Head Office, Building 1
11 Sir Donald Bradman Drive
Keswick Terminal
Adelaide, South Australia 5000

26 February 2023

Submission in response to the Commonwealth Government's Cyber Security Strategy Reforms

Introduction

The Australian Rail Track Corporation (ARTC) welcomes the opportunity to provide feedback to the Commonwealth Government on the 2023-2030 Australian Cyber Security Strategy and associated 2023-2030 Australian Cyber Security Action Plan.

Cyber security is an important issue and it is important that appropriate processes and governance arrangements are put in place to protect all Australians, essential infrastructure and the broader supply chain.

ARTC is proud of the vital role we play in Australia's transport supply chain and in the economic development of the nation. As one of the country's largest Rail Infrastructure Managers, ARTC maintains and operates 8,500km of the national rail network across five states, managing the transit of around 450 trains per day across New South Wales, Victoria, Queensland, South Australia and Western Australia.

We employ more than 2,000 people and continue to invest in Australia's future prosperity and growth through the delivery of transport infrastructure projects which enhance the safety, reliability and efficiency of our rail network.

Each day our network transports intermodal containers, agricultural products, general freight and passenger services, as well as hundreds of thousands of tonnes of coal and minerals. We efficiently get freight off roads and reduce congestion, which improves our environment and increases the safety of motorists and local communities.

We continue to meet the changing needs of our customers and are committed to the health and safety of our people, the environment and the local communities in which we operate.

Feedback – Consultation Paper

Below are suggestions ARTC would like to put forward as opportunities to strengthen the proposed Cyber Security Strategy Reforms, as well as a summary of all recommendations.

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

In line with the overarching goal of securing IoT devices, ARTC suggests the inclusion of a specific emphasis on ensuring that security settings and configurations are enabled by default. Implementing a secure-by-default approach is crucial in mitigating potential vulnerabilities and reducing the risk of cyber incidents.

By mandating that security features are activated upon device deployment, users can benefit from a heightened level of protection without the need for manual intervention. This not only enhances the overall security posture of IoT ecosystems but also contributes to a more user-friendly experience, as end-users can have confidence in the out-of-the-box security of their devices.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

No suggested feedback.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate

ARTC suggests that careful consideration is given to defining the boundaries between industry stewardship and regulatory compliance activities. In order to maintain a robust regulatory framework and encourage engagement during cyber incidents, it is essential that regulatory agencies have the ability to contact organisations directly and use their powers when needed.

ARTC suggests the following to be included in the 'prescribed security purposes' for a limited use obligation on cyber incident information shared with ASD and Cyber Coordinator:

- Consequence management - further clarification on what specific actions or measures are encompassed within this function. Clearly defining the scope of consequence management would provide a more precise understanding for stakeholders;
- Specificity in "Improving Incident Response Mechanisms" - specifying how the improvement process will be undertaken. This could include considerations for standardisation, interoperability, and lessons learned from previous incidents; and
- Operationalisation of "Stewardship and Advice to Industry - include the mechanisms for advice dissemination, the involvement of industry stakeholders, and the practical implementation of best practice recommendations.

Additionally, the following restrictions / considerations should be applied to the sharing of cyber incident information:

- Privacy - any shared information is appropriately anonymised or stripped of personally identifiable information to protect individual privacy rights;
- Business Confidentiality - clear guidelines on what types of information can be shared without compromising the competitive advantage or proprietary nature of businesses;
- National Security Interests - mechanisms to prevent the unintentional sharing of information that could be exploited by adversaries;
- Legal and Regulatory Compliance - ensure that the sharing of information complies with relevant laws, including data protection and privacy regulations;
- Informed Consent - ensures that entities are aware of and agree to the sharing of their data;
- Third-Party Access Restrictions - restrict access to shared information to authorised entities and establish protocols to prevent unauthorised third-party access; and
- Strategic Information Classification - implement a classification system to categorise the sensitivity of shared information. This might be based on the PSPF.

There are also several opportunities for government to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident. These include:

- Incident Response Assistance - offer government assistance in incident response and recovery efforts. This can include technical support, expertise, and resources to help entities effectively mitigate and recover from cyber incidents.

- Financial Incentives and Grants - provide financial incentives, such as grants, to entities that actively engage in information sharing and collaborative efforts.
- Training and Capacity Building - offer training programs and capacity-building initiatives to enhance the cybersecurity capabilities of participating entities.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

ARTC suggests the following should be considered following a cyber security crisis incident as part of an in-depth debrief / lessons learned protocol:

- Purpose - the CIRB should serve as a valuable tool for learning from cyber incidents, promoting collaboration, and driving continuous improvement in the overall cybersecurity posture of the nation;
- Size - should be large enough to encompass various domains, including technical cybersecurity, legal, regulatory, and industry-specific knowledge; and
- Subcommittee consideration - considering the establishment of subcommittees or expert groups for specific incidents allows for flexibility in managing the workload without overwhelming the entire board.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

The proposed amendments to the SOCI Act should emphasise the importance of proactive cybersecurity measures while ensuring regulatory requirements are feasible and conducive to effective business operations.

Consideration must also be given to the financial and non-financial impacts of the proposed amendments. Organisations should evaluate potential costs, resource requirements, and implications for data usability in their business operations. Classifying data across the organisation and ensuring the Information classification policies and procedures are in place and implemented across all departments could take 1 – 3 years dependent on size of organisation. This may be an opportunity for the ASD and ACSC to provide assistance and support.

ARTC manages risk to corporate networks and systems that hold business critical data through several mechanisms, including the maintaining of a risk management framework to categorise data, and by implementing appropriate security controls that mitigate threats.

Measure 6: Improving our national responses to the consequences of significant incidents – Consequence management powers

The proposed principles and safeguards appear comprehensive and are likely to provide sufficient oversight for the use of the power. However, it is essential to ensure that implementation guidelines are clear and should be consistently applied to avoid ambiguity or misuse of authority. Additionally, mechanisms for independent review or oversight of decisions made under this power could enhance accountability and public trust.

The principles and safeguards outlined provide a structured framework for managing the use of the consequence management power. However, it is essential to ensure that oversight mechanisms are robust and transparent. This includes regular reporting on the use of the power, consultation with affected entities and relevant authorities, and clear criteria for assessing the necessity and proportionality of issuing directions.

ARTC suggests consideration be given to existing legislation and policy frameworks at both the Federal and State/Territory levels, to avoid duplication of effort and ensure coherence in regulatory responses. Coordination with relevant laws, such as state emergency management acts or privacy regulations, should be prioritised to facilitate effective implementation and compliance.

Overall, ARTC position on the proposed framework is that it offers a sound, structured approach to managing incident consequences while safeguarding critical infrastructure and national interests.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

Adopting a harms-based approach for information disclosure under the SOCI Act provides clearer guidance to entities on when to share information. While this approach introduces flexibility, it may also complicate decision-making processes, as entities must assess potential harms to various interests, including security, commercial interests, and public welfare. However, by clarifying the boundaries for disclosure, this change can enhance transparency and community trust in information sharing practices.

Additionally, broadening provisions for disclosure to include all Commonwealth, State, and Territory Government entities regardless of policy responsibility is crucial for promoting seamless incident response coordination and collaboration. Addressing gaps in categories of entities eligible to receive protected information ensures comprehensive support for incident response efforts and strengthens national security and resilience.

Benefits may also be realised by amending existing sections concerning authorised disclosure to the Inspector-General of Intelligence and Security (IGIS) to include voluntary disclosures would facilitate the agency's functions and enhance Australia's overall security apparatus. Removing barriers to voluntary disclosure encourages proactive engagement with oversight bodies, contributing to a more robust security framework.

While a move towards a harms-based threshold for information disclosure may initially complicate decision-making, it ultimately provides a more nuanced framework for assessing the need for information sharing. This change may require entities to conduct more comprehensive risk assessments but ultimately facilitates more informed and targeted information disclosure practices.

Overall, the proposed revisions represent positive steps towards improving the effectiveness and efficiency of the information sharing regime under the SOCI Act, fostering greater collaboration, and enhancing national security and resilience.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

While the proposed review and remedy power introduces a mechanism for addressing deficiencies, it complements a preventative risk approach by encouraging entities to continually enhance their risk mitigation plans. The collaboration between the CISC and industry, coupled with oversight mechanisms and proportionate responses, creates a framework that encourages entities to proactively manage and address risks before they escalate. ARTC suggests the ASD and ACSC provide training programs or access to appropriate risk management tools or training in effective risk management frameworks and tools.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

TSRMP and notifications obligations will undoubtedly impact business operations if appropriate governance and oversight is not carefully implemented. To effectively manage these risks, ARTC suggests:

- Align TSRMP with internationally recognised security standards, such as ISO/IEC 27001, to ensure a comprehensive and globally accepted framework.
- Interaction with Other Requirements: Clarity is needed on how TSRMP interacts with existing state, territory, and Commonwealth requirements. Clear guidelines should be provided to avoid duplications and ensure a coherent regulatory landscape.
- Barriers to Notification Process: Streamlining reporting mechanisms, providing clear guidelines, and offering support for compliance can enhance industry participation.
- Harmonisation and Co-Design: Engaging industry stakeholders in the development process will ensure that the framework is practical, minimises complexity, and addresses sector-specific nuances.
- Loss of Cyber Maturity and Security Standards: Transparent criteria for evaluating and preserving existing security levels should be established.
- Alignment with Other Critical Infrastructure Sectors: The alignment of obligations for telecommunications entities with other critical infrastructure sectors is welcomed. This approach promotes consistency and facilitates a holistic approach to cybersecurity across different sectors.
- Promotion of Uplift and Enhancement: Regular consultation and feedback mechanisms should be established to adapt the framework to evolving cybersecurity threats and technologies.