CIRMP Rules Consultation 2026

Dear Sir/Madam,

Thank you for the opportunity to respond to the proposed changes to the Critical Infrastructure Risk Management Program (CIRMP) rules.

We are an Australian organisation whose mission is to radically improve trust in digital transactions for the benefit of all. We have an expert perspective on specific areas of the proposed changes and, as Australians, we are personally motivated to have critical infrastructure that keeps working in times of increasing geopolitical uncertainty.

In our response we argue that trustworthy digital credentials are a foundation of all critical infrastructure and hence should be included as a "fifth element" of the existing Critical Infrastructure Risk Management Model. We see the issuance, management and verification of trustworthy credentials as a common requirement across each of the four presented pillars (Cyber, Personnel, Supply Chain, Physical), critical in supporting the resilience of interactions and trust between those involved (organisations, individuals, software and systems) during normal operation and in response to failures.

Further, we believe that the Australian Government's investments in Digital ID infrastructure (the Digital ID Act, AGDIS, ongoing work on verifiable credentials etc.) can be used to provide a legally bound foundation for higher trust, lower risk and more resilient authentication that can reduce the cost and burden of existing checks in normal operation, let alone when outages and failures occur. This also increases the return on investment in Digital ID solutions, infrastructure and governance by Australia.

On the topic of Supply Chain Hazards, we believe that the Australian Government should look at the work of the UN and the UN/CEFACT projects on supply chain transparency and trust at scale. These initiatives are establishing open, royalty free, global standards that follow a "protocol not platform" approach to maximise trust, minimise cost, and maximise the return on existing investments in platforms and infrastructure.

We would welcome discussion on these observations and recommendations.

John Phillips
Co-Founder
Sezoo

Jo Spencer
Co-Founder
Sezoo

Questions from Consultation Paper

For ease of reference we have repeated the specific questions raised in the paper.

As we are not a provider or operator of critical infrastructure, there are some questions for which we are not in a position to respond. For these we have provided a “N/A” response. Where we have provided a response, this is from our perspective as experts in digital trust and as Australians who are dependent on the services provided by critical infrastructure.

Section	Regulatory Impact / Policy Design Questions	Sezoo Response
All-hazard measures **All-hazard 1: Consideration of specified risk advice**	Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation? Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?	**Yes**. Use a combination of the Digital ID Act and AGDIS for onboarding and authentication of all people working on CI and extend the work on Verifiable Credentials (within the Department of Finance) such that each individual has the appropriate verifiable credentials to support their role and duties.
All-hazard 2: All-hazard material risks - foreign ownership, control and influence	Are there other specific material risks, like those arising from FOCI, that your organisation minimises or eliminates in their CIRMP? Does your organisation currently consider FOCI risks in their CIRMP?	N/A However, we believe that the Government should look to work such as the UN/CEFACT projects on supply chain transparency and trust, as well Linux Foundation work on securing Open Source Software contributions as elements of FOCI risk reduction.
All-hazard Measures - Regulatory Impact Analysis	1. Does your organisation already respond to risk advice in this manner? For example, acting upon it as soon as practicable to ensure continuity of operations? 2. What changes would you need to make to your current processes? 3. What one-off costs would you expect (e.g., new workflow tools, staff training)? 4. What ongoing costs would you expect (e.g., staff time to review specified advice, update CIRMP)? 5. How did you estimate these costs? 6. How much time would you need to implement these changes? 7. Are there any limitations that would make this difficult for your organisation	N/A
Cyber and Information Security Hazard measures **Cyber 1: Cyber security framework uplift**	• Where applicable, what maturity/profile does your organisation seek to achieve? • How does your organisation invest in security beyond achieving minimum cyber framework compliance? • Does your organisation face challenges in obtaining the necessary investment in security to reach compliance, or (where necessary) go beyond the minimum cyber framework?	N/A

Section	Regulatory Impact / Policy Design Questions	Sezoo Response
Cyber 2: Critical systems network protection	• What current measures does your organisation implement to segregate critical systems from all other internet facing and less secure systems? • Does your organisation mandate security awareness training for users with access to critical systems? • What measures does your organisation undertake to log who has access and can make changes to your critical systems? • Does your organisation undertake logging and monitoring of network traffic?	Firstly we support the observations and intent behind this section of the paper. Further, we see inter-agent trust (human, organisation, software API, AI Agent etc.) as a fundamental pre-requisite of a trustworthy system, and that in order to achieve resilience and be anti-fragile, inter-agent trust must be a peer-peer, decentralised, and in -real time calculation. This is why we strongly recommend that the opportunity presented by verifiable credentials is pursued by the Australian government for all critical infrastructure trust operations. Federated models, models with exchanges and other forms of centralised trust cannot be "operationally independent". They are **fragile**, **single points of failure**, no matter how thick we make their walls. We have no direct response to the policy design questions but we note that none of these questions address the issue of resilience (segregation is necessary but does not guarantee resilience).
Cyber 3: Multi-factor authentication (MFA)	• What type of systems in your organisation are currently protected by MFA? • Are there system or/circumstances in which MFA is not reasonably practicable to use? If so, what other compensating controls are, or could be implemented?	While we support the intent of the message here, we feel that the proposal is outdated, insufficient, and that (it appears) that too much time is given to implement. The text "to have a documented plan within the CIRMP that details how compliance will be accomplished in attestation periods leading up to the September 2028 attestation period." doesn't make it clear whether a **plan** is needed **before** Sept 2028 and compliance **by** Sept 2028, or that *only* a plan is needed by Sept 2028. Either way, two years is a significant window in these geo-politically unstable times. We propose that the Government look to apply the existing work on MyID and AGDIS across the Critical Infrastructure landscape such that 1) onboarding is dependent on presentation of a strong government ID through MyID (or equally authoritative government source) 2) Credentials are not possible to transfer no matter the vector. Here we would look to technology such as passkeys, biometrically bound credentials and liveness checks that are used on every interaction subject to risk.

Section	Regulatory Impact / Policy Design Questions	Sezoo Response
Cyber 4: Enhancing cyber material risks	1. Is your organisation already compliant with one, or more of these four amendments? If so, please tell us which ones. 2. If you are not compliant with these amendments, which one would be most challenging for you? Why? 3. What one-off costs would you expect (e.g., hardware/software upgrades, consultancy)? 4. What ongoing costs would you expect (e.g., monitoring, audits, licence renewals)? 5. How did you estimate these costs? 6. How much time would you need to implement these changes 7. Are there any dependencies or constraints (e.g., physical configuration of OT/IT systems, vendor availability, certification cycles)?	N/A
Supply Chain Hazard measures **Supply Chain 1: Supply chain vulnerability mapping**	• To what level of upstream and downstream detail does your organisation currently map their supply chain? • Does your organisation keep a list or record of alterative approved suppliers? • Does your organisation have real-time access to data surrounding supplier availability?	We strongly recommend that the Government look to the work of UN/CEFACT projects on supply chain transparency, such as the United Nations Transparency Protocol (https://untp.unece.org/) and Global Registrar Information Directory (https://un.opensource.unicc.org/unece/uncefact/gtr/) These are global initiatives with aims to significantly increase supply chain transparency at scale. In addition, they are actively being supported and/or led by Australian organisations. There are a growing number of commitments to implementations of these protocols with announcements expected soon from some of the world's largest and most valuable companies on their commitment, and the requirement for their suppliers to commit, as well as UN Member State commitments to develop pilots.
Supply Chain 2: Vendors of concern	• How does your organisation currently map vendors of concern in your supply chain? • What current security measures are put in place if a vendor of concern is identified? • Does the wider government provide adequate material to support you to identify a vendor of concern and mitigate their potential impact? • Are there other options to reduce the FOCI risk posed by vendors of concern, either in addition to or instead of the proposed approach?	Adoption of UNTP and GRID would not only provide Critical Infrastructure operators with significantly increased confidence in their suppliers (and their supply chains), but also enable trustworthy identification and communication of vendors of concern by the regulator.

Section	Regulatory Impact / Policy Design Questions	Sezoo Response
Supply Chain Hazard - Regulatory Impact Analysis	1. Is your organisation already compliant with one, or both, of these amendments? If so, please tell us which ones. 2. What changes would you need to make to your procurement or supplier management processes? 3. What one-off costs would you expect (e.g., mapping tools, supplier audits)? 4. What ongoing costs would you expect (e.g., periodic reviews, monitoring)? 5. How did you estimate these costs? 6. How much time would you need to implement these changes? 7. Are there practical limitations (e.g., lack of alternative suppliers)? 8. Would this limit the supply of good and services you provide, or potentially your competitiveness in the market? If yes, please describe how.	Both UNTP and GRID are designed as a low cost "and" to existing investments. They are "protocols not platforms" - no new infrastructure is required and implementation costs are minimal
Personnel Security Hazard measures **Personnel 1: Personnel security plan**	• Does your organisation have a personnel security plan, or equivalent in place? • Would a personnel security plan requirement improve security posture or duplicate existing controls? • Does your organisation currently use background checking as a security control? • How many AusCheck background checks do you anticipate undertaking each year? • What practical limitations do you foresee for your organisation if required to implement a personnel • security plan?	N/A - although we would like to point out that the use of Verifiable Credentials, supported by MyID, allows for the separation of "identification" of individuals and their role based credentials **AND** the ability to support decentralised verification of these artefacts. Our proposal that MyID be required as the government ID would also help to reduce the background checking and security control.
… continuation	1. Is your organisation already compliant with this amendment, or does it have a similar onboarding process in place. Please describe the similar process if it exists. 2. What changes would you need to make to your HR or onboarding processes? 3. What one-off costs would you expect (e.g., system updates, training)? 4. What ongoing costs would you expect (e.g., fees per check, staff time)? 5. How did you estimate these costs? 6. How much time would you need to implement these changes? 7. Are there any challenges in defining "critical workers" for your organisation?	See above. Nothing further to add.
Physical and Natural Hazards	• Does your organisation have a broader physical security plan? • What type of physical security measure would be beneficial? • Would a mandated physical security measure would be beneficial and how it could be effectively applied to your asset? • Are there other additional material risks that your organisation considers could be included for physical or natural hazards?	N/A