ABSIA Australian Business Software Industry Association

217 Flinders Street
Adelaide SA 5000
info@absia.asn.au | www.absia.asn.au

16 September 2020

The Department of Home Affairs &
Critical Infrastructure Centre

Via submission form.

To whom it may concern,

Re: ABSIA's Response to Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of our members and the software industry. This submission has been prepared with input from members, our government relations sub-committee and board members.

With the possibility of payroll, superannuation and e-Invoicing networks being classified as critical infrastructure, there are potential impacts to ABSIA members who include Digital Service Providers (DSPs) and Sending Service Providers (SSPs) as well as superannuation and payroll software providers across the digital service provider industry.

ABSIA welcomes the Department of Home Affairs approach to building upon rather than recreating existing frameworks. ABSIA sees this initiative as an expansion and maturation of the need to protect critical infrastructure, which in turn protects Australian citizens. The continued increase in digital expansion and cyber activities, suggests that expanding frameworks will help strengthen capabilities as opposed to implementing new and, at times, conflicting sets of rules.

In summary, our submission has made the following points:

- Payroll, superannuation and e-Invoicing networks should be classified as regulated critical infrastructure;
- The current definition of critical infrastructure is too broad and need to be more focused;
- Existing security standards such as the ATO's DSP Operational Framework and the Security Standard for Add-on Marketplaces (SSAM) currently satisfy the PSO meaning there is no need for additional regulatory frameworks for these entities;
- The preferred regulator for payroll / Single Touch Payroll (STP) may not be the owner and operator, in this instance, the ATO. We suggest an association like ABSIA instead;
- We see the main benefits as threat intelligence sharing, access to expertise and assistance if our members are subject to an attack. However, for all participants, more information is needed about the expected benefits for them;

- To support what is currently outlined in the legislation, detailed scenarios are needed for when the government can get involved in immediate and serious threats; and
- Overall, we support the government's increased involvement in the security of critical infrastructure and the support they can provide to industry participants and stakeholders.

ABSIA would appreciate the opportunity to engage further on these issues. For further information about this submission, please contact Maggie Leese, ABSIA Marketing & Membership, on maggie@absia.asn.au.

Your faithfully,

Chris Howard,
President & Director, ABSIA.

ABSIA's Response to Protecting Critical Infrastructure and Systems of National Significance Consultation Paper

1. Do the sectors capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms?

Yes, we believe that the sectors outlined in the discussion paper capture the functions that are currently vital to Australia's economy, security and sovereignty. There are no further sectors that we can suggest at this time. However, this list should be re-examined every few years to ensure that emerging or newly identified critical infrastructure is included.

While the vital sectors are covered, there are also the systems that operate across sectors that should be considered as critical infrastructure. These systems include payroll, superannuation, and e-invoicing (including Peppol and legacy EDI networks).

2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

We believe that the current definition of critical infrastructure is too broad and needs to be more focused. With the expansion of the definition to incorporate further "critical infrastructure", ABSIA recommends the creation of more precise definitions of what critical infrastructure is. This activity will help the industry to have a more clear understanding of those assets that require greater focus and protection. This, in turn, will lead to future initiatives that will help mature and protect these critical assets.

4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?

ABSIA would like to put forward the following threats that may impede our members and the wider industry:

- Reliance on Australia's data network and telecommunications links; payroll, superannuation, banking and financial organisations all have a significant reliance on Australia's data and telecommunications networks.
- Cyber activity from malicious actors; ABSIA recognises that cyberattacks are increasing at a rapid pace. Sadly, cybercriminals are innovating as fast or faster than government regulation and industry development. The need for industry wide frameworks will continue to be required as Australia pursues a digital agenda.
- Systems reliability and availability, including disaster recovery and business continuity needs; as more critical infrastructure is digitised, there will be further need for these systems to have adequate protection and recovery capabilities to help foster trust and confidence.

5. How should criticality be assessed to ensure the most important entities are covered by the framework?
Criticality should encompass much of what is included in the definition of critical infrastructure. If such entities were to be destroyed, degraded or rendered unavailable for a period of time, it would impact providers of those entities, businesses and individuals in Australia.

From our point of view, if the STN or STP were to be impacted on, either by a direct interruption or one to a certain provider, for a significant amount of time, many Australians would likely not be able to get paid or pay their own employees. The outcome of such a situation would have a significant impact on the economy, could lead to claims, litigation and, potentially, unnecessary impacts to Australian's confidence in their employers, banks and financial institutions.

6. Which entities would you expect to be owners and operators of systems of national significance?
In our experience, the owners and operators of critical infrastructure are the industry participants. Individually, they provide a piece of the puzzle that helps our economy move. However, with increased digitisation, the introduction of single touch payroll (STP), increased governance on superannuation and the introduction of e-invoicing, these operators will become increasingly important in protecting the reliability, security and support of these systems. This may also be true for those systems classified as systems of national significance.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?
Please refer to our answer to question 19.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?
ABSIA believes the principles based outcomes consider all aspects of security, however, the broadness of these may lead to assumptions that are not in line with desired outcomes. The Department of Home Affairs should provide more precise definitions of support statements for these principles that will offer industry stakeholders the opportunity to better understand the principles and to take any necessary steps to embrace or adopt the same.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?
While we believe that the security obligations are broad and provide a balance, the Department of Home Affairs should avoid using vague language in the final version of the PSO considering that there will be legal obligations on owners and operators of critical infrastructure. Detailed information should be provided about each obligation to avoid different interpretations and therefore applications.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Industry members are generally operating in line with current frameworks, such as the Australian Tax Office's DSP Operational Framework[1] and SSAM[2] (discussed in more detail below). More precise classifications of "critical infrastructure" will assist industry members to understand their obligations in aligning with these principles. ABSIA recommends the creation of more precise definitions of critical infrastructure and the reuse of the Operational Framework and SSAM to reduce costs, complexity and confusion to industry participants.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

ABSIA welcomes the Department of Home Affairs' approach to building upon and not recreating existing frameworks. Taking this into consideration, many ABSIA members and other DSPs and super gateways are already meeting security standards such as the DSP Operational Framework, the SSAM as well as other local and international standards that currently satisfy these principles. At this point in time, there is no need for additional regulatory frameworks for the payroll and superannuation industries.

The cost of the Operational Framework and other compliance work is an issue for many in the industry[3]. Several millions of dollars of investment have already been made to support the first version of the Operational Framework and as the framework changes to reflect threats in the industry, more investment will be required from DSPs.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

In its current form, the proposed regulatory model seems to avoid duplication with existing oversight requirements. However, we would assume that as this legislative framework comes into play, this model may be refined to better work with existing oversight requirements in certain sectors.

[1] https://softwaredevelopers.ato.gov.au/operational_framework
[2] https://www.absia.asn.au/industry-standards/addon-security-standard/
[3] Concerns around compliance work are addressed throughout ABSIA's Business Software Industry COVID-19 Impacts Report released July 2020

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?
With incident reporting, would entities need to report to their usual regulator and this will then be sent through to the relevant government body or would entities need to report both separately? The first option, to avoid double reporting from entities, would be a favoured option. Similarly, with compliance reporting for those sectors that already have a defined regulator in place, will they continue to report as normal or will these procedures change?

With the potential for slightly new procedures for those now being defined as critical infrastructure, will there be a documented approach about non-compliance and what the penalties will be? Furthermore, how long will it be before those take effect?

17. Who would you consider is the best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?
Of the sectors and entities that ABSIA is familiar with, the respective owners and operators of each entity are currently:

- Payroll / Single Touch Payroll - ATO
- Superannuation Transaction Network - Gateway Network Governance Body (GNGB)[4]
- E-invoicing - Peppol[5] (whole of network), ATO (Australian network)
- EDI - no independent regulator

While the ATO are considered to be the operators of payroll, including STP, systems, when it comes to a designated regulator, we would suggest that an association or body such as ABSIA should take up this role. ABSIA is independent and represents the needs, wants and voices of DSPs. Utilising an independent organisation offers the Department of Home Affairs the opportunity to expand its reach and contact with industry participants as well as ensuring that the principles are being maintained as an independent and impartial set of principles.

The EDI network is currently lacking an independent regulator. With our suggestion above, perhaps an association or body needs to be created to provide oversight. However, as e-invoicing starts to gain momentum and address some of the limitations of EDI, it will rapidly become a critical network much like the STN and STP networks. There may be an overlap here in determining the regulator of both these networks.

ABSIA would welcome the opportunity to take part in the mapping of regulated critical infrastructure entities to provide insight into the above networks as most of our members are involved in one or more of these areas.

[4] https://www.gngb.com.au/
[5] https://peppol.eu/

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?
In some circumstances, financial support would be beneficial for regulators to ensure they have the appropriate resources to undertake this regulation. With increased oversight and the need for industry support, investments would offer the industry the opportunity to adopt, mature and improve the principles and outcomes related to their specific responsibilities.

19. How can Government better support critical infrastructure entities in managing their security risks?
Where possible, access to government technology, such as myGovID, would be beneficial so that entities can leverage existing technology and lessen their costs in meeting security requirements.

If an attack were to occur within a sector that is relevant to ABSIA, we would appreciate assistance to help provide education and resources to our members to address any vulnerabilities that may exist. Similarly, ABSIA would also appreciate access to expertise and threat intelligence sharing so that we can share this with our members.

Finally, funding could be considered for critical infrastructure entities where additional work is required to meet the PSO, especially for those that will be new to this kind of regulation.

20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?
ABSIA suggests that security assessments may be incorporated into existing frameworks, such as the Operational Framework and the SSAM thereby allowing for the increased oversight, while not overlaying significant burden on the industry for further assessments.

23. What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?
Essentially, ABSIA would like to see greater threat intelligence sharing with the industry alongside other security information sharing. ABSIA would appreciate the opportunity to be privy to such information so we can share this with our community. We do recognise the sensitivity of such information, but can also see that sharing with trusted industry participants will help improve industry readiness and responsiveness to such events.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?
ABSIA could provide information about the SSAM and common threats that are encountered here. We could also potentially provide information passed on from our members as needed. ABSIA are additionally an independent organisation who represent the industry and act as a bridge between industry and government agencies. We often share information between the industry and government to improve outcomes for the Australian digital economy.

Within the industry, we anticipate that payroll, superannuation and EDI / e-Invoicing entities would be happy to voluntarily share information about their systems. Many DSPs and SSPs would be used to some level of information sharing through the requirements of the Operational Framework.

28. What safeguards or assurances would you expect to see for information provided to government?
As such information will often be shared voluntarily, the industry would expect a relatively high level of protection for this information.

29. In what extreme situations should government be able to take direct action in the national interest? What actions should be permissible?
While the legislation is reasonably clear about when the government can get involved, the industry needs detailed scenarios to better understand how and where this could happen.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for government?
Throughout the discussion paper, the roles and responsibilities for both the government and industry have been adequately outlined. We welcome the increased participation of the government in protecting critical infrastructure and look forward to their continued support of the industry here.

Overall there needs to be more information about the benefits for owners, operators and entities. This would include information about the support they would receive under these changes and if there will be any financial assistance offered.