With reference to:

https://www.homeaffairs.gov.au/reports-and-pubs/files/co-design-governance-rules-risk-management-summary.pdf

"What we heard ... personnel security was often treated separately [silos serve a purpose] due to privacy obligations"

We agree.

However, in terms of the personnel security theme, the term "Background Check" for emaple is defined in legalisation but was not mentioned in the summary paper.

The CIC's original charter included reducing the risk of malicious trusted insider threats - ie. "espionage, coercion and sabotage".

Australian Government | Critical Infrastructure Centre

The Australian Government established the Critical Infrastructure Centre (the Centre) in January 2017, to safeguard Australia's critical infrastructure. The Centre brings together expertise and capability from across the Australian Government to manage the increasingly complex national security risks of sabotage, espionage and coercion.

Half of the public submissions referred to *personnel security* - for it not be in the summary seems to be an oversight or obfuscation.

For example, "Union in fight against new laws that would force 2 million workers to turnover internet history, emails."

https://www.miragenews.com/union-in-fight-against-new-laws-that-would-592823/

In response to the Consultation Paper, the Department of Home Affairs received 194 submissions.

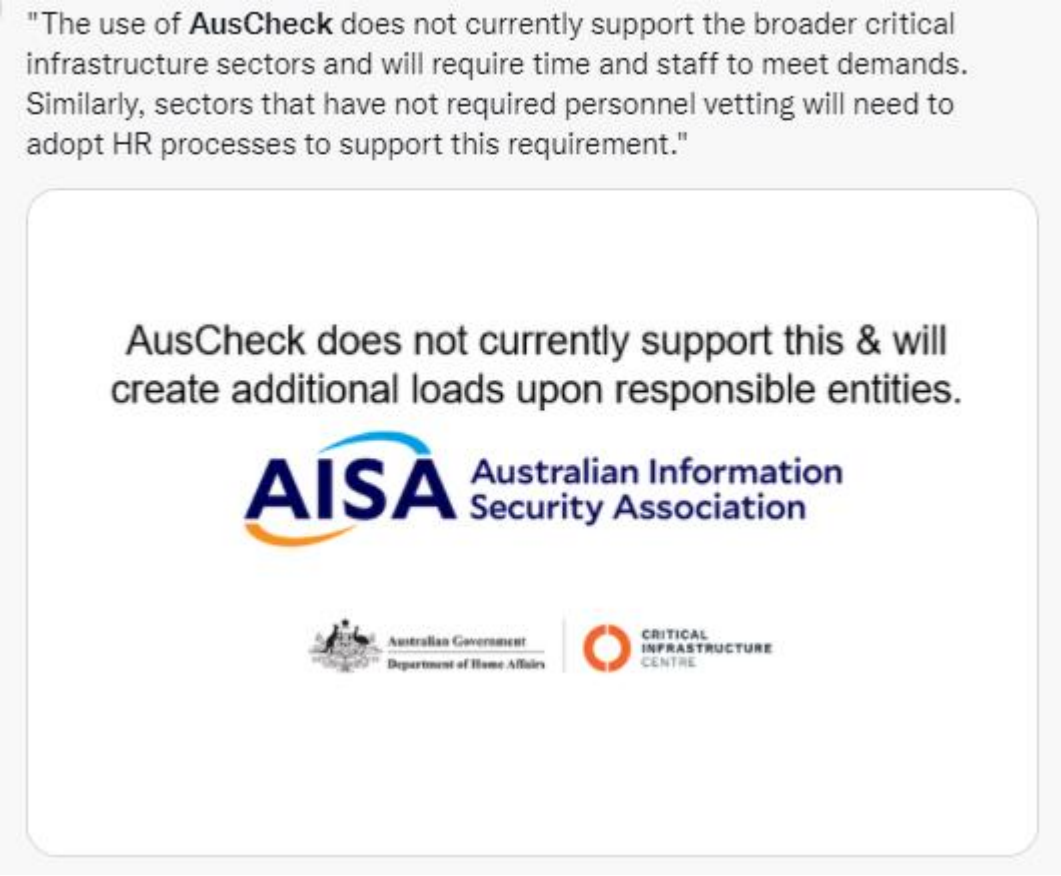
128 public submissions are public.

60 (or 47%) made comments relating to personnel security.

Here is a summary: 58 excerpts (left column) with their source link.

https://www.cleard.life/critical-infrastructure-public-submissions-react-to-trusted-insider-risk-mitigation-options/

If "Background Check" is defined in legislation exclusively as an Auscheck check, with an Australian-based ID check and an ASIO Assessment, then this would be an unworkable definition for all two million employees residing inside & outside of Australia. For example:



"Industry stakeholders supported the need to avoid duplication, including by cross-referencing existing risk frameworks. Further suggestions were made that risk frameworks should be aligned with ISO31000, an international standard widely adopted across sectors in Australia."

Please note that the Australian Standards 4811 Employment Screening (2022 soon to be released) seems to align with ISO 31000.

Scope/Context/Criteria– The employment screening will need to take into account: drug use, financial vulnerabilities, data breaches, theft or fraud or sexual misconduct in the workplace (not reported to Police), AVOs or DVO's outside of the workplace. Critical infrastructure sectors will need to consider foreign influence risks – such as state-based espionage or sabotage.

Risk Identification – inclusion of the 21 dimensions of a person's background that the PSPF use in which 440,000 people have been screened against in Australia.

Risk Analysis – use the fair, non-discriminatory PSPF Adjudicative Guidelines.

Risk Evaluation – an easy to understand Green (favourable), Amber (Caution) , Red (Adverse) result gives actionable intelligence.

"TISN is a trusted, non-competitive environment for the critical infrastructure community to better plan, prepare, respond and recover in the face of all hazards."

However, there is no standardised background check that is used for users to gain access to TISN. The Protective Security Police Framework notes that all government employees and contractors must have a suitability assessment done before accessing commonwealth resources and information.

TISN leaders have stated that they *trust* that the member organisations have a trusted workforce and the people they select to be part of TISN are also trustworthy. This occurs with no verification or assurances. This does not seem PSPF compliant or consistent. TISN should at least use the standard PSPF12 suitability assessment (Baseline-equivalent) of which there are commercial options available.

Thank you for your time and consideration.

This submission can be published.