PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE

Department of Home Affairs
Australian Government

SUBMISSION

Submitted by

Organisation: (ISC)²
Lead Author: Tony Vizza, Director for Cyber Security Advocacy, Asia-Pacific
Email: [redacted]
Phone: [redacted]
Postcode: [redacted]
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's Department of Home Affairs (DHA) Call for Submissions in relation to Protecting Critical Infrastructure and Systems of National Significance.

(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 2,900 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 AS/NZS/ANSI/ISO/IEC Standard 17024. 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 Home Affairs will consider these views and incorporate the recommendations included as part of any future Critical Infrastructure and Systems of National Significance strategy to help deliver Australians a safer and more secure cyber world, both now and well into the future.

TABLE OF CONTENTS

EXECUTIVE SUMMARY ***2***

FORMAL RESPONSES TO QUESTIONS ***4***

QUESTION 16: THE SECTOR REGULATOR WILL PROVIDE GUIDANCE TO ENTITIES ON HOW TO MEET THEIR OBLIGATION. ARE THERE PARTICULAR THINGS YOU WOULD LIKE TO SEE INCLUDED IN THIS GUIDANCE, OR BROADER COMMUNICATION AND ENGAGEMENT STRATEGIES OF THE REGULATOR? **4**

A – ENDORSEMENT, PROMOTION AND ADOPTION OF ISO/IEC 27000:2018 FAMILY OF CYBER SECURITY CONTROLS 4

B – ENDORSEMENT, PROMOTION AND ADOPTION OF AS/NZS ISO/IEC 17024:2012 CYBER SECURITY PERSONNEL ACCREDITATIONS 5

C – ADOPTION OF RECOGNISED CYBERSECURITY SKILLS FRAMEWORKS 5

D – ESTABLISHING APPROPRIATE LEVELS OF INFORMATION SECURITY EXPECTATIONS FOR REGULATED ENTITIES 5

E – MODERNISING AND STRENGTHENING PRIVACY PROVISIONS AND REGULATIONS 6

F – IMPLEMENTING REGULATIONS REQUIRING MINIMUM LEVELS OF CYBER SECURITY FOR CONSUMERS 6

G – PARTNERING WITH GLOBALLY RECOGNISED INTERNATIONAL INDUSTRY BODIES AND ASSOCIATIONS 6

QUESTION 21: DO YOU HAVE ANY OTHER COMMENTS YOU WOULD LIKE TO MAKE REGARDING THE PSO (POSITIVE SECURITY OBLIGATION)? **7**

ABOUT THE LEAD AUTHOR ***8***

FORMAL RESPONSES TO QUESTIONS

QUESTION 16: THE SECTOR REGULATOR WILL PROVIDE GUIDANCE TO ENTITIES ON HOW TO MEET THEIR OBLIGATION. ARE THERE PARTICULAR THINGS YOU WOULD LIKE TO SEE INCLUDED IN THIS GUIDANCE, OR BROADER COMMUNICATION AND ENGAGEMENT STRATEGIES OF THE REGULATOR?

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 indicates 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]

These results are further reinforced by a report from the Australian Signals Directorate in conjunction with the Australian Federal Police and the Australian Criminal Intelligence Commission indicating that over 59,000 cybercrime reports were received in the 2019-20 financial year, with 2,266 incidents responded to by the Australian Cyber Security Centre.[3] In fact, the report illustrated that over the period, over 1,070 cyber incidents to organisations defined by DHA as critical were reported.[4]

Clearly, organisations are in desperate need of guidance on how to meet their cyber obligations, particularly organisations in the Critical Infrastructure arena as well as those in sectors of national significance. Recommendations to address some of these concerns include the following:

A – ENDORSEMENT, PROMOTION AND ADOPTION OF ISO/IEC 27000:2018 FAMILY OF CYBER SECURITY CONTROLS

To achieve better cybersecurity resilience for organisations, **DHA should endorse, promote and adopt the internationally accepted ISO/IEC 27000:2018 family of Information Security Management System accreditations[5] for use by sector regulators and regulated entities to help ensure that they meet their information security obligations.**

The family of ISO/IEC 27000:2018 accreditations recommended for endorsement, adoption and promotion includes 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).

By promoting adoption of the ISO/IEC 27000 family of standards to regulated entities, sector regulators for critical infrastructure and systems of national significance can expect elevated levels of cyber resilience by regulated entities and will increase the capability of these entities in protecting the information security assets of their own operations as well as of their stakeholders. By adopting this recommendation, many of the actions listed in the Australian Governments *2020 Cyber Security Strategy* can be realised. Crucially, the critical infrastructure sector will lead by example to further promote positive cybersecurity measures across broader society and in non-critical sectors as well.

In relation to adoption of ISO/IEC 27000:2018 certification by regulated entities, the DHA could consider subsidising or funding the cost of certification, either on a grant's basis, via tax relief or other funding arrangement.

---

[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] Australian Cyber Security Centre, 'ACSC Annual Cyber Threat Report – July 2019 to June 2020', https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020.
[4] Ibid. Refer to page 7. This number includes all sectors listed as defined by DHA as 'critical' for the purposes of the consultation paper.
[5] 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.

B – ENDORSEMENT, PROMOTION AND ADOPTION OF AS/NZS ISO/IEC 17024:2012 CYBER SECURITY PERSONNEL ACCREDITATIONS

To ensure that the cyber workforce in regulated entities are trained in globally recognised, quality-assured and industry relevant knowledge, **the DHA should endorse, promote and adopt the internationally accepted AS/NZS ISO/IEC 17024:2012 Personnel Accreditation[6] scheme**. This will ensure that cyber security professionals employed by regulated entities are accredited in globally recognised cybersecurity certifications, such as those administered by (ISC)[2], all of which are AS/NZS ISO/IEC 17024 accredited.

In addition, **the DHA should consider following the lead set by the Government of Victoria in mandating that public sector staff who manage cyber security for Victorian Government departments are trained and certified in AS/NZS ISO/IEC 17024 accredited certifications.**[7] Since October 2019, the Victorian Government has actively been promoting the CISSP, SSCP, CCSP, CSSLP and HCISPP certifications administered by (ISC)[2] to staff in their IT and cybersecurity functions. This complements the Victorian Government strategy that all public sector workers, regardless of job role, should receive some level of cyber security awareness and training, contingent on job function. A similar approach by sector regulators to regulated entities will yield additional benefits in ensuring that cyber security outcomes for these entities can be realised.

C – ADOPTION OF RECOGNISED CYBERSECURITY SKILLS FRAMEWORKS

Cybersecurity is a vast area comprising of a number of different skills needed to ensure that organisations adequately protect from, detect and respond to cyber incidents. In recognising this, **the DHA should consider the adoption of the Australian Signals Directorate *Cyber Skills Framework***[8] which leverages the widely adopted and highly regarded US Government National Institute for Cybersecurity Education (NICE) Framework.[9] By adopting the *Cyber Skills Framework,* sector regulators will leverage a standardised reference structure that describes the interdisciplinary nature of the knowledge, skills and abilities required to perform all aspects of cyber security work, including technical, operational, management, governance, risk and compliance based cybersecurity work. This will also ensure that regulated entities are cognisant of which knowledge, skills and abilities are valuable and consistent with best practice as deemed by the Australian Signals Directorate as well as through NICE.

D – ESTABLISHING APPROPRIATE LEVELS OF INFORMATION SECURITY EXPECTATIONS FOR REGULATED ENTITIES

In order to achieve the aims of resilience, workforce and skills, business growth and innovation, **the DHA should consider setting the appropriate levels of expectation in relation to how regulated entities conduct themselves regarding their information security posture.** Recommendations to help achieve this goal include:

- The Federal Government partially or fully subsidising the cost of ISO/IEC 27000:2018 certification for regulated entities to ensure that those organisations are employing best practice information security management practices and techniques in their day-to-day business.
- The Federal Government partially or fully subsidising the costs of AS/NZS ISO/IEC 17024:2012 personnel certification for regulated entities to ensure that personnel working in these organisations protecting information assets are experienced, ethical and verified experts in their field.

[6] 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.
[7] For further information, please contact the Department of Premier and Cabinet, Victorian Government – https://www.vic.gov.au/department -premier-and-cabinet.
[8] Australian Signals Directorate, 'ASD Cyber Skills Framework', https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework.
[9] 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.

E – MODERNISING AND STRENGTHENING PRIVACY PROVISIONS AND REGULATIONS

Many jurisdictions around the world have strengthened privacy rules to ensure that citizens are able to use technology and exercising a level of privacy that they deem acceptable. **The DHA should consider the promotion of reforms of the Commonwealth *Privacy Act 1988*** to ensure that the privacy needs of individuals and businesses who may be customers of regulated entities are met in today's digital era. As guidance, DHA should refer to the European Union's General Data Protection Regulation (GDPR)[10] and the *California Consumer Privacy Act of 2018*[11] as good examples for such reform.[12]

F – IMPLEMENTING REGULATIONS REQUIRING MINIMUM LEVELS OF CYBER SECURITY FOR CONSUMERS

The DHA should consider the adoption of regulations that ensure that regulated entities who manufacture or provide information technology products and services incorporate best practice cyber security protections within these products they manufacture and/or distribute to ensure those products meet a minimum level of protection for consumers. The state legislature of California in the United States has legislated Senate Bill No. 327[13], popularly known as the '*IoT Security Law*' offering consumers appropriate levels of protection, and DHA should promote the adoption of similar regulation at a federal level to ensure IT products are fit for sale to customers of regulated entities. This is particularly important as consumers may consider that products supplied by regulated entities in the critical infrastructure sector to be inherently 'cyber safe' by virtue of their origin.

G – PARTNERING WITH GLOBALLY RECOGNISED INTERNATIONAL INDUSTRY BODIES AND ASSOCIATIONS

The DHA and sector regulators should partner with globally recognised international peak industry bodies and associations such as (ISC)² and encourage regulated entities do the same. This will ensure that strong alignment exists between sector regulators, regulated entities and the broader global cyber security community represented by cybersecurity professionals and professional bodies that represent the cybersecurity industry.

By partnering with global peak industry bodies, the relevance of measures that the DHA and sector regulators are undertaking can also be showcased at an international level, demonstrating both sovereign capability as well as export capacity for high quality cyber security know-how and products and services reliant on these capabilities.

---

[10] European Commission, 'EU data protection rules', https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[11] *California Consumer Privacy Act of 2018*, 160 Cal Civ Code § 1798.100 – 1798.199 (2018).
[12] European Commission, 'EU data protection rules', https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[13] *Senate Bill No. 327 Information Privacy: Connected Devices* (California), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

QUESTION 21: DO YOU HAVE ANY OTHER COMMENTS YOU WOULD LIKE TO MAKE REGARDING THE PSO (POSITIVE SECURITY OBLIGATION)?

From a cyber and critical technology perspective, there are a number of principles that would be applicable to a proposed Positive Security Obligation that should be considered, further to the recommendations already made in this submission. 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 as well as the wider world**. As an association, it is the primary mission of (ISC)[2] to realise a safer and more secure cyber world.
- **The concept of 'security by design and 'privacy by design', ensuring that both concepts are incorporated at the planning stage of any critical infrastructure system reliant on electronic communication.** By adopting security and privacy by design, the Critical Infrastructure sector can demonstrate that it is adopting security considerations as a primary issue rather than an afterthought, and this will translate into better security outcomes for regulated entities as well as their stakeholders.
- 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[14] (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***[15] 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.

[14] ICAO, 'Convention on International Civil Aviation – Doc 7300', https://www.icao.int/publications/pages/doc7300.aspx.
[15] United Nations (UN), 'Universal Declaration of Human Rights', https://www.un.org/en/universal-declaration-human-rights/.

ABOUT THE LEAD AUTHOR

Tony Vizza
Director for Cyber Security Advocacy
Asia-Pacific
(ISC)²

Tony Vizza has been involved in the information technology, information security and privacy fields for more than 25 years.

Tony has completed a Bachelor of Science in Computing Science from the University of Technology, Sydney and a Global Executive MBA from the University of Sydney which included study at Stanford University in the United States, The London School of Economics in the UK and the Indian Institute of Management, Bangalore in India. Tony is currently studying for a Juris Doctor law degree at the University of New South Wales.

Tony's information security credentials include CISSP (Certified Information Systems Security Professional), CCSP (Certified Cloud Security Professional), CIPP/E (Certified Information Privacy Professional / Europe), CRISC (Certified in Risk and Information Systems Controls), CISM (Certified Information Security Manager) and he is a certified ISO/IEC 27001 Senior Lead Auditor.

Tony is a member of the Board of Directors for the Australian Information Security Association (AISA), a Cyber Security Ambassador for the NSW Government, the co-chair for the (ISC)² Asia-Pacific Advisory Council, a member of the Cybersecurity Industry Advisory Committee for the NSW Government, a member of the Technology and Business Services Industry Skills Reference Group for NSW TAFE, a member of the Data Security Standards Committee for Blockchain Australia and has provided expert services to the Australian Government's Australian Prudential Regulation Authority (APRA), the Law Society of NSW, the Australian Security Industry Association Limited (ASIAL), the Australian Institute of Project Management (AIPM) as well as numerous boards.

Tony is an expert speaker on information security regularly speaking across the Asia-Pacific region on information security matters. He has also taught and mentored young and aspiring information security students through Victoria University, TAFE NSW and TAFE Victoria in association with Infoxchange and has lectured cybersecurity students at the University of Technology, Sydney, the University of New South Wales and the University of Queensland.

Tony is a regular contributor to numerous cyber security and IT industry publications including CSO Magazine, Infosecurity Magazine, Cyber Today Australia, Security Insider Magazine, Australian Reseller News (ARN), Channel Reseller News (CRN) and Lifehacker, amongst others, regarding information security, business and channel strategy.