Notitia
Level 4
152 Elizabeth Street
Melbourne, VIC 3000
+61 404 233 903
hello@notitia.com.au
notitia.com.au

14 February 2025

The Hon Tony Burke MP

Minister for Home Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Dear Minister for Home Affairs

Re: Submission to the Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)

Notitia is a leading Australian data and digital transformation firm, specialising in providing strategy and tactical solutions to organisations operating in highly regulated industries, including government, healthcare, and critical infrastructure.

We work closely with entities managing business-critical data, supporting them in implementing secure, scalable, and compliant data management and enabling organisation-wide data-driven decision making.

Notitia welcomes the opportunity to provide feedback on the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Amendment (Data Storage Systems) Rules 2024*, which seek to clarify and strengthen obligations

under the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023*.

Notitia fully supports the intent behind these changes and we highlight areas where further alignment with existing frameworks is needed to facilitate a smooth adoption and implementation.

We advocate on behalf of our clients, including business owners who will be impacted by these changes. Many of our clients operate in industries that rely on efficient and cost-effective data management solutions. We seek to ensure that the amendments provide practical, scalable, and well-supported measures to help businesses maintain operational continuity while improving cyber resilience.

If you have any questions regarding this submission, please feel free to contact me directly via email Alex.Avery@notitia.com.au or mobile 0404 233 903.

Yours sincerely

Alex Avery
Managing Director

Submission to the Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)

Rule: Submission on the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Amendment (Data Storage Systems) Rules 2024

1. Introduction

Notitia is a leading Australian data and digital transformation firm, specialising in providing strategy and tactical solutions to organisations operating in highly regulated industries, including government, healthcare, and critical infrastructure.

We work closely with entities managing business-critical data, supporting them in implementing secure, scalable, and compliant data management and enabling organisation-wide data-driven decision making.

Notitia welcomes the opportunity to provide feedback on the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Amendment (Data Storage Systems) Rules 2024*, which seek to clarify and strengthen obligations under the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023*.

Notitia fully supports the intent behind these changes and we highlight areas where further alignment with existing frameworks is needed to facilitate a smooth adoption and implementation.

We advocate on behalf of our clients, including business owners who will be impacted by these changes. Many of our clients operate in industries that rely on efficient and cost-effective data management solutions. We seek to ensure that the amendments provide practical, scalable, and well-supported measures to help businesses maintain operational continuity while improving cyber resilience.

In this submission we will refer to the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023* as the "2023 CIRMP Rules" and the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Amendment (Data Storage Systems) Rules 2024* as the "2024 Amendments".

2. Integration of data storage systems into existing risk management programs

The "2023 CIRMP Rules" require critical infrastructure entities to develop, implement, and maintain a Critical Infrastructure Risk Management Program (CIRMP). The proposed "2024 Amendments" expand these obligations to explicitly include "data storage systems that hold business-critical data".

Key considerations:

- Entities must now "identify, assess, and mitigate risks related to data storage systems", even if these systems are not the primary function of the critical infrastructure asset.
- Risk assessments should extend to third-party cloud providers and data processing partners.
- The definition of 'business-critical data' needs to be refined to avoid over-regulation of general operational data.

Recommendation:

- Ensure risk assessments are proportionate to the sensitivity and function of the data stored.
- Provide guidance on compliance expectations for hybrid environments, multi-cloud architectures, and third-party dependencies.
- Allow alignment with existing risk management frameworks (e.g., ISO 27001, ACSC Essential Eight) to prevent regulatory duplication.

3. Clarification of responsibilities in outsourced data storage arrangements

The "2023 CIRMP Rules" already require entities to manage risks arising from third-party dependencies. The "2024 Amendments" emphasise the need for clear responsibility delineation in data storage arrangements.

Key considerations:

- Many entities rely on third-party cloud storage (AWS, Azure, Google Cloud, private data centres) but retain ultimate accountability under the SOCI Act.
- The "2024 Amendments" mandate notification requirements for third-party data providers under section 12F of the SOCI Act.

Recommendation:

- Establish a clear shared responsibility framework, outlining specific security obligations for entities and their third-party service providers.

- Mandate contractual obligations to ensure third-party compliance with CIRMP standards.
- Provide guidance on assessing third-party risk management under CIRMP requirements.

4. Alignment with existing cyber security frameworks

The “2023 CIRMP Rules” already require alignment with best-practice security frameworks, including the ACSC Essential Eight, ISO 27001, and the Information Security Manual (ISM). The “2024 Amendments” should ensure consistency with these existing regulations.

Key considerations:

- Entities managing critical infrastructure are already subject to multiple overlapping security regulations.
- Duplicative reporting and compliance efforts may increase operational costs without improving security outcomes.

Recommendation:

- Allow entities demonstrating compliance with ISO 27001, NIST CSF, or SOC 2 to use these certifications as evidence of meeting CIRMP obligations.
- Align “incident reporting requirements” with existing frameworks to prevent unnecessary administrative burdens.
- Provide a regulatory mapping document showing how CIRMP obligations align with existing cyber security standards.

5. Proportional compliance for SMEs and mid-sized entities

While the “2023 CIRMP Rules” apply to “all entities managing critical infrastructure”, the “2024 Amendments” introduce new compliance requirements for data storage systems, which could disproportionately impact smaller organisations.

Key considerations:

- Smaller organisations may lack resources to implement new security measures quickly.
- Overly broad compliance obligations could discourage cloud adoption, pushing organisations towards less secure on-premise storage.

Recommendation:

- Implement a tiered compliance model where obligations scale based on risk profile, data sensitivity, and organisation size.
- Provide government-backed support mechanisms, including compliance grants or security advisory services for SMEs.
- Extend the six-month compliance period to 12 months for SMEs and mid-sized organisations.

6. Extended compliance timeframes and industry support

The "2024 Amendments" propose a six-month grace period for compliance after the rules take effect. Given the complexity of CIRMP implementation, this may not be sufficient for many organisations to assess, implement, and integrate new risk management obligations.

Recommendation:

- Extend the compliance period to 12 months for entities requiring significant security enhancements.
- Develop government-led training programs and industry workshops to assist entities in understanding and fulfilling new obligations.

7. Conclusion

Notitia fully supports the intent of the "2024 Amendments" to strengthen cyber security protections for data storage systems in critical infrastructure. Ensuring clarity, proportionality, and regulatory alignment will be essential for practical implementation.

We urge the government to consider:

1. Refining the definition of "business-critical data" to focus on "high-risk categories".
2. Providing clear guidance on "shared responsibility models" for outsourced data storage.
3. Ensuring CIRMP obligations align with existing cyber security frameworks to prevent unnecessary duplication.
4. Implementing a tiered compliance model for SMEs to reduce undue regulatory burdens.
5. Extending compliance timeframes and providing industry support to facilitate smooth adoption.

Notitia
Submission to Minister for Home Affairs: Consultation on Subordinate Legislation

---

We welcome continued engagement with the government on this critical legislative reform and remain available to provide further insights based on our industry expertise.

Submitted by: Notitia
Date: Friday, 14 Feb 2025

Contact Information:
Alex Avery, Notitia Managing Director
Alex.Avery@notitia.com.au
+ 61 404 233 903