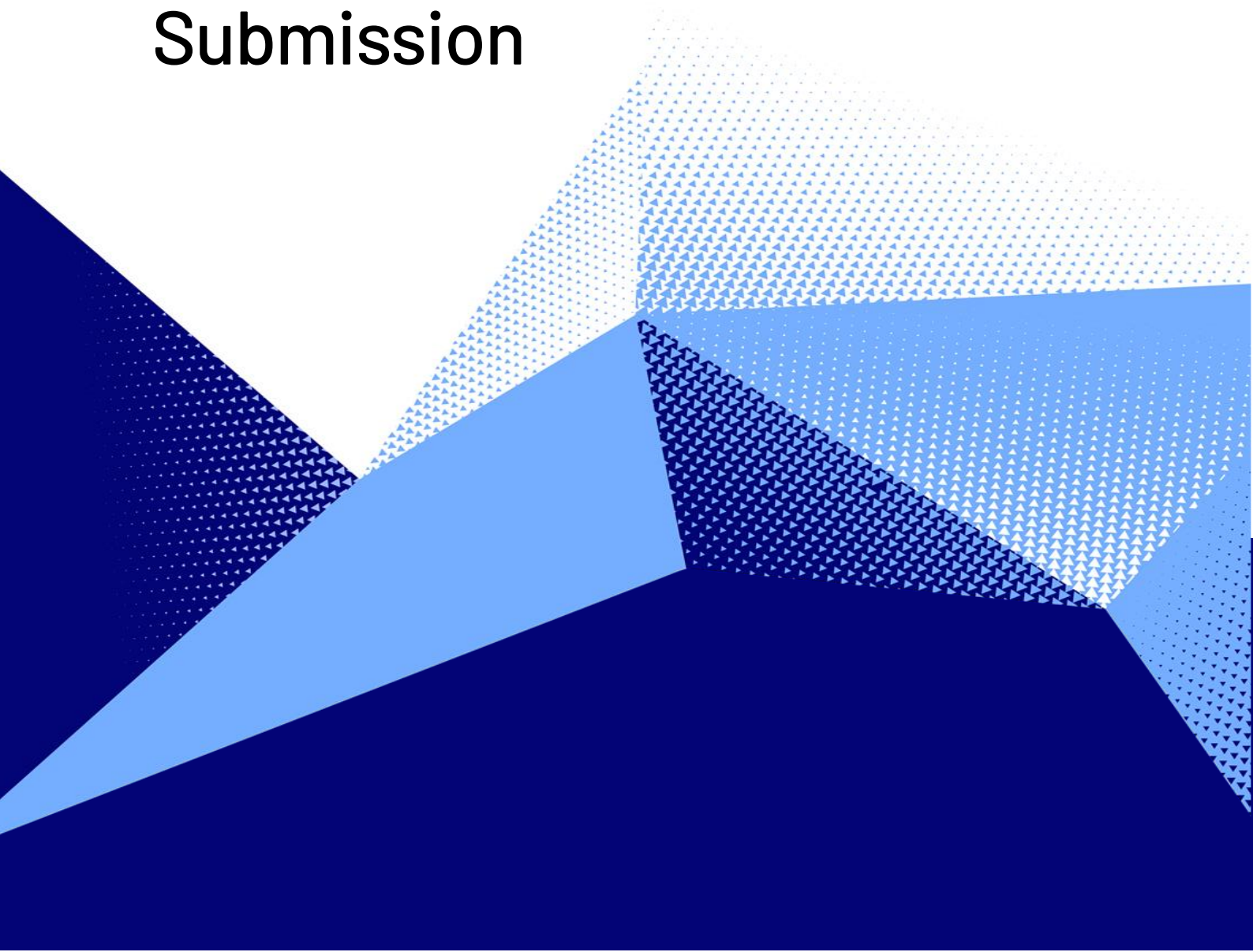
CyberCX

Protecting Critical Infrastructure and Systems of National Significance Submission



1 Introduction

CyberCX, as Australia's largest cyber security professional services company, welcomes the opportunity to provide a submission in response to the Australian Government's *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* (consultation paper).

This submission comprises our views and recommendations, but these are shaped by our engagement with our clients, including 30 of Australia's leading, listed companies.

The consultation paper, read alongside the *Cyber Security Strategy 2020*, highlights that there are few issues as vital to Australia's safety and prosperity as cyber security.

In critical infrastructure sectors, the cyber security challenge is acute and the consequence of failure debilitating. Australians therefore expect critical infrastructure providers to manage data and systems with technology that is secure, available, and reliable.

Malicious actors - whether nation states or criminals - have demonstrated their willingness and capability to breach Australian critical infrastructure through cyber security vulnerabilities. Whether these attacks are targeted or indiscriminate, the net result is the same: enormous impact across vital, connected systems.[1]

We believe this targeting, alongside our level of connectivity and interdependence, means the current legislated definition of critical infrastructure is too narrow.

Across our critical systems, there are too many competing priorities, regulatory uncertainties, and insufficient capability from Government, industry and professional services to combat cyber threats. This means that too frequently, businesses only seriously consider cyber security *after* an incident has occurred.

For these reasons, CyberCX supports the Government's plans to reform Australia's cyber security regulatory landscape, both as it relates to critical infrastructure and the economy more broadly.[2]

However, the wide-ranging proposals need further detail and consideration. Imposing new obligations across the economy and significantly expanding the power and responsibilities of the Government, particularly the Australian Signals Directorate (ASD), deserves an extended consultation.

---

[1] For example, the 2017 NotPetya attack effected a number of high profile Western critical infrastructure assets including energy companies, power grids, airports and banks. The estimated financial impact was over USD$10 billion.

[2] In the *2020 Cyber Security Strategy* the Government indicated it will consider legislative changes that set a minimum cyber security baseline across the economy. This will include multiple reform options, including: the role of privacy, consumer and data protection laws; duties for company directors and other business entities; obligations on manufacturers of internet connected devices.

© CyberCX 2020

CyberCX can appreciate the Government's urgency to legislate. But we believe there is merit in undertaking further engagement prior to enacting legislation, to enhance Government's visibility of critical infrastructure and its understanding of assistance during an incident. A more detailed discussion is required to prevent potentially conflicting outcomes from the legislation, in particular:

- regulatory duplication;
- technical barriers;
- risks associated with ASD intervention, and direct action;
- impacts to data confidentiality, integrity and availability; and
- clarity around compliance and obligations for critical infrastructure sectors.

The consultation paper notes the Government intends to design the new legislation around a principles-based framework based on a practical risk assessment of specific critical infrastructure sectors. We support this. In addition, legislation and regulation should be phased and apply only once the relevant sector has clarity on compliance obligations. It should increase Government's capacity to assist critical infrastructure entities practicably, and ensure it is not increasing their reliance in place of building native capability.

This submission examines the Government's proposed critical infrastructure changes in three key areas:

- The case for greater regulation;
- Issues, concerns and challenges with the regulatory reforms; and
- Our recommendations.

1.1 About CyberCX

CyberCX is the largest sovereign cyber security company in Australia, with over 500 professional staff nationwide.

It comprises several specialist cyber security practices that provide comprehensive end-to-end services to both Government and private enterprise clients.

CyberCX's attributes reflect who we are and how we work:

- **Relentlessly Cyber** – We are cyber security experts first and foremost. Our only focus is managing our client's cyber risk and reputation.
- **Client Obsessed** - Global threats solved locally. We intimately understand our clients and the risks they face.
- **Unified Expertise** - Our people are the most skilled, certified, and highly qualified. Together on a single mission*: to protect and defend Australian organisations from cyber threats.*

2 The need for greater cyber security regulation

Ideally, market factors drive the adoption of new security practices. However, where the market fails, or where change is too slow, there is a role for Government to propose and enact obligations to protect the safety and prosperity of organisations and individuals.

In the physical world, the introduction of vehicle safety standards or occupational health & safety laws, are well-established examples of regulation for positive impact. Likewise, cyber security risk to Australia has reached this point: we believe more interventionist Government action is required.

The *SOCI Act* established a foundation to improve the resilience of our most vital critical infrastructure entities. Whilst ambitious and necessary, it is not sufficient to regulate the diverse and connected nature of Australia's critical systems, and does not go far enough to mitigate cyber security risk. It is for these reasons that CyberCX supports the changes proposed under the *Enhanced Critical Infrastructure and Systems of National Significance* regulatory regime. CyberCX agrees with the Government that the legislative and regulatory reforms:

- Need to be **principles based** - compliance itself does not create security. Having a mature understanding of risk and mitigation, and the wherewithal to respond does.
- Need to be **proportionate and reasonable** - there is no point in a framework that either cannot be implemented, or which results in companies becoming unprofitable or unworkable. Risk, especially cyber security risk, can never be eliminated. Therefore, it is about doing what is reasonable.
- Should take a **proactive** approach to encouraging cyber mitigations.
- Should start by clarifying and setting **roles, responsibilities** and – importantly - **expectations**; and that Government should use its unique sovereign capabilities to help address serious cyber threats to Australia.

While organisations cannot stop every cyber incident from occurring, they need to attempt to reduce the likelihood and ensure they remain resilient. Resilience for CyberCX means being able to **detect risk being realised, act quickly to counter its threats and vulnerabilities, remediate harm, and re-commence operations**. This expectation is not only achievable, it is good business.

3 Clarity and certainty: establishing the way forward

The consultation paper serves as a useful first step in establishing a cyber security regulatory baseline – and acts as a significant market signal for action - for critical infrastructure owners and operators. However, success will depend on greater clarity of key elements of the proposed reforms. Government needs to avoid unintended consequences. And critical infrastructure owners and operators need certainty to plan long-term system and network upgrades, as well as have a clear understanding of how they will interact with the Government, particularly ASD.

© CyberCX 2020

A cyber security uplift across industry will require sustained investment over an extended period to ensure continuity in services and avoid the imposition of prohibitive costs on network owners. With many critical infrastructure providers operating on slim margins, and with requirements to plan expenditure well in advance, operators need additional clarity to make informed investment decisions. Failure to do this will potentially reduce the effectiveness of the reform. Further public consultation once the framework is more developed is therefore required to enable meaningful engagements regarding the implications for industry.

4 Issues, concerns and challenges

In the absence of further detail, CyberCX has identified six high-level concerns with the consultation paper's proposed reforms.

4.1 Government Assistance (Directions and Direct Action)

CyberCX supports the Government having the capability and capacity to provide assistance to critical infrastructure entities where requested.

Where critical infrastructure providers are unwilling to cooperate with Government in the event of a serious cyber security incident, CyberCX further supports Government having the power to compel a reasonable action or inaction. Currently, the Government does not have near real-time powers to compel such actions, and system owners and operators can largely ignore requests from Government. Additionally, current *SOCI Act* Ministerial Directions are "slow time", requiring extensive attempts to work cooperatively before the Minister may consider a Direction. CyberCX believes any such new power to compel an action or inaction should only be issued by the Minister or a member of the judiciary in a similar way to that law-enforcement warrants are issued, but there needs to be a more flexible way for Government to direct entities to take action in the national interest. CyberCX further supports the use of 'safe harbour' legal protections for owners and operators compelled to take certain actions or inaction at the direction of Government.

CyberCX has reservations about the introduction of a new power allowing Government to step in and directly take control of a critical infrastructure provider's systems or networks. This power should lie with those best placed to respond in a critical cyber incident. In almost all instances it is those who manage the critical systems (i.e. the critical infrastructure company or its service provider) who are best placed to take effective action while minimising harmful consequences. The transfer of this power to Government has the potential to result in significant unintended consequences and transfers responsibility in a way that oversteps the reasonable role of Government. The establishment of a direct-action power may also result in some owners and operators failing to invest sufficiently in their own capabilities based on the belief that Government will come to the rescue.

© CyberCX 2020

4.2 Definitional uncertainty

We note the consultation paper includes discussion of an 'imminent cyber threat or incident' or 'immediate and serious cyber threat'. There need to be clear, measurable, definitions of what these 'immediate' and/or 'serious' scenarios look like and how the Government would practically engage with the critical infrastructure system in such an event. For example, it is unclear how the proposed legislation would engage with a server being used as a relay point for an attacker. We consider that, at a minimum, this threshold should compare to the threshold that is used to define a terrorist act. For example, for ASD to intervene on a critical infrastructure network it must reasonably suspect that a cyber security incident is likely to cause one or more of the following:

- death, serious harm or danger to a person;
- serious damage to property;
- a serious risk to the health or safety of the public; or
- serious interference with, disruption to, or destruction of critical infrastructure.

CyberCX agrees with the proposed sectors for inclusion in the expanded critical infrastructure definitions. However, Government needs to provide entities with certainty of legislative obligations and enough flexibility to ensure it remains relevant as threats, entities, technologies and society evolve.

It is unclear how exactly the legislation would define critical infrastructure operators. These uncertainties are compounded by the lack of baseline technical standards in the cyber goods and services that operators rely upon to build and run their networks, especially with respect to Operational Technology.

It is also uncertain as to how a regulator would assess a 'reasonable' level of cyber security in the implementation of a principles-based regulatory framework. If this is to be determined by market conditions and practices, Government must set clear expectations for how standards would rise.

In many cases, even with extensive resources directed at enhancing cyber resilience, a true increase in cyber security maturity might take years to be realised. Industry therefore needs to know how regulation would be implemented over time to understand the implications for their specific businesses and to budget for the increased regulatory costs.

The sector-specific regulatory reforms deserve a measured and collaborative consultation.

4.3 Regulatory overlap and complexity

A further complicating factor is the treatment of large enterprises and the inter-relationship of the proposed reforms with existing regulatory frameworks. While noted in the consultation paper, CyberCX considers that public mapping and harmonisation with existing regulation (and among potential cyber regulators) is essential.

For example, there are significant security requirements enshrined in telecommunications legislation under the TSSR, which were developed through collaboration between industry and Government, and have been operating for the past two years. There are also a range of other telecommunications sector specific legislative instruments and regulation that are relevant to security and an "all hazards" approach in the sector.

There should be careful analysis of the competitive, commercial, economic and social impacts of the significant changes proposed, especially if increased regulatory obligations fetter Australian companies when competing both locally and globally.

4.4 Tier Design

There is a need for greater clarity on how Government will categorise critical infrastructure operators and entities, and how they might move between regulatory tiers over time. The Government should consider developing a framework whereby membership of a specific tier within the regime is based on criticality, vulnerability, size, reach or impact rather than necessarily membership of, or relationship to, a specific sector. This framework should be measurable, transparent and objective, enabling entities to assess and understand where they are likely to sit (both now and over time) and therefore their likely level of impact. Such a framework would also ideally enable consideration of whether an entire entity or just elements of their business would be designated under the *SOCI Act*.

This holds true for entities we would expect to be owners and operators of systems of national significance. The entities that attract this designation should be able to vary over time based on the thresholds set by Government and their operating conditions.

This approach would allow the most critical components of a business to be designated a system of national significance. For example a single part of operational technology that controls power for a region or the SWIFT payment mechanism as opposed to an entire bank, or – more broadly – every bank, while other parts of the banking system, and banks themselves, would be lower in the critical infrastructure tiers holistically.

In determining criticality, the Government could consider a categorised approach with classifications such as risk to life, risk to economy, or risk to national defence, with their level of significance dictated by how quickly their disruption could gravely damage any of the three categories (hereinafter '*risk consequence*'). In addition to interdependency with other functions and consequence of compromise the Government could also consider including the attractiveness of target or the threat landscape (hereinafter '*risk likelihood*'). Furthermore, there may be value in empowering Government to designate entities based on repeated failures or compromises. We consider this would be less relevant in determining whether an entity is included under the proposed *SOCI Act* expansion, and more relevant in determining the level of obligation imposed on them under the legislation.

In this way electricity, SWIFT and vital parts of defence industry might be designated systems of national significance, while education and space would be deemed less critical.

4.5 Timing

CyberCX has significant concerns with the Government's proposed legislative timeline for changes to *the SOCI Act* and subsequent sector-by-sector regulatory reform.

The current *SOCI Act* includes powers that could drastically increase Government's visibility and understanding of the complexities of critical infrastructure entities, their associated cyber security maturity and risk profile. CyberCX therefore supports the Government introducing legislation to include additional critical infrastructure sectors in the existing *SOCI Act* regime this year, with the current *SOCI Act* obligations to apply to these entities.

To mitigate the most serious incidents, CyberCX further supports Government introducing legislation this year that would provide Government with the power to compel an entity to take an action or inaction.

However, the applicability of the regime and the practical consequences of the new 'positive security obligations' and 'enhanced cyber security obligations' have not been sufficiently articulated or explored. CyberCX therefore considers that these additional obligations should not be legislated until Government has undertaken further discovery – by using the information gathering powers of the *SOCI Act* - regarding current sector-specific cyber security maturity.

This discovery would enable Government to design the new legislation, proposed tier memberships and additional specific obligations around a principles-based framework based on a practical, evidence-based risk assessment of critical infrastructure sectors. The legislation and regulation should then be phased and apply only once the relevant sector has clarity and an opportunity to respond to proposed compliance obligations.

4.6 Implementation

The consultation paper indicates a broadening of ASD's remit by introducing powers to protect critical infrastructure onshore. The paper suggests that ASD, with agreed consent under *SOCI Act* amendments, would be permitted to 'sit inside' private sector organisations to detect and defend against 'critical cyber threats'. Such activity would represent a notable departure from ASD's existing remit. Government and industry must closely consider the practical consequences and privacy implications of such activity with strict definitions and proportional controls. Further public consultation is therefore needed to define and discuss the extent of these changes.

Furthermore, where Government is required to monitor systems to enable defence, that telemetry should be provided to the businesses to enable them to enhance their own maturity and build capability in the sector. This must also be segregated from other collection functions of Government.

© CyberCX 2020

A key consideration in defining when, and if, Government would intervene is Government's current capacity. If ASD and the ACSC do not currently have the resources to protect or manage a critical cyber incident of the nature described, it might be considered overreaching to legislate for a power that it cannot execute. Moreover, it might give critical systems owners and operators, and the broader public, a false sense of security of Government's abilities, and lead to reduced private sector investment in cyber security.

5 Recommendations:

CyberCX recommends the following:

1. **Consider** removing the power for Government to take direct action in an emergency, with this power to remain vested in owners and operators of critical infrastructure entities and supported by robust powers for Government to compel action or inaction.
2. **Provide** clear, measurable definitions of what 'immediate' and 'serious' scenarios look like and how Government would practically engage with the critical infrastructure system in such an event.
3. **Develop** a measurable, transparent and objective framework whereby membership of specific tiers is included based on criticality, vulnerability, size, reach or impact. This should consider a categorised approach based on *risk likelihood* and *risk consequence*.
4. **Phase** implementation of legislation to expand its application and introduce the power for Government to compel an action or inaction, with additional amendments to follow a period of discovery and consultation using the existing powers legislated under the *SOCI Act*.
5. **Undertake** further detailed consultation regarding the practical consequences and privacy implications of ASD expanding its mandate to include the ability to 'sit inside' critical infrastructure networks.
6. **Align** increases in industry's cyber security obligations with growth in Government's capacity to assist critical infrastructure, and ensure this growth in capacity does not increase industry's reliance on Government.
7. **Provide** telemetry collected to monitor systems to businesses to enhance their own maturity and build capability in the sector, and ensure this data is segregated from other collection functions of Government.

6 Conclusion

The proposed reforms to critical infrastructure legislation represent a positive and necessary change to the way cyber security of critical infrastructure is managed in Australia. Successful, measured implementation has the potential to not only save businesses money and reputational damage, but also make Australia less attractive to those who wish us harm.

© CyberCX 2020

However, these positives are not absolute. The change that accompanies the proposed legislation is immense, industry needs sufficient time and information to understand how they would be impacted and provide advice to Government. No one is better placed to understand the complexity of these changes than the businesses themselves and implementing this legislation without sufficient consultation and reasonable pace has the potential to do more harm than good.

There is also a need for further discussion regarding the role of ASD on private networks. Government should have the power to compel critical infrastructure providers to protect Australians when our collective security is at risk. But this must not be at the expense of allowing those who are best placed to respond to do their jobs. Government clearly signalled in the *Cyber Security Strategy 2020* that industry needs to play its part in better securing the nation from cyber security threats. Any action taken as part of this legislation needs to support that idea, not increase reliance on Government resources or create promises that cannot be kept.

CyberCX Pty Ltd
Level 27, 101 Collins Street
Melbourne, VIC 3000, Australia

ABN: 90 629 363 328

T: 1300 031 274

info@cybercx.com.au
www.cybercx.com.au

© CyberCX 2020