CYBER AND CRITICAL TECHNOLOGY INTERNATIONAL ENGAGEMENT STRATEGY

Department of Foreign Affairs and Trade
Australian Government

SUBMISSION

Submitted by

Organisation: (ISC)²
Lead Author: Tony Vizza, Director for Cyber Security Advocacy, Asia-Pacific
Email: tvizza@isc2.org
Phone: 0413 598 768
Postcode: 2000

Category: Other – (ISC)² – Information Security Industry Body – Not for Profit
Consent: This submission can be published.

EXECUTIVE SUMMARY

(ISC)² welcomes the Australian Government Department of Foreign Affairs and Trade (DFAT) Call for Submissions in relation to Australia's Cyber and Critical Technology International Engagement Strategy (CCTIES).

(ISC)² is an international non-profit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, the Certified Cloud Security Professional (CCSP®) certification, the Systems Security Certified Practitioner (SSCP®) certification, the Certified Secure Software Lifecycle Professional (CSSLP®) certification and the Healthcare Information Security and Privacy Practitioner (HCISPP®) certification, amongst others, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 150,000 strong, of which over 2,800 members are in Australia, consists of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education™.

(ISC)²'s mission is to support and provide members and constituents with credentials, resources and leadership to address cyber, information, software and infrastructure security to deliver value to society. The association was the first information security certifying body to meet the requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. All (ISC)² certifications have been accredited against this standard, making (ISC)² credentials a must-have among information security professionals and employers. (ISC)² credentials are recognised by the United States Department of Defense (DoD) through the 8140.01 and 8570.1 Directives, the National Recognition Information Centre (NARIC) in the United Kingdom, the Australian Signals Directorate through the Information Security Registered Assessors Program (IRAP) and the Enhanced Competency Framework on Cybersecurity (ECF-C) by the Hong Kong Monetary Authority, to name a few.

In Australia, (ISC)² has formed strong, strategic partnerships with the Department of Home Affairs' Australian Cyber Security Centre (ACSC), the Australian Information Security Association (AISA) and the Australian Computer Society (ACS). In addition to this, partnerships have been formed with the Government of Victoria and Government of New South Wales as well as working relationships with other state governments. (ISC)² also works collaboratively with AustCyber, the Office of the e-Safety Commissioner, universities across Australia as well as allied industry bodies including the Australian Security Industry Association (ASIAL), the IoT Alliance of Australia, the IoT Security Institute, the Australian Institute of Project Managers (AIPM), the Financial Services Council and Blockchain Australia.

Around the world, (ISC)² has formed strong and long-lasting partnerships with the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and National Institute for Cybersecurity Education (NICE) in the United States and the International Standards Organisation (ISO) at a global level. (ISC)² works closely with government agencies and bodies across the Asia-Pacific region and around the world. Regional examples include the Cyber Security Agency of Singapore and the Tokyo Metropolitan Police Department in Japan. As a result of the leadership position (ISC)² has taken to promote a safer and more secure cyber world, (ISC)² credentials are considered to be the gold standard in cyber security certification and excellence around the world.

This response offered by (ISC)² represents the collective views of over 150,000 certified cyber security professionals globally. These professionals are tasked with protecting and securing public and private sector organisations including national, state and regional governments, Fortune 100 companies, large enterprise, NGO's as well as SME/SMB across all industries, verticals and sectors.

It is hoped that the Department of Foreign Affairs and Trade will consider these views and incorporate the recommendations included as part of any future CCTIES strategy to help deliver Australians a safer and more secure cyber world, both now and well into the future.

TABLE OF CONTENTS

FORMAL RESPONSES

WHAT SHOULD AUSTRALIA'S KEY INTERNATIONAL CYBER AND CRITICAL TECHNOLOGY OBJECTIVES BE? WHAT ARE THE VALUES AND PRINCIPLES AUSTRALIA SHOULD PROMOTE REGARDING CYBERSPACE AND CRITICAL TECHNOLOGIES?

The current cyber threat environment is well documented by agencies both in Australia and globally. The gravity and severity of the cyber threat situation as it currently stands is best illustrated by World Economic Forum research that indicated that cyber security and privacy-related risks are listed as two of the top ten global risks in terms of likelihood and impact.[1] The Australian Governments Office of the Australian Information Commissioner (OAIC) publishes statistics related to the Notifiable Data Breach scheme that has been in effect since 2018. The latest Notifiable Data Breaches Report for July to December 2019 showed an increase in data breach notifications of 19% over the previous period.[2] With the continuing development of digitization, interconnectedness, the ubiquity of social media platforms, the age of the Internet of Things (IoT) and the erosion of the concept of privacy, there is significant risk that the current cyber threat environment will only escalate.

Cognisant of this, Australia is well placed to develop globally leading objectives for cyberspace and critical technologies that will not only ensure that it can meet the challenges associated with these emerging areas, but to benefit from them on the global stage. These include:

- **Advocating for an internationally agreed to multi-lateral treaty governing cyber space** with a particular focus to "de-weaponize" cyberspace. In doing so, the overall goal of the Australian government should be to promote a safer and more secure cyber world, one that seeks to ensure that sovereign states are using cyberspace peacefully and deploying cyber security technologies only for defensive capabilities.

1. **Advocating for internationally recognised cross-border information privacy principles in line with Article 12 of the United Nations Declaration of Human Rights**[3] to ensure that Australians as well as global citizens hold sovereignty over their own personal data and can enforce the levels of privacy as appropriate to their wishes.
2. **Pursuing the global standardisation of cyber security concepts though a common industry lexicon** such as the (ISC)[2] Cybersecurity Lexicon[4] for example.
3. **Endorsing and promoting the internationally accepted ISO/IEC 17024:2012 Personnel Accreditation**[5] scheme to ensure that cyber security professionals around the world and in Australia are accredited in a globally recognised cybersecurity certification, such as those administered by (ISC)[2] which are ISO/IEC 17024 accredited.
4. **Endorsement of the internationally accepted ISO/IEC 27000 series of Information Security Management accreditations**[6] to demonstrate that organisations such as government departments, NGO's and private enterprise are capable of protecting the information security assets of both its own operations, as well as of their stakeholders.

[1] World Economic Forum, 'Global Risk Report 2020', http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.
[2] Office of the Australian Information Commissioner, Australian Government, "Notifiable Data Breaches Report – July-December 2019", https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/
[3] United Nations (UN), 'Universal Declaration of Human Rights', https://www.un.org/en/universal-declaration-human-rights/.
[4] The (ISC)[2] Cybersecurity Lexicon – An introduction to basic cybersecurity terminology and concepts, https://www.isc2.org/-/media/ISC2/Training/The-ISC2-Cybersecurity-Lexicon.ashx
[5] International Standards Organisation (ISO), 'ISO/IEC 17024:2012 Conformity Assessment – General Requirements for bodies operating certification of persons', https://www.iso.org/standard/52993.html.
[6] International Standards Organisation (ISO), 'ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary', https://www.iso.org/standard/73906.html.

HOW WILL CYBERSPACE AND CRITICAL TECHNOLOGY SHAPE THE INTERNATIONAL STRATEGIC/GEOPOLITICAL ENVIRONMENT OUT TO 2030?

The current cyber threat environment is well documented by agencies both in Australia and globally and recent cybersecurity events since the emergence of the COVID-19 pandemic have illustrated that drastic action is required both now and well into the future. In Australia, a number of high-profile breaches and incidents have occurred since the COVID-19 pandemic that have affected critical systems. These include breaches of Toll Group[7], BlueScope[8], Bigfooty.com[9], the NSW Government[10] and Lion Group[11] to name a few.

As indicated prior, the cyber threat situation indicates that cyber security and privacy-related risks are listed as two of the top ten global risks in terms of likelihood and impact.[12] The Australian Governments Office of the Australian Information Commissioner (OAIC) has also indicated an increase in data breach notifications.[13] With the continuing development of digitization, interconnectedness, the ubiquity of social media platforms, the age of the Internet of Things (IoT) and the erosion of the concept of privacy, there is significant risk that the current cyber threat environment will only escalate out to 2030, with the potential that cyberspace and critical technology will be leveraged by nation states as a geopolitical and economic bargaining tool, or perhaps, even as a weapon. Given this context, it is likely that cybersecurity will become a "Top 3" risk for organisations, rivalled only by climate change and global pandemics in terms of magnitude and impact out to 2030.

Compounding this dire outlook, it is well documented both by international organisations such as (ISC)² in its annual Cybersecurity Workforce Study[14] as well as Australian government entities such as AustCyber[15] that a global cybersecurity skills shortage exists. Addressing the skills gap to ensure that the Australian economy both trains and retains quality cyber security talent will be essential to meeting the challenge of remaining competitive on the world stage.

As the world's largest association of certified cyber security professionals, (ISC)² contends that the single biggest area for focus by government to meet future challenges in cyberspace, both in Australia as well as globally, will be in the cyber security education area. Measures that can be adopted by the Federal Government to meet these challenges can include but should not be limited to:

- **Ensuring cybersecurity professionals are duly certified in globally recognised cybersecurity certifications such as those accredited by the ISO/IEC 17024 standard to demonstrate** knowledge, skills and abilities in line with industry best practices, helping to ensure their organisations are adequately protected.
- **Ensuring adequate investment in cyber education from a young age, including at the pre-school level and continuing through primary and secondary school**, to ensure that toddlers, children and teenagers understand cyber threats as they grow up and as social environments they belong to evolve.
- **Ensuring vocational education providers such as TAFE's and private sector providers align their cyber security course curricula to global industry standards** such as those provided in the Australian Signals Directorate's proposed *Cyber Skills Framework*.
- **Ensuring Australia's universities and TAFE's align their cyber security programs to global industry standards and partnering with global peak industry bodies such as (ISC)²** to ensure that graduates possess both the appropriate skills as well as prudent mindset required to be effective cyber security professionals.

---

[7] IT News, 'Toll Group's corporate data stolen by attackers', 12th May 2020, https://www.itnews.com.au/news/toll-groups-corporate-data-stolen-by-attackers-548033
[8] ZDNet, 'BlueScope reports cyber incident affecting Australian Operations', 18th May 2020, https://www.zdnet.com/article/bluescope-reports-cyber-incident-affecting-australian-operations/.
[9] Nine News, 'Exclusive: 70 million records exposed in data leak from AFL fan website, cyber researchers claim', 29th May 2020, https://www.9news.com.au/national/afl-fan-website-70m-data-leaks-expose-users-private-conversations-phone-numbers-emails/4b6f5c5c-7a76-4198-8e24-b90270faf2b3.
[10] ZDNet, 'Citizen data compromised as Service NSW falls victim to phishing attack', 14th May 2020, https://www.zdnet.com/article/citizen-data-compromised-as-service-nsw-falls-victim-to-phishing-attack/.
[11] IT Wire, 'Australian drinks maker Lion shuts systems after cyber incident', 10th June 2020, https://www.itwire.com/security/australian-drinks-maker-lion-shuts-systems-after-cyber-incident.html.
[12] World Economic Forum, 'Global Risk Report 2020', http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.
[13] Office of the Australian Information Commissioner, Australian Government, "Notifiable Data Breaches Report – July-December 2019", https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/
[14] (ISC)², 'Cybersecurity Workforce Study, 2019', https://www.isc2.org/Research/Workforce-Study
[15] AustCyber, 'SCP – Chapter 3 – The Challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development', https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3

HOW SHOULD AUSTRALIA PURSUE OUR CYBER AND CRITICAL TECHNOLOGY INTERESTS INTERNATIONALLY?

From a cyber and critical technology perspective, there are a number of principles Australia should be cognisant of when determining the pursuit of its cyber and critical technology interests at an international level. These include:

- **The understanding that a safe and secure cyber world, which includes the safety of critical technology, is in the fundamental best interests of both Australia and the wider world**. As an association, it is the primary mission of (ISC)[2] to realise a safer and more secure cyber world.
- Given the borderless nature of the internet, **in order for Australia to manage its cyber and critical technology interests internationally, it is imperative that a multi-lateral approach to the issue is considered.** Simply speaking, Australia cannot "go it alone" and will need to ensure that it works pragmatically with international partners and NGO's such as (ISC)[2] to derive an approach that will best protect governments, businesses and individuals.
- **Given the continuing rise of state-sponsored cyber threat actors, it is in Australia's strategic national interest to work with international partners on a multi-lateral strategy that seeks to address this**. This could be in the form of a cybersecurity version of the Convention on International Civil Aviation[16] (the *Chicago Convention*), signed in 1944, which to this day continues to successfully govern the civil aviation industry.
- As a stable, mature and free democracy with constitutionally-entrenched protections for individuals and their personal data, **Australia can lead the world in advocating for cross-border information privacy principles in line with Article 12 of the *United Nations Declaration of Human Rights***[17] to ensure that Australians as well as global citizens hold sovereignty over their own personal data and can enforce the levels of privacy as appropriate to their wishes. As an example, there is an increasingly prevalent view that privacy is being eroded due to the monetization of data by "big tech". As a result, many jurisdictions around the world are strengthening or planning to strengthen privacy rules to ensure that citizens are able to use technology, and are exercising a level of privacy that they deem acceptable. There is a case to be made for the harmonization of these rules to ensure cross-border compatibility.
- In terms of foreign trade opportunities, Australia should:
    - **Capitalise on the global demand for cyber security skills, knowledge and experience by utilising its network of world-leading universities, vocational education providers such as TAFE's and private sector providers to meet the cyber security skills shortage**, currently estimated by (ISC)[2] to be over 4 million people around the world.[18] Most of this shortage exists in the Asia-Pacific region. By ensuring that graduates possess both the appropriate skills as well as a prudent mindset required to be effective cyber security professionals, this will ensure that Australia becomes a net exporter of high-quality cyber security workers.
    - **Promote Australian-made and Australian-owned cyber security and world-leading information technology products and services to the world**, with a particular focus on the small to medium enterprise market. Whilst entities such as AustCyber have achieved good results in this arena, there is significantly more that can be realised. As nation states are seeking to develop (or in many cases re-develop) domestic manufacturing capabilities in the aftermath of the COVID-19 pandemic and its economic after-effects, a strong local cyber security and critical infrastructure sector is also vital for Australia's domestic economic interests.
    - **Promote the adoption of regulations ensuring manufacturers of information technology products incorporate best practice cyber security protections within the products they manufacture** to ensure they meet a minimum level of protection for consumers. A good example of this is Senate Bill No. 327[19] passed by the State of California in the United States.

[16] ICAO, 'Convention on International Civil Aviation – Doc 7300', https://www.icao.int/publications/pages/doc7300.aspx.
[17] United Nations (UN), 'Universal Declaration of Human Rights', https://www.un.org/en/universal-declaration-human-rights/.
[18] (ISC)[2], 'Cybersecurity Workforce Study, 2019', https://www.isc2.org/Research/Workforce-Study.
[19] *Senate Bill No. 327 Information Privacy: Connected Devices* (California), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

HOW CAN GOVERNMENT, INDUSTRY, CIVIL SOCIETY AND ACADEMIA COOPERATE TO ACHIEVE AUSTRALIA'S INTERNATIONAL CYBER AND CRITICAL TECHNOLOGY INTERESTS?

There is a pressing need for government, industry, academia and society to cooperate to achieve its needs and interests related to cybersecurity and critical technology at an international level. Steps that will help facilitate this cooperation include:

- **Ensuring these sectors actively contribute to the Australian Government's proposed *2020 Cyber Security Strategy*** as is currently being developed by the Department of Home Affairs by ensuring that their voices, opinions and recommendations are incorporated into that strategy.
- Given the continuing rise of state-sponsored cyber threat actors that have actively targeted many of these sectors in recent times**, it is in Australia's strategic national and economic interests to better protect Australian institutions from foreign attack or infiltration**. A significant component of this will need to occur at the international level through the advocacy of multi-lateral conventions on matters related to cyber security and critical infrastructure. Again, this could be in the form of a cybersecurity version of the Convention on International Civil Aviation[20] (the *Chicago Convention*).
- Ensuring that Australian government departments, private enterprise, NGO's and other organisations protect their information according to information security best practices and develop organisational resilience to issues of cyber security. (ISC)^2 maintains that the best method of achieving this is for **the Government to endorse, promote and adopt the internationally accepted ISO/IEC 27000:2018 family of Information Security Management System accreditations.[21]**
- Ensuring that cybersecurity personnel employed in the government, academic and civil sectors are duly accredited to an internationally recognised standard that demonstrates skills, experience and adherence to a code of ethics, while requiring credential holders to continually update their knowledge through the pursuit of continuing professional education. To this end, **the Federal Government should consider endorsing, promoting and adopting the internationally accepted ISO/IEC 17024:2012 Personnel Accreditation[22] scheme** to ensure that cyber security professionals in Australia and around the world are skilled, experienced and accredited in a globally recognised cyber security certification, such as those administered by (ISC)^2, certifications which are all ISO/IEC 17024 accredited.
- **Capitalising on the global demand for cyber security skills, knowledge and experience by utilising its network of world leading universities, vocational education providers such as TAFE's and private sector providers to help meet the cyber security skills shortage**, currently estimated by (ISC)^2 to be over 4 million people around the world.[23] In addition, it would be prudent to ensure that the programs taught by academia are globally relevant and meet the needs of industry and government. In ensuring that graduates possess both the appropriate skills, experience and mindset required to be industry-ready and work-ready cyber security professionals, this will ensure that Australia becomes a net exporter of high-quality and in demand cyber security workers.
- **Government, academic, industry and civil entities partnering with globally recognised international industry bodies such as (ISC)^2** to ensure that the cyber skills gap both in Australia and abroad is systematically addressed and converted into a nationally strategic advantage.

[20] ICAO, 'Convention on International Civil Aviation – Doc 7300', https://www.icao.int/publications/pages/doc7300.aspx.
[21] International Standards Organisation (ISO), 'ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary', https://www.iso.org/standard/73906.html.
[22] International Standards Organisation (ISO), 'ISO/IEC 17024:2012 Conformity Assessment – General Requirements for bodies operating certification of persons', https://www.iso.org/standard/52993.html.
[23] (ISC)^2, 'Cybersecurity Workforce Study, 2019', https://www.isc2.org/Research/Workforce-Study.

WHAT POLICIES AND FRAMEWORKS EXIST IN OTHER COUNTRIES THAT DEMONSTRATE BEST PRACTICE APPROACHES TO INTERNATIONAL CYBER AND TECHNOLOGY POLICY ISSUES?

There are a number of policies and frameworks formulated or adopted outside of Australia that the Government, both Federal and State, should consider helping to develop a coherent approach to managing international cyber and technology policy issues. For example:

1. To help Australia advocate **for an internationally agreed multilateral treaty governing cyber space and privacy** with a particular focus to "de-weaponize" cyberspace, it would be a prudent move to consider the development and success of multilateral treaties that have helped to standardise industries that in past years were novel in their own right. An excellent and enduring example of this is the Convention on International Civil Aviation[24] (otherwise known as the *Chicago Convention*), which was signed in 1944 and continues to effectively govern the civil aviation industry to this day. By advocating the cause of an international convention on cyberspace, Australia can take a leadership role in helping to promote a safer and more secure cyber world.
2. To assist Australia in ensuring that cybersecurity personnel are accredited to an internationally recognised standard, **the Government should consider endorsing, promoting and adopting the internationally accepted ISO/IEC 17024:2012 Personnel Accreditation[25] scheme** to ensure that cyber security professionals around the world and in Australia are accredited in a globally recognised cybersecurity certification, such as those administered by (ISC)[2] which are ISO/IEC 17024 accredited.
3. To ensure that Australian government departments, private enterprise, NGO's and other organisations protect their information and data assets according to information security best practices, **the Government should consider endorsing, promoting and adopting the internationally accepted ISO/IEC 27000:2018 family of Information Security Management System accreditations[26]** for use in Australia and around the world. These include ISO/IEC 27001 (Information technology — Security techniques — Information security management systems — Requirements), ISO/IEC 27005 (Information security risk management), ISO/IEC 27014 (Security Governance), ISO/IEC 27017 (Cloud Security) and ISO/IEC 27034 (Application security). Adoption of the ISO/IEC 27000 family of standards will help demonstrate that organisations such as government departments, NGO's and private enterprise are capable of protecting the information security assets of both its own operations, as well as of their stakeholders.
4. **Considering the adoption of the highly regarded US Government NICE Framework**[27] as a basis for the Australian Government's *Cyber Skills Framework* currently under development by the Australian Signals Directorate. Such a framework will serve as a reference structure describing the interdisciplinary nature of the work involved in cyber security.

[24] ICAO, 'Convention on International Civil Aviation – Doc 7300', https://www.icao.int/publications/pages/doc7300.aspx.
[25] International Standards Organisation (ISO), 'ISO/IEC 17024:2012 Conformity Assessment – General Requirements for bodies operating certification of persons', https://www.iso.org/standard/52993.html.
[26] International Standards Organisation (ISO), 'ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary', https://www.iso.org/standard/73906.html.
[27] National Initiative for Cybersecurity Education (NICE), U.S. Department of Commerce, United States Government, 'NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.