Public Consultation on ‘Draft SOCI Risk Management Program (RMP) Rules’

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

COVERING LETTER

18.11.2022

The Department of Home Affairs
E-submission via ci.reforms@homeaffairs.gov.au

Dear Minister for Home Affairs,

Re: Public Consultation on 'Draft SOCI Risk Management Program (RMP) Rules'

We have attached a submission on the Public Consultation on Draft SOCI Risk Management Program (RMP) Rules' from our perspective as the peak professional body for information security and cyber security in Australia.

Thank you for the opportunity to contribute our views and your consideration. Please do not hesitate to contact Michael Trovato, or myself if you would like clarification of any of the comments made in this submission.

Sincerely,

Damien Manuel
Chairperson, AISA

Email: damien.manuel@aisa.org.au
Mobile: +61 439 319 603

INTRODUCTION

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. We welcome the request for submissions in response to Public Consultation on the 'Draft SOCI Risk Management Program (RMP) Rules'. AISA has previously provided a submission for the Security Legislation Amendment (Critical Infrastructure) Bill 2020 Exposure Draft Bill.

Established in 1999 as an independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and security-related privacy matters 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 for a world where all people, businesses and governments are educated about the risks and dangers of invasion of privacy, 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. AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education and organisational excellence.

This submission represents the collective views of over 9,500 cyber security, information technology and privacy 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 Institute of Company Directors (AICD); the Australian Security Industry Association Limited (ASIAL); Australian Women in Security Network (AWSN); Cyrise; grok academy; International Association of Privacy Professionals (IAPP); the Risk Management Institute of Australia (RMIA); the Oceania Cyber Security Centre (OCSC); untapped; as well as international partner associations such as ISACA; $(ISC)^2$; and the Association of Information Security Professionals (AISP). AISA also works closely with both federal and state / territory governments to ensure a robust and safe sector.

It is AISA's hope that our views will be considered. In this submission, we have covered matters of particular interest to AISA at this stage of the consultation.

EXECUTIVE SUMMARY

AISA welcomes the opportunity to provide feedback on the 'Draft SOCI Risk Management Program (RMP) Rules'. We offer our perspective as a members-based association, and as advocates for enhancing responsible information security standards and initiatives that in turn will address systemic challenges, improve digital trust, and enhance resilience in a cyber world.

A strong and effective government-industry partnership is central to achieving the Australian Government's vision for critical infrastructure security and resilience. Building on industry engagement during the development of amendments to the Security of Critical Infrastructure Act 2018 (the SOCI Act), Home Affairs have consulted widely with government and industry partners in developing asset definitions and risk management program rules. AISA understands the aim is to ensure that vital services to Australia's security, economic prosperity and way of life are included and to reduce the regulatory burden on industry.

Since 9/11 the discussion of impacts to critical infrastructure have been widely informed, discussed, and debated. Sadly, much of this has resulted in to slowly developed or no legislation and limited regulation of critical infrastructure world-wide, as well as Australia. AISA supports and encourages the enactment of SOCI, amendments, and evolving regulation.

Under Legislation, responsible entities – the owner or operator of a critical infrastructure asset – will need to develop an RMP and have this signed off by their board, council, or other governing body. In developing their programs, responsible entities will need to comply with RMP Rules, which focus on four key hazard domains: cyber and information security, personnel hazards, supply chain, and physical security hazards and natural hazards. Governance rules that outline what an entity must have regard to in the development of their risk management program, must also be adhered to.

AISA participated in the Cyber and Infrastructure Security Centre (CISC) all sector introductory town hall meetings on in October to commence consultation. At the meetings, the CISC provided information on the formal consultation process and the proposed RMP Rules, RMP Guidance, AusCheck background check for critical infrastructure, Protected Information Guidance, and an RMP Annual Report Submission form.

Observations of particular interest from AISA are listed below. Overall, AISA support the implementation of RMPs and the requirement for management and boards to attest to their use and management of risk to acceptable levels.

RMP cyber standards purpose and scope

Many have called for use of voluntary standards and the appeal is both that this is politically palatable, business friendly, and allows for greatest flexibility. Essentially this is what we have now, which many AISA members would tend to agree has not worked that well – if it did, we would not be having the scale of service outages and data breaches we have today.

Section 8 of the Exposure Draft 'Cyber and information security hazards'; Paragraph 8(4)(a) of the instrument requires that the entity's program must comply with one of the frameworks contained in the documents as listed in the table as in force from time to time. The five documents (frameworks) for compliance within that table are known well within industry.

AISA recommends changing the language from compliance to implement and utilise to manage risks, as these standards were not developed as compliance regimes.

AISA fully supports #2 Essential Eight Maturity Model published by the Australian Signals Directorate, without qualification.

AISA also understands the desire for flexibility in using different models but wants to highlight the nuance with respect to the models suggested below, and the key question they generally answer as described in the table below.

Purpose and scope	ISO 27000 Series (1)	NIST CSF (3)	C2M2 (4)	AESCSF (5)
	How is cyber security managed?	**How good are we at using industry standards and best practices to manage our cyber security risks?**	**How mature are our cyber security capabilities? Can we measure them?**	**How mature are our cyber security capabilities? Can we measure them using a tool specifically developed for the Australian Energy sector?**
	The ISO 27000 Series provides a broad range of best practice recommendations on information security management. It covers monitoring, risk management, measurement, analysis, and evaluation of the Information Security Management System (ISMS). ISO 27000 Series are arguably the most well-known, international set of standards on information security. **These standards are broad and independent of industry.**	A high level, taxonomy of non-prescriptive cyber security outcomes and a methodology to assess and manage those outcomes. Focuses on cyber security, not information security (i.e., does not include physical information). A very popular framework originating from the US critical infrastructure sector. Provides Informative references and mapping to several control frameworks. **The standard is cyber security specific and (although initially designed for critical infrastructure in 2014) independent of industry.** **It can be used to measure maturity of capabilities but was not initially designed for it.**	The Cybersecurity Capability Maturity Model (C2M2) contains a set of common cyber security practices that can be used to evaluate, prioritise, and improve cyber security capabilities. As a maturity model, C2M2 includes practices that range from foundational to more advanced in terms of either technical sophistication or consistency and repeatability. This enables C2M2 to be used to understand the current state of a cyber security program and track growth over time. **The standard is cyber security specific and (although initially designed for critical infrastructure) independent of industry. It was designed to measure maturity of a cyber security program.**	The framework's purpose is to enable the Australian energy sector to assess, evaluate, prioritise, and improve their cyber security capability and maturity. It leverages Electricity Subsector Cybersecurity Capability Maturity Model (ES- C2M2), NIST CSF, Australian Privacy Principles and ACSC Essential Eight. **The standard is designed for the Australian energy sector and cyber security specific. It was designed to measure maturity of a cyber security program. In 2022, the framework was planned for extension to the liquid fuels sector.**

AISA recommends an RMP for all organisations where they utilise #1 to support their ISMS, plus #2 Essential Eight to manage certain cyber risks, and then a choice of #3, #4, or #5 depending on sector/situation, versus using just one framework as suggested in the draft instrument.

Draft AusCheck background check

As part of the consultation process, a draft AusCheck Background Checks for the purpose of a Risk Management Program was provided. It outlines how background checks for the RMP obligation will be undertaken through the AusCheck scheme. Feedback gathered will be used to amend the AusCheck Regulations 2017 and establish the checking mechanism. We understand there is a desire to provide this level of background check as an option for personnel associated with roles that may impact critical infrastructure, particularly for cyber in lieu of a professional accreditation program. It was discussed during consultation that there is an intent to develop a digital ID system as well.

AISA recommends that any digital ID systems be developed using the Trusted Digital Identity Framework, enabled by Digital Transformation Agency's proposed Digital Identity Legislation 2021 to limit the risks to our members' personal information.

The shared risks landscape

We are witnessing how data breaches have a direct impact to individuals critical infrastructure organisations can be called upon to combat cybercrime[1]. Interconnectivity and dependencies on material service providers will not go away. As such, Home Affairs should look at increasing risk management requirements and obligations in relation to supply chains. However, it is important to acknowledge that the definition of materiality in relation to service providers will vary greatly from entity to entity and AISA recommends Home Affairs works with organisations to define suppliers who actually are critical, highly linked or have access to large customer data sets.

AISA recommends Home Affairs to consult the Commonwealth Risks Management Policy [2] and consider the definition of 'shared risk' and consider the benefit of its inclusion as an element of the instrument.

According to the Department of Finance, shared risks are those risks extending beyond a single entity which emerges from a single source and impacts interrelated objectives of entities. A collaborative approach to managing shared risk is required to: identify accountability, nominate transparent roles and responsibilities, define risk appetite boundaries, and seek agreement between all parties. This may require extended application of RMPs to supply chain entities of all industry types across several verticals. Additional delays managing the risks of fourth parties may be encountered due to contractual uplift requirements with service providers.

The cyber security skilled gap and lack of standardised accreditation

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 Australian public as well as businesses and government in Australia. This month, as part of the Australian Cyber Conference 2022, also known as CyberCon, in her opening speech, The Hon Clare O'Neil MP said:

"*The new Government in Australia has made the decision to have a cyber security minister because we want to elevate this issue to the level of importance that it so clearly is for Australia business, for Australia citizens and very much for our nation. Cyber is everything and it is everywhere. A resilient cyber ecosystem is going to be fundamental to our country's future. Cyber security underpins economic growth both here in Australia and across our region more broadly. It provides confidence in the services and infrastructure that enable business activity. It supports our economy, and it enables our way of life."*

[2] https://www.finance.gov.au/government/comcover/commonwealth-risk-managment-policy

AISA applauds the announcement but is also raises the following statistics of concern that APRA entities will have to confront:

The severe shortage or accessibility of job-ready cyber security and technology focused risk professionals will remain a key challenge. It is estimated that Australia may need around 30,000 additional cyber security workers for technical as well as non-technical positions by 2026. Growth is not sufficient to meet demand.[3] While there are challenges to solve at both the supply (education) and demand (hiring / employer) sides it is evident that remediation will take many years while the cost of obtaining and retaining cyber security, cloud and technology risk staff will continue to increase.

Support for industry accreditation is mixed and not sufficiently supported by industry leaders. Recent AISA Research into Cyber Security Accreditation in Australia [4] indicates that: (i) support for industry accreditation is mixed. Only 53.1 % of respondents support accreditation of the sector to ensure a base level of qualification and standard; and (ii) Industry leaders from Executive Advisory Board for Cyber (EABC) see accreditation of the cyber sector as unnecessary and complex to be inclusive. In addition, hiring managers consider a candidate's aptitude, attitude and work experience to be the most important when making hiring decisions. Industry certifications and educational background are deemed much less important when recruiting cyber security staff.

AISA acknowledges that a holistic approach for skilled cyber security work force is required to address market complexities and existing challenges across the industry. AISA urges that Home Affairs will consider the need for **detailed succession plans** for key security roles and the transition of "institutional knowledge" in order to support resilience.

[3] Data raised by The Upskilling and Expanding the Australian Cyber Security Workforce research report from CyberCX September 2022.
[4] https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/2022/AISA%20Accreditation%20Survey%20Report.pdf

About the Lead Authors

Michael Trovato – AISA Board Member, MAISA, GAICD, CISA, CISM, CDSPE

Mike Trovato joined IIS in 2018 with over 40 years' experience in consulting and financial services in Australia, Asia Pacific, and the USA. He is a cyber security, privacy and technology risk advisor to boards, board risk committees, and executive management.

Mike focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

At IIS, Mike has led over 100 privacy and security governance, risk, and compliance client engagements across government, health care, education, retail, financial services, and technology sectors. He has also advised clients about the direct impact of cyber security on privacy and data protection and how to provide greater resilience to assure better organisational outcomes.

Mike also serves as ICG's Global Cyber Practice Leader and IIS is an ICG Affiliate. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York; and has held financial services industry roles at Salomon Brothers and Mastercard International. At EY, Mike was responsible for creating the largest, sustained "Big-4" cyber security practice, deploying Privacy and Data Protection solutions, and building the Melbourne Advanced Security Centre (ASC), specialised in attack and penetration testing.

As the NAB's first Group Technology Risk and Security GM, Mike was responsible for risk assessment, strategy, and the security program with a budget of AU$6 million, 11 direct reports and 40+ team members. He focused on enhancing technology risk and security governance, functional security analysis capabilities, and establishing key regulatory and compliance activities.

Mike is a Non-Executive Director of au Domain Administration Limited (auDA), a not-for-profit organisation established by the Australian Internet community to administer a trusted .au for the benefit of all Australians, and champion an open, free, secure and global Internet. He is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (MAISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); and Certified Information Systems Auditor (CISA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of The New Governance of Data and Privacy: Moving from compliance to performance, Australian Institute of Company Directors, November 2018.

Contributors

Damien Manuel – Chairperson, AISA and Adjunct Professor

As an experienced, results-driven ICT business professional, Damien Manuel has more than 25 years of experience specialising in cyber security, business governance, compliance and risk management.

Damien is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level. Damien also provides advice to several boards both in Australia and internationally. He is a well-known leader in the Australian cyber security sector and works closely with both federal and state / territory governments.

In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. He also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra and Melbourne IT and is currently on CompTIA's Executive Advisory Committee.

Damien has supported CompTIA for over 14 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and more recently the CompTIA Advanced Security Practitioner certification.

Damien's passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus.