18 November 2022

Providence

Providence Consulting Group Submission into the proposed Risk Management Program Rules enabled by the *Security of Critical Infrastructure Act 2018* (SOCI Act)

Providence Consulting Group (Providence) welcomes an opportunity to make a submission to the Department of Home Affairs (Department) on the draft Risk Management Program (RMP) Rules enabled by the SOCI Act.

Providence recognises the importance of public-private partnerships in developing and implementing these critical reforms to the Australian critical infrastructure sectors. We remain committed to partnering with the Government and critical infrastructure entity owners and operators to improve risk management and protective security outcomes for a critical infrastructure asset by offering our experience as a leading expert in personnel security, international supply chain personnel security risk advice, insider threat management, security education, security governance and protective security capability development.

We respectfully offer the following submission which provides Providence's comments and observations on the draft RMP Rules.

Overview of the RMP requirements

The SOCI Act has a power to require a responsible entity for critical infrastructure assets to have, and comply with, an RMP. The RMP asks critical infrastructure entities to identify material risks that could have an impact on the critical infrastructure asset and, as far as reasonably practicable, minimise, eliminate or mitigate the risk from being realised.

To achieve effective security risk management, critical infrastructure entities are required to identify critical assets, threats, vulnerabilities, consequences and mitigations. The RMP is required to focus on the key elements of the protective security: cyber and information, physical (including natural hazards), supply chain and personnel security.

The flexibility of the RMP Rules allows critical infrastructure entities to tailor the RMP in a way that best suits their individual security goals and objectives, their specific risk, threat environment and security capability. Section 30AG of the SOCI Act provides that critical infrastructure entities will be required to provide an annual report, endorsed at board level, about their RMP performance and development to the Department.

Current threat environment

Understanding the current threat environment and specific security risks for critical infrastructure entities is one of the key elements to appropriately tailor effective protective security solutions. Threats ranging from natural hazards, such as extreme weather events, through to human

40 Macquarie Street, Barton ACT 2600 | PO Box 4490, Kingston ACT 2604 | providenceconsulting.com.au | ACN 117 321 552

induced threats including foreign interference, cyberattacks and trusted insiders, all have the potential to significantly disrupt critical infrastructure.[1]

Espionage, sabotage and foreign interference are currently the most serious security threats facing Australia.[2] In terms of scale and sophistication, espionage and foreign interference threats are outpacing terrorism threats.[3] Threat of aggregation of ownership by a single country can afford foreign powers and their proxies greater influence with which to conduct foreign interference.[4] This latter point is highly relevant to critical infrastructure.

The 2022 geostrategic shifts characterised by disrupted patterns of global trade, geopolitical tensions and growing investment in defence capabilities further roiled the global security environment[5]. The invasion of Ukraine by Russia has marked an unprecedented level of malicious cyberactivity on a global level. For example, malicious cyberactivity against Ukraine networks, including critical infrastructure, has been quite prolific.[6]

Recent cyber-attacks on Optus, Medibank Private, EnergyAustralia and other commercial entities – seemingly by cyber criminals – illustrate the complex and shifting nature of cybersecurity and threats to the operation of Australia's critical infrastructure assets.

To counter the threats to critical infrastructure an enhanced security framework is required which takes a comprehensive approach to what is regarded as critical infrastructure and the risks that need to be managed. Such an approach to security risk management acknowledges the unique context of each entity. Post-incident consequence and response management alone is inadequate to ensure the protection of Australia's critical infrastructure. Prevention and risk management is essential to make a substantial impact on the security and resilience of critical infrastructure.

Protective Security Risk Management

A genuine risk-based approach to managing protective security yields superior outcomes. Despite this approach being referred to, and required by, many government and industry standards[7] the understanding of how it works in practice remains immature and hence the full benefits of the approach are not realised.

Applying a security risk management approach seeks to determine what security practices and measures are appropriate to an organisation. Broadly, this requires an analysis of:

- what assets enable essential organisational functions and, therefore, are necessary to protect
- which threats are more (or less) likely to disrupt those essential assets

---

1 Second reading speech of the Hon Karen Andrews MP, Minister for Home Affairs, on 10 February 2022
2 Australia: Energy Sector Threat Assessment 2022
3 ASIO Annual Threat Assessment 2022
4 Australia: Energy Sector Threat Assessment 2022
5 Global megatrends impacting the way we live over coming decades, July 2022
6 Ms Abigail Bradshaw CSC, Head of the Cyber Security Centre and Deputy Director-General, Australian Signals Directorate, Proof Committee Hansard, Canberra, 16 March 2022, p. 52.
7 Including: ISO31000; HB167:2006; the Protective Security Policy Framework (PSPF)

- what are the security controls that genuinely protect against those threats present or operating suitably to achieve the desired protective effect.

The outcome of the security risk management approach is identification of security measures that are both organisation and context specific. The security risk management approach accepts the axiom that no two organisations (or their operating contexts) are the same. They are unique, they face different security threats/risks, therefore requiring different security mitigation strategies.

This is not the approach generally adopted across many government organisations and parts of industry. There has been a prevailing tendency to reduce organisational security measures and practices to 'checklists' where compliance with those measures is viewed as an indication of security maturity. This approach does not consider whether the security measure/practice is appropriate (or even necessary) to the organisation. It simply assumes that it is.

Put another way, the compliance approach ignores the context in which the desired security measure is deployed, often resulting in an investment yielding no measurable reduction in actual risk.

Too often organisations seek to comply with a set of prescriptive security measures on the belief that doing so protects them from disruption and exploitation. It is the ensuing false sense of protection that gives way to apathy often resulting in an organisation security posture incapable of quickly adapting to changes in the security environment.

Personnel security and insider threat mitigation

In this submission, Providence will focus on the personnel security aspect of the RMP as we believe that people are the most significant critical asset but may also pose the greatest security risk. Cyber security industry studies show that employees' actions lead to the majority of cybersecurity incidents, often by mistake or because employees do not have the required training and education to demonstrate how to behave appropriately for the protection the entity they work for. This type of threat is known as the 'unintentional insider' and of all insider threat types is the most straightforward to mitigate, and probably the least expensive to treat, if the appropriate mitigations are in place.

In Australia, the Protective Security Policy Framework (PSPF), administered by the Attorney-General's Department, is the primary national policy that sets personnel security standards. In addition, there are number of international and Australian standards that provide best practice guidance. Personnel security is a set of measures to manage the risk of an employee exploiting their legitimate access to an entity's critical assets (people, systems, facilities) for illicit gain or to cause harm.

There is no one-size-fits-all approach to personnel security – every organisation is unique and requires solutions tailored to its specific needs[8]. Critical infrastructure entities need to establish and implement robust personnel security frameworks to build an understanding of any insider threats facing the business and harness the tools required to manage any related risks. Such a

[8] This statement aligns to ISO31000 and HB167

framework will also enable an entity's managers to afford a level of trust in employees, contractors and suppliers so these people can be given access to the business.[9]

Workforce screening

A fundamental element in effectively mitigating the risk of trusted insider is workforce screening (background checking/vetting) – this is a core component of the personnel security framework. Workforce screening is a risk-based approach that provides an organisation with a level of initial and ongoing assurance around the eligibility and suitability of an individual (which the SOCI Act refers to as a critical worker) to access organisation assets in order to help achieve the organisation's objective.[10]

The purpose of workforce screening is to give an entity confidence in prospective employees, check their level of integrity (soundness of character and moral principle), screen and assess individuals against risk factor areas of the clearance subject's life, including personal relationships, employment history, behaviour and financial habits, all of which contributes to an assessment of a clearance subject's integrity.[11]

The workforce screening of an individual needs to establish confidence that they possess a sound and stable character, that they are not unduly vulnerable to influence or coercion, identify any security risks that individual poses to inform mitigation and monitoring strategy.

Contemporary workforce

Evolving labour markets and workforce cultures are important aspects for critical infrastructure entities to consider in establishing or reviewing personnel security frameworks.

COVID-19 has encouraged people to rethink the role of work in their lives and the value they place on flexibility and activities outside of work.[12] The onset of COVID-19 has triggered a rapid and widespread uptake of teleworking. Before COVID-19, around 25% of employees worked from home at least once per week compared to the start of 2021, where over 40% of workers regularly work remotely.[13]

The majority of Australians (72%) prefer a hybrid working model rather than working exclusively from home or in the office.[14] Hybrid work increases personnel and cyber security risks. To reduce the risks associated with working from home, businesses need to consider their security measures, ensure that staff have access to a safe and secure working environment and have been meaningfully educated about security.

These changes are occurring in the broader context of a multi-generational workforce. Different generations of workers can hold different expectations around work-life balance, technology, job

9 Managing the Insider Threat to your business, AGD, 2014
10 AS 4811 2022 Workforce Screening Standard
11 Policy 12, Protective Security Policy Framework
12 Leong L, Ross M, Tickle M (2021) Here comes the great resignation. Why millions of employees could quit their jobs post-pandemic. Sydney: ABC News (24 September 2021).
13 ABS (2021) A year of COVID-19 and Australians work from home more. Canberra, Australia: Australian Bureau of Statistics (17 March 2021).
14 Gash C (2020). Moving beyond remote: Workplace transformation in the wake of COVID-19. 7 October 2020, Slack.

security and stability, among other factors. Employers will need to be mindful of adapting their personnel security settings to these diverse and evolving employee preferences.[15]

Recruitment in the contemporary post-COVID workforce environment has become increasingly challenging and competitive. To keep pace with technological change, Australia will need around an additional 6.5 million digital workers by 2025 – an increase of 79% from 2020.[16] This means that Australian critical infrastructure companies will be competing to attract more workers from overseas, who will not be Australian citizens with checkable backgrounds. To effectively mitigate the risk of trusted insider, critical infrastructure entities will need to consider a threshold for when overseas checks are required and factored into the organisational risk assessment process and clearly define checkable background period.

AusCheck background check

The 2022 legislative amendments to the SOCI Act and the *AusCheck Act 2007* enabled an AusCheck background check as a voluntary option for critical infrastructure entities to help mitigate a risk of trusted insider. Providence notes that although the AusCheck background check addresses some of the elements required to help mitigate insider threat (such as identity verification, criminal history and national security assessment (terrorism associations)), the check offers limited value for critical infrastructure entities. The AusCheck background check is mainly fit for employees who are Australian residents or citizens with the checkable background.

Providence believes the AusCheck background check does not fully meet the intent of the RMP Rules nor the needs of critical infrastructure entities.

First, the policy behind the AusCheck background check is arguably out of date. The AusCheck background check was established following a recommendation of Sir John Wheeler's *Airport Security and Policing Review* report and as part of the Government's commitment to improve aviation and maritime security in the post 9/11 attacks environment to mitigate terrorism and criminal threats.[17]

The AusCheck background checking policy set between 2004-2006 to address threats in the aviation and maritime transport sectors has not been substantially reviewed. There is no evidence to suggest that it is fit for purpose to address threats and security risks that 11 critical infrastructure sectors face in 2022, noting threats are much broader than terrorism and criminality of 20 years ago. To be able to effectively mitigate the risk of trusted insider the policy behind the AusCheck background check would benefit from the substantial review in light of the current threat environment.

Second, any outsourced checking, whether it is the AusCheck background check, Commonwealth vetting or a background checking conducted by a private company, does not properly equip critical infrastructure entities to understand the threat environment, existing

[15] Hamer B. Why attracting and retaining the top Millennial talent is key to future success (cited 12 November 2021). Available from: https://www.pwc.com.au/digitalpulse/millennials-five-generations-workplace.html.
[16] AlphaBeta (2021) Unlocking APAC's digital potential: Changing digital skill needs and policy approaches. Singapore: AlphaBeta commissioned by Amazon Web Services.
[17] An Independent Review of Airport Security and. Policing for the. Government of Australia by. The Rt Hon Sir John Wheeler DL

personnel security risks of individuals and hence to effectively manage personnel security in their organisations. Outsourced checks are a 'moment-in-time' check and do not offer ongoing suitability and continuous assessment capability.

A background check is one element of a comprehensive approach to the challenge of SOCI personnel security. To have the most impact – to be a foundation stone in personnel security mitigation - a background check can be coupled to a comprehensive personnel security framework.

Providence Workforce Security Risk Methodology

Providence has developed a Workforce Security Risk Methodology that may assist SOCI entities achieving security outcomes sought through the RMP Rules. Our approach is tailored to non-government entities and non-citizens for which Commonwealth vetting is not an available mitigation – this is the SOCI entities' workforce.

The Workforce Security Risk Methodology enables:

- establishment of in-house ownership of personnel security risks, mitigation and controls preserving trust of your employees and consistent with privacy obligations
- shared responsibility for personnel security within your company
- help for your business to effectively manage insider risk and establish early detection capability
- management of the lifecycle of your employees, including continuous suitability monitoring, based on the risk profile of your company and individual risk profiles
- conduct of tailored individual and personality assessments for employees in critical roles
- conduct of background check for employees from overseas
- bolstered wellbeing, employee performance, staff retention and diversity
- post-employment conditions that protect an entities IP and operational security.

These features are elements of a contextualised security risk management framework designed to safeguard assets and operations of SOCI entities. A key feature of the Workforce Security Risk Methodology is mitigation of the insider threat.

Using this approach would enable risk-based consideration of the suitability of a candidate. For example, a background check might return advice on a conviction. The Providence approach would see that piece of information taken into context with respect to the potential value of the candidate joining a SOCI entity: how long ago was the conviction, what were the circumstances, is the offence committed relevant to the type of employment anticipated for the SOCI entity? The Workforce Security Risk Methodology offers the capability to make such assessments to both capture and retain highly skilled and valuable employees and contractors.

Insider Threat

Providence's team has developed Insider Threat expertise based on leading academic and practitioner study and advice. Further, Insider Threat is where Providence's select partners come to the fore. Providence has teamed with DTEX, a company renowned internationally for its Insider Threat capability, to provide highly effective options for continuous assessment of critical infrastructure workforces. DTEX has a mature relationship with the US company MITRE, which

has an impressive record of critical infrastructure protection in the United States, and which is commencing operations in Australia. Providence is also partnering with another Australian company with the capability to conduct open-source searches to gain insight into the activities of critical workers as these activities might be relevant to the security of the critical infrastructure entity.

Providence's approach to security risk assessment, contextualised protective security risk management frameworks, personnel security, workforce assurance, background checking, insider threat detection and ability to bring significant partners capability represents a sophisticated capability that can enable the RMP outcomes that will underpin the operational success of the SOCI Act and deliver the desired outcome of enhancing the security and operations of Australia's critical infrastructure.

Our approach enables the identification of aberrant behaviours that may indicate insider threat activity – be that intentional or unintentional – so that the organisation can best understand the behaviour in the context of the individual and determine the best path of engagement with the person to remediate behaviours, support the wellbeing of the person and bolster the operating and security cultures of the organisation. The approach is configured to reach an outcome positive for both the employee and the organisation, except in the instance where a person is a malicious insider. In that situation our approach identifies and remediates the insider threat for the benefit of the critical infrastructure, the entity and the workforce.

Conclusion

Providence commends the Commonwealth Government on its continuing engagement with industry to refine Australia's ongoing critical infrastructure reforms. Providence appreciates the Government's review of this submission and welcomes further opportunities to contribute our substantial experience as a leading protective security adviser and to help bridge the theoretical-practical gap in RMP operationalisation.

Providence is supportive of background checking as part of the RMP, recognising that type of mitigation as an important element of a more comprehensive and dynamic approach to personnel security. However, not all background checks are of equal merit. The RMP allows critical infrastructure entities flexibility to choose a background check – they are not obliged to use AusCheck – and Providence recommends critical infrastructure entities search for a background checking solutions that best meet their business needs.

Providence is well positioned to contribute meaningfully to future discussions, particularly those concerning personnel security, insider threat management and the personnel security aspects of supply chain. Providence is committed to being a productive security partner of the Government, SOCI entities and the Australian people.