need for a cultural shift in responding to cyber security. Greater connectedness of individuals, appliances, houses and workplaces brings great benefits, but also the potential for great disruption. Managing this will require awareness to be raised across society. This can be promoted through efforts in the education system, the professional and vocational skills and training systems, and broader community awareness campaigns.

For businesses, it is important to recognise that a broad brush should not be applied across the

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

industry sectors in managing cyber security. This is especially the case for those that may not be well-informed as ICT enablers. In such cases, it would be most effective if there is targeted and clearer guidance on the Government and society's expectations of best practice in managing cyber security. More data in these instances would assist in providing more effective remedies against cyber security issues specific to each sector.

Anecdotal feedback suggests some small- and medium-sized enterprises (SMEs) are not as well aware or prepared for managing cyber security risks and would like greater clarity from Government on what is required to manage cyber security. This is a common question in our work with SMEs as part of the Australian Government's Entrepreneurs' Infrastructure Programme, which includes a requirement for SMEs to put in place an appropriate cyber security strategy.

Developing best practice and standards

It would be useful in the immediate term to develop a guide(s) on what is best practice for each industry and sector. The review has initiated discussion on this, but more work will need to be done to develop a clear statement of expectations for adequate cyber security management.

This will require proper consultation on businesses' current cyber security practices and their perceived and actual success in managing the frequency and severity of, and resilience to, cyber security events. This will assist in establishing appropriate benchmarks relevant to each sector. To be clear, such benchmarks should be conceived as an aid to improved performance, not a uniform mandate for regulated practice. We would be happy to engage further with Government and our members to form a better understanding of the extent of cyber security issues and readiness in this area.

Global engagement

As the digital economy is a global economy, cyber security is a global issue, where threats often originate across borders. The Expert Panel for this review rightly includes international experts. Without ongoing engagement at an international level, there is a risk of fragmentation and lack of interoperability in handling cyber security.

Government and businesses should therefore support ongoing international collaboration in developing best practice and standards. Concepts of best practice and standards need to be better aligned between governments and businesses worldwide. For our part, Ai Group is collaborating with partners from across the B20 Coalition countries to promote growth of the global digital economy, and included in this agenda is addressing cyber security risks. We encourage Government and businesses to actively look for opportunities to collaborate with international partners so that there is a more effective global regime in place to address a global issue.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

We would be pleased to engage with the Government should there be a further opportunity. For further information in relation to this submission, please contact our adviser Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Peter Burn
Head of Influence and Policy