SECURITY LEGISLATION AMENDMENT

(CRITICAL INFRASTRUCTURE) BILL 2020

EXPOSURE DRAFT BILL

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

EXECUTIVE SUMMARY

AISA welcomes the request for submissions from the Australian Government's Department of Home Affairs in relation to the exposure draft bill for the proposed amendments to the *Security of Critical Infrastructure Act 2018* (Cth).

The Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and privacy in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

This response offered by AISA represents the collective views of over 7,000 cyber security and information technology professionals, allied professionals in industries such as the legal, regulatory, financial and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Cyber Security Centre, AustCyber, Cyrise, the Risk Management Institute of Australia (RMIA), the Australian Strategic Policy Institute (ASPI, the Australian Institute of Company Directors (AICD), the Oceania Cyber Security Centre (OCSC), the Australian Security Industry Association Limited (ASIAL) as well as international partners such as $(ISC)^2$, ISACA, the Association of Information Security Professionals (AiSP) and over twenty five Universities and TAFEs across Australia.

It is AISA's hope that the Department of Home Affairs will consider the responses to the Exposure Draft Bill and incorporate recommendations included as part of a holistic drive by the Australian Government to help deliver a safer and more secure cyber world for the people of Australia, both now and well into the future.

THE AISA VIEW OF THE EXPOSURE DRAFT BILL

The Australian Information Security Association (AISA) is supportive of the process to seek consultation with industry and the broader community on the strategy to improving the cybersecurity strategy enunciated in the Federal Governments '*Australia's Cyber Security Strategy 2020*' released on 6th August 2020.

AISA notes the work to date from the Australian Government, particularly through its approach towards securing the digital economy through the passage of a tranche of legislation directed at improving Commonwealth powers that provide oversight of activities ranging from the '*Foreign Transaction and Acquisition Act 1975'*, the '*Telecommunications and Other Legislation Act 2017 (TOLA)'* through to the '*Security of Critical Infrastructure Act* 2018' (Cth) (SOCI).

The caveat of 'national security' has remained a constant theme to the focus of each piece of legislation with an underlying direction towards the improvement of cybersecurity management. Indeed, the impact arising from these changes has required review and amendment to other legislation including *the Criminal Code Act 1995*, A*dministrative Decisions (Judicial Review) Act 1997*, and the *Intelligence Services Act 2001*. Notwithstanding this broad approach, there is yet further amendments leveraging a national security business theme with the '*Foreign Investment Reform (Protecting Australia's National security) Bill 2020* (in review process). Naturally, the difficulty associated with reviewing each piece of legislation and their interconnection is both complex and untimely.

In September of this year, the Department of Home Affairs (*the* ***Department***) through the Critical Infrastructure Centre (CIC) released a Consultation Paper – '*Protecting Critical Infrastructure and Systems of National Significance*' in which the principal tenet of proposed changes was introduced to the public for consideration and response through a five-week submission process. The Department received 194 submissions, 66 requesting confidentiality, with the remaining 128 now available on the Department's website for general access.[1] AISA contributed a response describing 'in-principle' support for a deeper and more granular definition of the composition of critical infrastructure, specifically with the focus upon the positive security obligation (PSO), enhanced cyber security obligations (ECSO) and government access, and notes a number of responses from AISA strategic partners such as (ISC)2,[2] AustCyber,[3] and the Oceania Cyber Security Centre,[4] that AISA is broadly in support of.

AISA members ascribe to a strong sense of civil liberties and the privacy rights of individuals and entities to operate in a democracy with a free-enterprise economy. In light of this, the use of an 'enlivening' approach to the Regulatory Powers Act in Section 37 of the legislation suggests an approach by Government that, far from collaborative in nature, is compromising of human rights and free enterprise. This approach combined by what may be construed as the punitive nature proposed in the legislation may serve to undermine the industry support necessary to foster a positive relationship between the private sector and the Commonwealth and this risk should be noted.

In lieu of a detailed analysis of the exposure draft, AISA will contribute its assessment whilst protesting the inadequate time provided for review and consultation with our membership and a broader community and industry audience. Three weeks is not considered an appropriate length of time for the review of important legislation where the complexity does not lie in the authorship of legislation, but instead relies upon the support and input from industry. Indeed, the success of the desired outcome is wholly dependent upon input and collaboration from the private sector. It is also unremarkable that the aspect of inadequate consultation time and review is reflected '*simpatico'* throughout many of the 128 submissions.

[1] 'Protecting Critical Infrastructure and Systems of National Significance', Department of Home Affairs, Australian Government, <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>.
[2] Ibid. Please refer to the (ISC)2 submission under 'Submissions to the Consultation Paper.
[3] Ibid. Please refer to the AustCyber submission under 'Submissions to the Consultation Paper.
[4] Ibid. Please refer to the Oceania Cyber Security Centre submission under 'Submissions to the Consultation Paper.

The exposure draft legislation for the Security of Critical Infrastructure (SOCI), (*the **Legislation***) released on 9th November for public comment follows the blueprint described in the initial consultation paper with some inclusions and exclusions evident in the draft Bill. Additionally, to support the Exposure Draft of the legislation, the Department also released an accompanying draft Explanatory Document and an exposure draft (and accompanying explanatory Statement) for the Exposure Draft of the Intelligence Services Regulations 2020 (the Regulations). The legislation incorporates greater detail in relation to the role of the Australian Signals Directorate (ASD), (*the **Agency***) and its subordinate elements orchestrated through the Australian Cyber Security Centre (ACSC). Similarly, powers given to the Secretary of the Department (*the **Secretary***) are detailed and expansive.

AISA contends that the documents provided by the Department comprise a significant amount of material with wide implications and outcomes reflecting national security and national interests, and again, reiterates the view that the compressed timeframes provided do not allow for due process to be enacted in a matter so vital to the national interest.

The three 'Town Hall' consultations revealed that the legislation is to be submitted to the House in the December 2020 sitting period. Once submitted, the nature of the legislation will mandate its review before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) which is currently facing no less than ten pieces of legislation, including the 'controversial' legislative aspects contained in TSSR (TOLA). An unsettling aspect of the legislation is its reference to the TSSR review. It is noted that several critical infrastructure sectors refer to the Regulator underpinned by the TSSR legislation. Therein, a degree of uncertainty exists with regard to the regulated management of some critical infrastructure sectors as the outcome of TSSR (TOLA) is not yet finalised. Importantly, some of these elements may be classified as systems of national significance. These regulatory complexities were acknowledged in the explanatory notes, particularly where critical infrastructure sectors and the associated assets may be outsourced to industry however remain under the control of the respective State or Territory government. Accordingly, industry is likely to face a myriad of complex, confronting and contradictory legal frameworks.

Crucially, there is no indication of how the cost for implementing the approach described in the legislation will be met by industry or supported by Government. The only section in the legislation with regard to compensation addresses the matter of compensation for acquisition of property. Yet, the legislation is replete with penalties and fines for failure to comply. In times of economic uncertainty such as those currently faced, there is a credible argument that costs will be borne entirely by the regulated entities could eventuate in poor resilience outcomes, defeating the purpose of the regulation.

Simply put, given the rate of legislative development, AISA contends that the minimalist approach to consultation will undermine the successful implementation of managing critical infrastructure. It is difficult to establish and build collaboration and trust between the government and industry when the environment is not fully engaged. The current process will realise further legislation before the House wherein critical elements necessary for its successful implementation such as consultation groups with industry are only just beginning. The 'co-design' process touted in the explanatory notes is due to commence in parallel to the legislation's process through the House. It is doubtful that any meaningful outcomes through an industry discourse will be completed before the legislation gains royal assent.

Understanding the priority on addressing the rising threat environment, if it is passed as-is, at a minimum, we would suggest a circuit breaker assessment at one year to review and amend the legislation after further consultation.

SPECIFIC AREAS OF CONCERN

Rather than attempt to address each aspect of this considerable raft of documentation, AISA has identified the following key areas of concern contained within the Exposure Draft:

1. The nature of the intent and language present in the explanatory document to the SOCI Bill ascribes to multiple aspects that are not addressed in the legislation. For example, there is no mention of:
    i. the Critical Infrastructure Centre (CIC).
    ii. The Trusted Information Sharing Network (TISN).
    iii. The Protective Security Obligation.
    iv. Collaboration.
    v. Threat management.
    vi. Information sharing.
    vii. Co-design.
2. Definitions. This section has undergone significant change with 29 pages representing 141 new definitions with a focus towards defining those elements relating to sector-specific environments, especially where computer assets or access requirements are described. For example, the definition of '*asset*' includes:
    a. A system, a network, a facility, a computer, a computer device, a computer program, computer data, premises, and 'any other thing'.
        i. Whilst noting that any judicial decisions will take context into account in any ruling. the last component of this proposal 'any other thing' is too broad and could potentially undermine the entire list prescribed under the definition of *asset*.
    b. There is a broad definition of a Critical Infrastructure Asset as: 'has the meaning given by subsection 8E(1)'. Paragraph 8E(1) states:
        i. 'An asset is a critical infrastructure sector asset if it is an asset that relates to a critical infrastructure sector'.
        ii. Similarly, the definition for critical infrastructure sector reflects:
            1. 'Each critical the critical infrastructure sector for a critical infrastructure asset is the critical infrastructure sector to which the asset relates'.
        iii. Each critical sector is defined separately and more specifically with deeming to ascribe assets to sectors relating to the legislation and the SOCI 2018 Act.
    c. The definitions that relate to information technology do not reflect any specific industry standard such as NIST, or the ASD Information Security Manual.
    d. Some definitions remain unchanged from the SOCI 2018 Act including '*National Security*'. This has broader implications arising from the use of the term 'national security business' that has been introduced as a concept across interrelated Acts (extant and pending) where the legislation is referenced.[5]

[5] This reference is directed at the Foreign Investment Reform (Protecting Australia's National security) Bill 2020 (before the House at present) that has wider implications where this proposed legislation is referenced.

3. Positive security obligation. Whilst the term is not contained in the legislation, the explanatory notes describe the PSO concept as 'holistic' that will build on the extant SOCI 2018 Act to embed preparation, prevention and mitigation activities into the BAU operations of critical infrastructure assets 'ensuring the resilience of essential services is strengthened' thereby providing increase 'situational awareness of threats'.

    a. The PSO is achieved through three initiatives:

        i. Adopting and maintaining an all-hazards risk management program,

        ii. Mandatory cyber security incident reporting to ASD), and

        iii. Where required, providing ownership and operational information to the Register of Critical Assets'.

    b. These initiatives will only apply once a rule is made that prescribes the asset as critical infrastructure.

    c. It should be noted that no timings or process for achieving the 'rules' are defined in the legislation. The explanatory document describes that 'responsible entities of critical infrastructure assets will be required to take an 'all-hazards' approach to risk management. Similarly, there is no context or definition to the term 'hazard', except in association with 'impact'.[6]

    d. Government and industry stakeholders will 'work together to co-design the sector-specific requirements that will 'underpin the risk management program obligation'. There is recognition in the explanatory document that the co-design process will 'develop a clear set of requirements' for each of the critical sectors which:

        i. Recognise and do not duplicate extant regulatory requirements,

        ii. Principles-based and risk-profile 'proportionate' to the critical sector. And

        iii. The 'least regulatory burden' to achieve security outcomes.

    e. The cost of implementing these initiatives is not addressed in the legislation.

    f. The legislation provides penalties should false or misleading information be provided when requested or directed. This aspect is defined under Division 3 and relates to actions that occur with a cyber incident. The legislation would allow this element to apply across all aspect of the legislation where an offence is committed against section 137.1 or 137.2 of the Criminal Code Act 1995 that relates to this Act.

[6] The concept of 'all hazards' approach was enunciated in the Critical Infrastructure Resilience Strategy: Policy Statement 2015 (Cth) and the Critical Infrastructure Resilience Strategy: Plan 2015 (Cth).

4. Critical Infrastructure Risk Management Program (CIRMP). (Part 2A)(30AA) This new requirement mandates that each responsible entity adopt and maintain a CIRMP that applies to the entity. It is 'principles based' reflecting the following outcomes:

    a. Identify material risks.

    b. Mitigate risks to prevent incidents.

    c. Minimise the impact of 'realised' incidents

    d. Effective governance.

    e. The CIRMP impact reflects:

        i. Additionally, the responsible entity must provide an annual report to the Secretary Failure to comply may result in a 200-penalty unit ($44,400) fine (for each offence by type or category, or a 150 unit ($33,300) fine for non-compliant reporting.

        ii. There are significant aspects associated with the CIRMP approach that reflect:

            1. Sectoral risk management. The legislation allows for flexibility and varied plans. However, it does not address the varied needs for each sector as there are varying capabilities within sectors. This is true of cybersecurity capable sectors such as banking and finance where some entities have extremely good cybersecurity whereas other in the same sector have far less technology, skills and knowledge.

            2. The use of AusCheck. This service does not currently support the broader critical infrastructure sectors and will require time and staff to meet demands. Similarly, sectors that have not required personnel vetting will need to adopt HR processes to support this requirement. This criterion will place additional load upon responsible entities.

            3. Staff training and awareness. Many sectors and respective assets do not have staff trained in risk management. The public submission by AustCyber draws clear reference to the difficulties faced by the problem of the skills shortage and specialist knowledge. [7] It should also be noted that awareness is only the first step and the longevity of awareness is short lived. The driver should be toward longer lasting behaviour change.

            4. Risk management standards. Whilst the Risk Management Institute of Australia is not listed amongst the public submissions their opinion should be evident in the explanatory document.

            5. Technology implications. Sectors will require the use of technology that is currently not present or capable of facilitating a CIRMP approach.

            6. Sovereign risk. Industry faces complex risk management where potential foreign interference and the bounds of national security place the responsible entity in an exposed position through actions of a third-party. The submission by the Cyber Security Cooperative Research Centre (CSCRC)[8] reinforced this issue through the recent decision to deny Chinese acquisition

[7] Submission 44 to Protecting Critical Infrastructure & Systems of National Significance
[8] Submission 112 to Protecting Critical Infrastructure & Systems of National Significance

of Lion Dairy.[9] A market announcement on the final outcome of this incident is detailed in recent media across Australia.[10] Commentary in the media suggest that this reality is yet another 'difficulty' created within the current Australia-China relationship.

iii. Sector-specific rules. (30AH)(1)(c) Essentially this approach is rules based in that as a minimum each sector and assets are expected to 'consider' and address risks in the following key domains:

1. Physical security
2. Cyber security
3. Personnel security
4. Supply chain risks.
5. Additionally, in certain circumstances the rules may also:
    a. Mandate the steps responsible entities should be taking through the CIRMP to address these risks (including in relation to governance arrangements);
    b. Accept the extant industry standards and practices are sufficient to meet aspects of the PSO; and
    c. De-conflict requirements for entities which fall within more than one definition of a critical infrastructure asset.

[9] AFR article link.
[10] ABC news – Bega cheese confirms purchase of Lion Dairy link.

5. Mandatory reporting of cyber security incidents. (Part 2B). Mandatory reporting of cyber incidents represents the third initiative within the PSO. Currently, industry is only bound through the data breach legislation to report a cyber incident. This new requirement lifts the standard significantly with reporting to ASD or through the ACSC. Of interest the legislation provides:

    a. 'If a cyber security incident has a relevant impact on a critical infrastructure asset, the responsible entity for the asset may be required to give a relevant Commonwealth body a report about the incident'.

    b. The key aspect is if the incident has a 'relevant' or a 'significant' impact on the availability of the asset.

    c. A responsible entity must report that a critical cyber security incident has or is occurring within 12 hours of the entity becoming aware that the incident has, or is having, a significant impact (whether direct or indirect) on the availability of the asset. In the case of any 'other' cyber incidents the mandatory reporting timeframe moves out to 24 hours. In each case the penalty for failing to report is 50 penalty units ($11,100).

    d. The implications arising from this requirement reflect:

        i. The responsible entity must be 'aware' of the incident',

        ii. The responsible entity must have a degree of cybersecurity awareness to recognise the threat, and thereby be able to classify the incident as either 'relevant' or significant'. Definitions within the legislation (8G) describe 'relevant impact of a hazard, and a cyber security incident in terms of:

            1. Availability

            2. Integrity

            3. Reliability

            4. Confidentiality

                a. Information about the asset,

                b. Information is stored in the asset (the information), and

                c. If the asset is computer data – the computer data.

    e. The difficult here arises in the assumption that all assets and entities have or can develop the skills necessary to ensure compliance with this requirement.

    f. Where a third-party supplier Is the provider then assets and responsible entities will bear the responsibility for ensuring contractual relationships are sufficient to protect both the asset, the third-party supplier and the responsible entity.

    g. The explanatory documents raise the concept of 'aggregated threat' management as a consequence of the visibility across sectors and assets arising from this approach. The term 'aggregated threat' is not reflected in the legislation. Similarly, there is no mention of the processes required to direct actions through or across the critical infrastructure sectors that would correlate and distribute threat management mitigation strategies as required.

6. Enhanced Cyber Security Obligations. (Part 2C). This element has been incorporated to address the needs of those assets described or recognised as 'systems of national significance (SoNS). The obligations under this initiative may not be voluntary, but rather enforced 'from time to time'. The impact of that requirement is that the responsible entity and the assets must remain at a preparedness level that reflects an optimal transition to the ECSO requirements with little to no notice. Additional aspects arising from this approach reflect:

    a. Statutory incident response planning. (Division 2) (30CB). The incident response plans are described in the explanatory document as 'playbooks' or plans to ensure that an entity has established processes and tools to prepare for and respond to security incident. Essentially the entity must have a formal IR plan.

        i. The failure to have a plan that is appropriate, managed and reported to the Secretary is subject to 200 penalty units ($44,400) (for each infraction).

    b. Cyber Security exercises. (Division 3) (30CS). This element describes an exercise that can be conducted as a 'tabletop' exercise, or where the scope could be expanded to include teaming exercises across multiple assets. The aim is to test the entities:

        i. Ability to 'appropriately' respond to the incident,

        ii. Preparedness to respond 'appropriately', and

        iii. Ability to mitigate the relevant impacts the cyber incident/s could have on the system/s.

            1. The failure to comply with the requirement to undertake a cyber security exercise and provide an evaluation report to the Secretary is subject to 200 penalty units ($44,400) (for each infraction).

    c. Vulnerability assessment. (Division 4). This requirement can be conducted in relation the system, all types of cyber security incidents or at any time deemed necessary or appropriate by the Secretary.

        i. Designated Officers. (30DQ). The legislation introduces the appointment and use of 'Designated Officers'. The definition afforded to this role is typically pointless; A *designated officer* is an individual appointed by the Secretary, in writing, to be a designated officer for the purposes of this Act. A designated office is to be an APS employee in the Department, or a staff member of ASD (within the meaning of the *Intelligence Services Act 2001* (Cth))[11].

            1. The role of the designated officer appears throughout the legislation and describes an important capability for the Department and the Agency in the performance of duties associated with the legislation. There is a section later that provides immunity from prosecution. In the conduct of a vulnerability assessment, designated officers may:

                a. undertake the assessment,

                b. gain access to premises, and

[11] Part 5A of the Intelligence Services Act 2001 describes who may be employed or engaged under the Director-General of ASD.

c. access to computers.

ii. Whilst consultation between the Secretary and the entity is described in the legislation, compliance is mandatory. An entity failing to comply may be subject to 200 penalty units ($44,400) (for each infraction).

7. Access to system information. (Division 5). This is the last element applicable to SoNS. System information is:

   a. information that relates to the operation of the computer needed to operate a system of national significance which may assist with determining whether a power under this Act should be exercised in relation to the system of national significance, in particular the powers set out in Part 3A.

   b. System information however does not include personal information within the meaning of the Privacy Act 1988.

   c. Where required, the Secretary may require the entity to provide reports to ASD. If necessary, those reports may be machine-generated or automated. The government will provide the program and the entity will comply. Whilst this aspect is described in the explanatory document it is not specifically referenced in the legislation.

      i. An entity is not excused from giving a report on the ground that the report might lead to incriminate the entity.

      ii. An entity must comply or is subject to 200 penalty units ($44,400).

8. Responding to Serious Cyber Incidents. Part 3A of the SOCI Act 2018 provides the Minister with power to issue a direction to a reporting entity or operator to require them t take action to mitigate risks. The draft legislation provides an 'emergency mechanism' which empowers the Minister to intervene in the event of an incident.

   a. New terms reflect 'seriously prejudiced', is 'seriously prejudicing', or 'is likely to seriously prejudice':

      i. the social or economic stability of Australia or its people:

      ii. The defence of Australia; or

      iii. National security; and

      iv. No existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

   b. If an incident meets these conditions, the Minister for Home Affairs may authorise the Secretary to do one or more of the following for a certain period of time:

      i. give directions to a specified entity for the purposes of gathering information;

      ii. give directions to a specified entity requiring the entity to take a specific action in response to the incident; or

      iii. give a request to an authorised agency to provide specified assistance and cooperation in response to the incident.

9. Information gathering directions. (Division 3). To give an information gathering direction, the Minister must be satisfied that it is likely to facilitate a practical and effective response to the incident. An entity must comply with an information gathering direction to the extent that the entity is capable of doing so. Failing to do so can result in a penalty of $33,300 (150 penalty units).

    a. To give an action direction, the Minister must be satisfied that all of the following criteria are met:

        i. the specified entity is unwilling or unable to take all reasonable steps to resolve the incident.

        ii. the direction is reasonably necessary for the purposes of responding to the incident.

        iii. the direction is a proportionate response to the incident, having regard to the impact of the direction on the activities carried on by the specified entity, the functioning of the asset concerned, the consequences of compliance with the direction and any other relevant matters; and

        iv. compliance with the direction is technically feasible.

    b. Failing to comply with an action direction can result in a penalty of 2 years imprisonment and/or a fine of $26,640.

10. Action Directions. (35AQ). Once the Minister is 'aware of the acts or things required to effectively respond to an incident', the Minister may authorise the Secretary to give specified entity a specified direction.

    a. In certain circumstances, the government may also authorise ASD to step in to respond to an incident including by accessing, modifying or analysing computer systems or data.

    b. The legislation does give rise to an aspect whereby immunity from prosecution is provided.

    c. These powers are defined, extensive, but contain considered efforts to constrain or prevent their misuse.

11. Intervention requests. This element permits that action may be undertaken but is constrained by four elements that determine if the specified direction is proportionate to the incident.

    a. There are further controls which the Minister must consider including of the direction is technically feasible, and that the course of action is reasonably possible to execute. Before an authorisation is given the Minister must seek the approval of:

        i. The Prime Minister and

        ii. The Defence Minister.

    b. Time constraints also apply to the direction.

    c. Of significant note, the entity, or its officer, employee or agent, is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction given under section 35AQ. This immunity will protect the entity from any civil claims that may arise as a result of complying with the direction.

    d. There is a significant list of activities that may be undertaken including:

        i. Access or modify a computer

        ii. Undertake an analysis of a computer, a program, computer data, or any device that relates to the computer's operation

        iii. Install a program access. Add, restore, copy or delete data held in a computer

        iv. Alter the functioning of a computer, or a device that is part of the asset

        v. Remove, disconnect, connect or add a computer or device

        vi. Remove from premises.

            1. The significance of these activities is associated with the stronger controls assigned to this type of authorisation.

            2. A designated officer can conduct these activities and may be assisted by a Constable (or equivalent under the *Criminal Code Act 1995*) (Cth). This aspect also allows for the use of 'reasonable force' to gain entry to a premise for the purpose of executing the direction. Note, the use of force against an individual is not permissible under the legislation.

            3. Importantly, IGIS has extensive oversight powers that include the Department, the Agency and those elements appointed by and acting on behalf of the Minister and the Secretary.

12. Information Gathering. The powers provided to the Minister have been extended to reflect the measures in the legislation under the *Regulatory Powers Act 2014* (Cth). The legislation 'enlivens' these powers with the consent of the entity or under warrant to:

    a. Monitoring powers. search premises, examine or observe any activity, inspect documents, operate electronic equipment and ask questions in order to determine whether an obligation under the Act is being complied with.

    b. Investigation powers. search premises, inspect documents, seize evidence, operate electronic equipment and ask questions in order to gather evidence in relation to the contravention of an obligation under the Act.

    c. As per the Regulatory Powers Act, a person who fails to answer a question from an authorised person, or to provide reasonable assistance and facilities to an authorised person and any person assisting the person, where premises have been entered under a warrant will be liable to a civil penalty.

        i. The use of these powers is described by the explanatory document as the intention to 'enliven' the associated parts of the Regulatory Powers Act belies the aggressive and proactive nature of legislation that is supposedly designed to reflect collaboration and co-design with industry. This is not so much as a 'carrot and stick' approach that is 'all stick'.

ABOUT THE LEAD AUTHOR

Scott Ainslie

Managing Director

Scott has served in a wide variety of roles across a career distinguished by the breadth and depth of his exposure to the modern threat landscape.

His knowledge reflects significant governance, risk and compliance elements with a focus on the regulatory and control requirements expected of diverse and complex environments. His experience reflects engagement with IT and OT associated with the critical infrastructure landscape in a practical manner and through his research and engagement across the wider ISAC community.

His multi-domain knowledge has significantly contributed to the introduction of risk-based approaches addressing critical areas not discussed previously in some business sectors. His demeanour and dynamic attitude contribute to cooperation and partnership with stakeholders to achieve a successful outcome.

His approach reflects extensive exposure to the physical, personnel and logical security domains, and his results are underscored by his use of intelligence-based threat and risk management approaches to address cybersecurity and associated critical infrastructure vulnerabilities. His personable approach and demeanour provide an ideal platform for collaboration and negotiation environments.

An Honorary Research Fellow at Federation University Australia (Faculty of Science and Technology) through his long-standing relationship with the Internet Commerce Security Laboratory. Scott was awarded a Master of Cyber Security, Strategy and Diplomacy from the University of New South Wales in 2018.

He is a member of multiple security, risk, intelligence, and information security-related organisations, and his active membership provides an ideal platform for applying an intelligence-based approach to cybersecurity risk management. His association with professional organisations empowers his ability to seek outreach from a broad global community of like-minded cybersecurity practitioners.

ABOUT CONTRIBUTING AUTHORS

Tony Vizza

Director of the Board

Australian Information Security Association

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, 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 United States Department of Energy, 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 works for $(ISC)^2$ as the Director for Cyber Security Advocacy for the Asia-Pacific.

Tony is an expert speaker on information security regularly speaking across the world and in 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.

SPECIAL RECOGNITIONS

AISA would also like to recognise the efforts of the following individuals in the preparation of this submission.

- Mr John Morss, Deakin University Law School
- Mr Michael Trovato, Member of the Board of Directors, AISA
- Mr Damien Manuel, Chairperson, AISA.