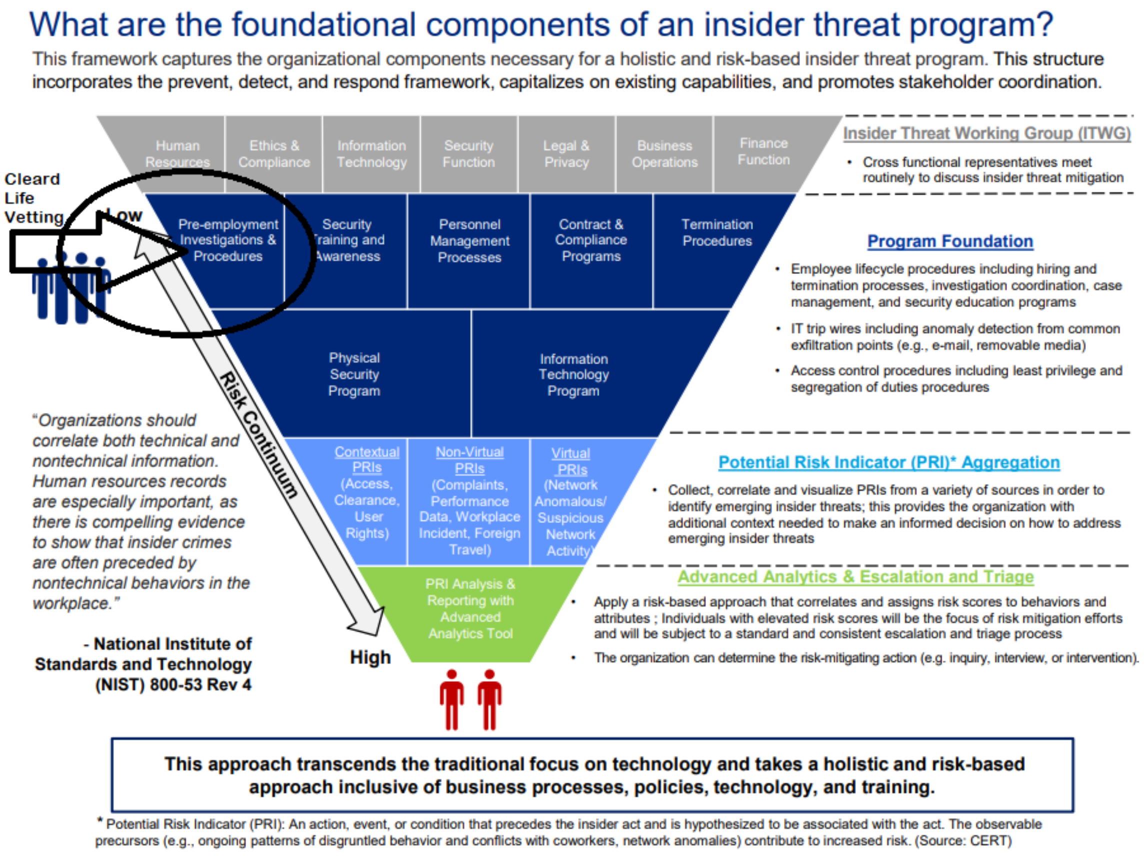
Submission No 1

INQUIRY INTO CYBERSECURITY

Organisation:	Crown Vetting and Cleard Life Vetting Agency
Date Received:	13 August 2020

Three Royal Commissions (Sexual Abuse, Banking & Aged Care) are helpful in reflecting societies' integrity standards and expectations on character. As a result, the Royal Commissioners have called for enhanced integrity and screening practices.

We have also seen the NDIS create screening legislation for its clearance. The Working With Children (WWCC) and the Working with Vulnerable People expect to screen 1:5 Australian Adults nationwide. Teachers are not required to hold a WWCC as they are screened in a different way, but are screened never-the-less. Aged Care will likely have its own clearance too. ASIO wants to pre-vet the naval industry, prior to a NV1/SECRET clearance. QLD has recently established an explosives security clearance (for mining & fireworks industries) that considers Domestic Violence issues. We also have ASIC & MSIC cards for port workers. Home Affairs has a Trusted Trader program that expects members to vet their import/export workforce. Even one of the top consulting firms in the world has commenced a 'continual vetting' regime on all of its 27,000 staff, worldwide. **Turning to Cyber**, 12% of submissions of the recent Home Affairs Cyber Strategy 2020 understand that malicious (not a fat finger or clicking on a bad link) trusted insider do some of the most harm. Here is an open source Big Four Consulting Firm Insider Threat Program example. (Note the NIST comments)



What are the foundational components of an insider threat program?

This framework captures the organizational components necessary for a holistic and risk-based insider threat program. This structure incorporates the prevent, detect, and respond framework, capitalizes on existing capabilities, and promotes stakeholder coordination.

Human Resources
Ethics & Compliance
Information Technology
Security Function
Legal & Privacy
Business Operations
Finance Function
Cleard Life Vetting
Low
Pre-employment Investigations & Procedures
Security Training and Awareness
Personnel Management Processes
Contract & Compliance Programs
Termination Procedures
Physical Security Program
Information Technology Program
Contextual PRIs (Access, Clearance, User Rights)
Non-Virtual PRIs (Complaints, Performance Data, Workplace Incident, Foreign Travel)
Virtual PRIs (Network Anomalous/ Suspicious Network Activity)
PRI Analysis & Reporting with Advanced Analytics Tool
Risk Continuum
High

Insider Threat Working Group (ITWG)

- Cross functional representatives meet routinely to discuss insider threat mitigation

Program Foundation

- Employee lifecycle procedures including hiring and termination processes, investigation coordination, case management, and security education programs
- IT trip wires including anomaly detection from common exfiltration points (e.g., e-mail, removable media)
- Access control procedures including least privilege and segregation of duties procedures

Potential Risk Indicator (PRI)* Aggregation

- Collect, correlate and visualize PRIs from a variety of sources in order to identify emerging insider threats; this provides the organization with additional context needed to make an informed decision on how to address emerging insider threats

Advanced Analytics & Escalation and Triage

- Apply a risk-based approach that correlates and assigns risk scores to behaviors and attributes ; Individuals with elevated risk scores will be the focus of risk mitigation efforts and will be subject to a standard and consistent escalation and triage process
- The organization can determine the risk-mitigating action (e.g. inquiry, interview, or intervention).

"Organizations should correlate both technical and nontechnical information. Human resources records are especially important, as there is compelling evidence to show that insider crimes are often preceded by nontechnical behaviors in the workplace."

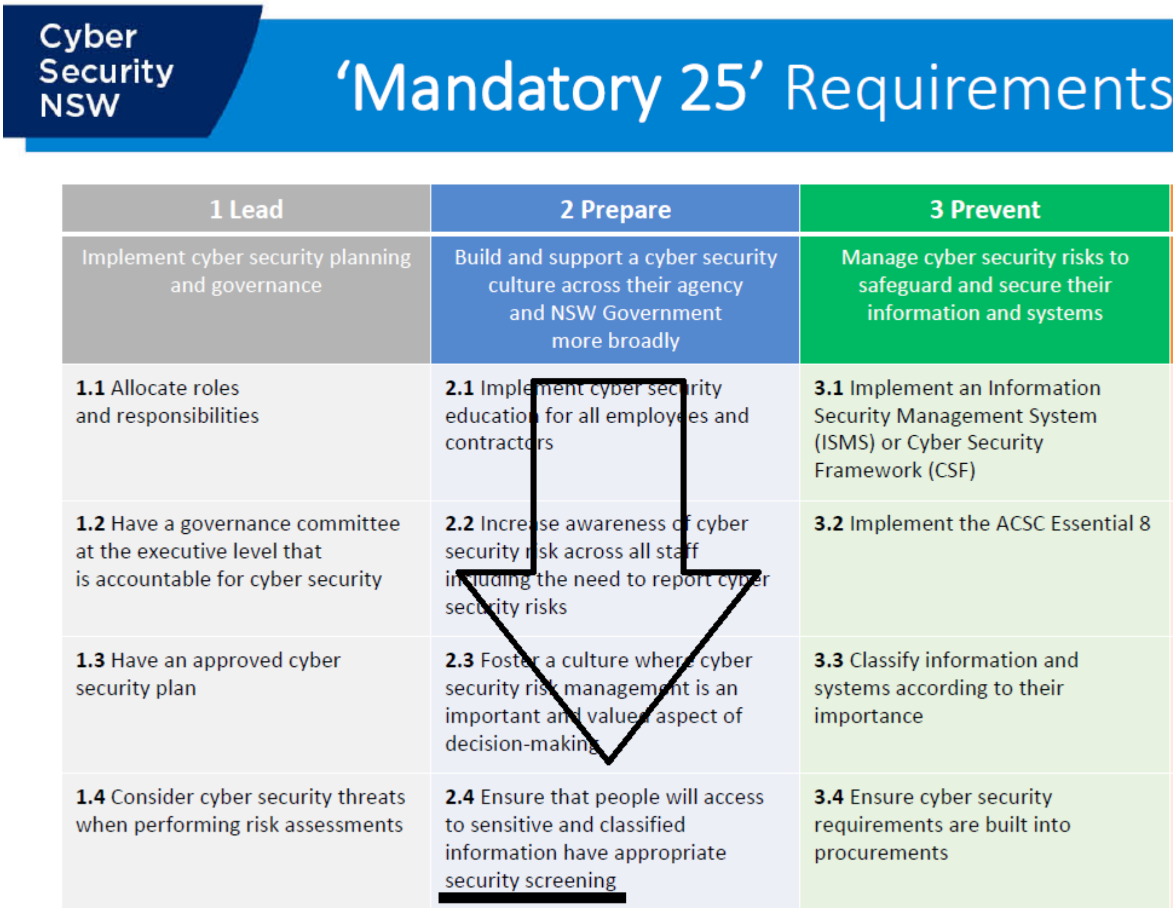
- National Institute of Standards and Technology (NIST) 800-53 Rev 4

This approach transcends the traditional focus on technology and takes a holistic and risk-based approach inclusive of business processes, policies, technology, and training.

* Potential Risk Indicator (PRI): An action, event, or condition that precedes the insider act and is hypothesized to be associated with the act. The observable precursors (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers, network anomalies) contribute to increased risk. (Source: CERT)

As NSW citizens provide sensitive and personal information to government, this information must be protected. The NSW Strategy framework draws on the National Institute of Standards and Technology (NIST) Framework which consists of standards, guidelines, and best practices to manage cyber security-related risk. As seen on page 1, NIST highlights the importance of human elements and screening.

Page 12 of the 2018 NSW Cyber Strategy recommended a review and reformulation of the Digital Information Security Policy (DISP) and development of a draft minimum cyber security standards model and mandatory reporting arrangements. It also referenced the 'Mandatory 25' Requirements for Cyber Security.



Cyber Security NSW

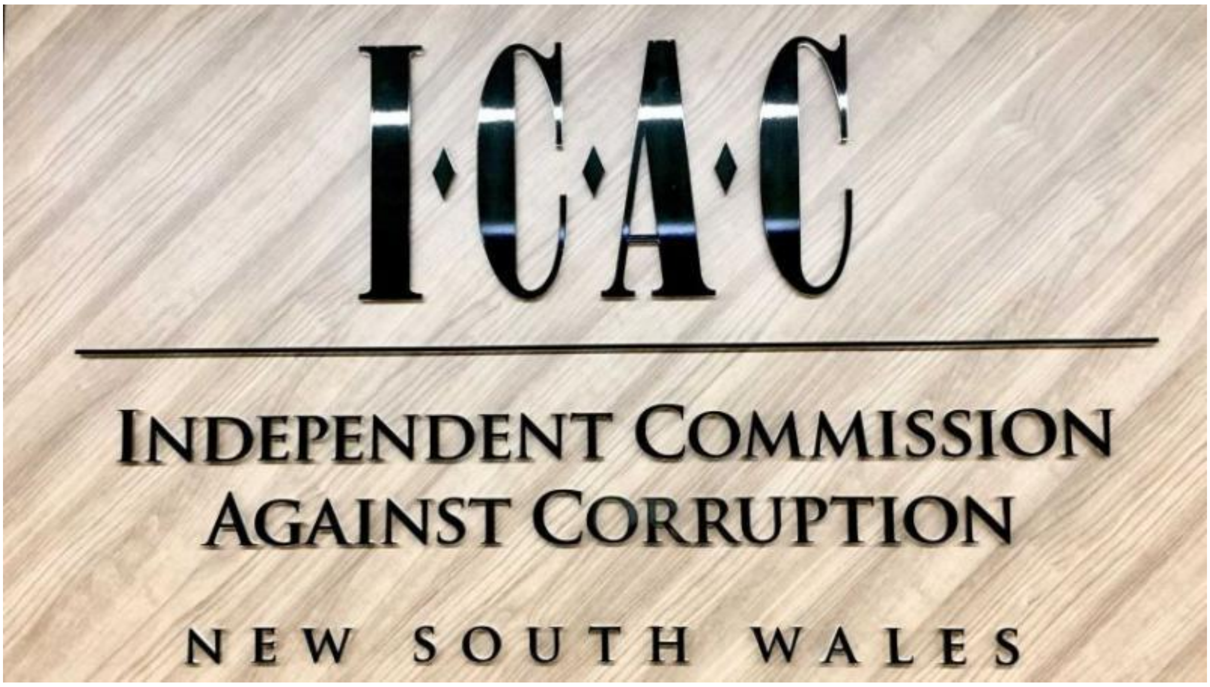
'Mandatory 25' Requirements

1 Lead	2 Prepare	3 Prevent
Implement cyber security planning and governance	Build and support a cyber security culture across their agency and NSW Government more broadly	Manage cyber security risks to safeguard and secure their information and systems
1.1 Allocate roles and responsibilities	**2.1** Implement cyber security education for all employees and contractors	**3.1** Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF)
1.2 Have a governance committee at the executive level that is accountable for cyber security	**2.2** Increase awareness of cyber security risk across all staff including the need to report cyber security risks	**3.2** Implement the ACSC Essential 8
1.3 Have an approved cyber security plan	**2.3** Foster a culture where cyber security risk management is an important and valued aspect of decision-making	**3.3** Classify information and systems according to their importance
1.4 Consider cyber security threats when performing risk assessments	**2.4** Ensure that people will access to sensitive and classified information have appropriate security screening	**3.4** Ensure cyber security requirements are built into procurements

2.4 States that NSW needs to ensure that people who have access to sensitive and classified information must have **appropriate security screening**. The Action Plan (Page 14 and 15) does not include Security Screening actions but obliges CISO's to report on 2.4. Without a minimum standard, it will continue allow for poor cyber hygiene and leave undetected and unmitigated people risk inside the organisation.

"Employers should have a robust process for responding to red flags that arise from employment screening checks." - ICAC NSW White paper: Strengthening employment screening practices

"Employment screening typically consists of checking a candidate's identity. There are better practices available to inform employment screening such as the Protective Security Policy Framework (PSPF) & Personnel Security Protocol." - ICAC NSW Employment Screening Handbook.



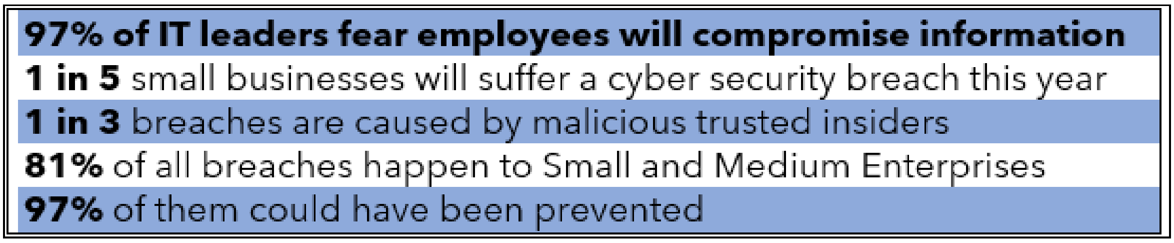
Summary:

- The trend is clear – enhanced integrity checks are needed and required in many spheres of work, sectors, and activity.
- Standardisation & transferability has not happened
- PSPF12 **requires** those who have access to resources to be checked for suitability **and** *recommends* that they are 'suitability assured' prior to a job offer, after the merit list. **A Police check is completely deficient for this purpose.** In fact a Royal Commission University of Melbourne research paper called it "futile".
- PSPF 'whole-of-person' vetting is slow, inefficient, or simply ignored.
- Proliferation and perpetuation of traditional (low-tech) security screening operations and yet *another screening unit* will not help.

Q. How can Cyber Security NSW create a standardised, transferable, common-sense approach to enable CISOs fulfil the "2.4" requirement?

NSW could consider strengthening and qualifying the "2.4" requirement by adopting a PSPF-compliant *simplified* civilian suitability clearance. Akin to a Baseline national security clearance, the NSW government's Accreditor would audit the civilian vetting agencies' processes to ensure PSPF compliance – including natural justice, procedural fairness and the whole-of-person protocol.

The implementation is simple. The CISO & CHRO could continue to use their HRIS, ATS and/or Vendor Management systems. The vetting vendor produce better, faster and fairer vetting while delivering an interoperable suitability clearance that would be approved, trusted and recognised by other employers. There could be a blockchain "trust" badge credential on workers Seek or LinkedIn profile, that signifies they have been vetted which in turn expedites the onboard process further.



97% of IT leaders fear employees will compromise information
1 in 5 small businesses will suffer a cyber security breach this year
1 in 3 breaches are caused by malicious trusted insiders
81% of all breaches happen to Small and Medium Enterprises
97% of them could have been prevented

By using *e-vetting* and *e-adjudication* platforms, built to the exacting standards of the Attorney General's Adjudicative Guidelines, it would reduce the time it takes to harvest aggravating and mitigating facts as well as the analysis. AGSVA Baseline application cycle can take 60-90 days vs *e-vetting's* 1 day.

E-vetting solutions (of which there is already one available in the commercial marketplace), or accredited *vetting-as-a-service* would assist CISOs to prepare & secure their workforce, contractors and third parties before access to sensitive 'people, assets and information' and therefore fully comply with the intent of "2.4" in the most appropriate way.

Maintenance of a civilian suitability clearance (PERSEC 13), change of circumstances analysis, multiple interested party mechanisms could also be solved by co-design and technology solutions (eg. Robotic Process Automation & AI) and market forces. This ought to be considered in light of the civilian vetting agency accreditation approval process administered by the NSW Government.

Public Submission.

Q#13. How can the NSW Government, educational institutes and industry build a market of high-quality cyber security professionals in Australia?

1:3 data breaches are done by malicious (not fat finger or clicking the wrong link) trusted insiders. Cyber security professionals should be vetted for suitability, just like government security cleared people. This can be done through the adoption of the Personnel Security (PERSEC) measures detailed in the Protective Security Policy Framework, PSPF12 & PSPF13 and the vetting practices contained therein. The NSW ICAC in its employment screening handbook has noted that this is a better approach to suitability.

Q#23. How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

Vendors selling cyber security and digital offerings should be evaluated and rated. The Rating system should include Top 4, Essential 8 and PERSEC maturity metrics.

Q#24. Are there any other insights or case studies you would like to share?

Home Affairs Cyber Strategy submissions should be considered (see next 3 pages). 12% of their submissions discuss the importance of PERSEC and clearly identify insider threat actor risk. Also, Vetting-as-a-Service platforms, such as Australian-owned Cleard Life Vetting Agency, are already commercially available in the marketplace, so adoption, can and should be immediate.

THE WORLD'S FIRST
ARTIFICIAL INTELLIGENCE
VETTING OFFICER

A BACKGROUND SCREENING SOLUTION
FOR THE CHALLENGES OF THE
COMPLEX MODERN WORKFORCE

☑ PSPF-Compliant Suitability Clearance.
Faster, Smarter, Fairer, Better.
Unprecedented Scalability.
Powered by Domain Experts.

Meet Stephanie

CLEARD LIFE
THE MISSING PIECE IS A CLEARD LIFE

www.cleard.life
Call 02 6171 4171

This is not rocket science. Most breaches are through people, some organisations will quote this stat at being over 90%. So that means good engaging awareness training, and then ensuring a culture of awareness in organisations.

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-2.pdf

If an employee gains authorised access to a network and uses it for malicious purposes, this may be a personnel security issues. This is a point that was somewhat overlooked in Australia's Cybersecurity Strategy 2016. All security areas are equally important for organisations to consider.

Office of the Victoria Information Commissioner
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-211.pdf

Currently only perceived as a requirement for government agencies to adhere, the Protective Security Policy Frame (PSPF) [PSPF 12 = PERSEC].... provide a means to address security gaps within private organisations. There is no direction or advice to business to comply with these controls, independent of their dealing with government. Promoting the implementation of these controls will begin to address this need. Improve security clearance procedures to offer faster service and to build a pipeline of multi-classification workforce which can be enacted on short notice.

Deakin University
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-183.pdf

One of the growing risks of cyber security is insider threat: the risks that current or past employees with access to critical cyber security information may pose a malicious threat. A model similar to the Department of Home Affairs' 'Trusted Trader' may be a useful paradigm to consider. Through a process of government vetting, businesses and individuals could become accredited as a trusted capability partner.

Accenture
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-189.pdf

To overcome these constraints, the Australian government could consider setting up a trusted vendor program – in a similar way that the trusted trader program exists with border industries importers. After vetting and under strict controls, more sensitive information can then be shared by Government to help industry counter cyber-attacks or develop better capabilities.

Unisys
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-93.pdf

Minimum personnel vetting to the same levels across industry and therefore ensuring that sensitive data/information doesn't find its way to someone that it shouldn't.

Queensland Government Cyber Security Unit
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-33.pdf

Ultimately, cyber is about people. People make mistakes; they can act with malicious intent.

Cyber Institute, The Australian National University
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-157.pdf

In recent times there has been a continuous evolution of policy, as the Protective Security Policy Framework (PSPF) has shifted focus from whole-of-government to whole-of-economy. The emphasis is for the PSPF to be supported and taken up by small and medium enterprises (SMEs) and the broader industry, which has not proven to be effective as there is no obvious or demonstratable return of investment for commercial entities, despite Government advice around the increasing threat landscape. … The most commonly identified constrains [to the develop of talent] is related to obtaining and maintaining security clearances. The process of obtaining clearance is often long and laborious, it is confusing for those what have never held a clearance.

Lockheed Martin
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-208.pdf

What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities? A simplified security "clearance" for this particular purpose could be considered on both permanent and temporary/as needed bases.

ACS
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-105.pdf

Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed? Two barriers; trust and cost. The recent Banking Royal Commission highlighted the lack of trust of insurance companies generally in Australia, unfortunately for good reason.

[comment: Three RC recommendations include better screening practices]
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-18.pdf

UWA believes that the Government should consider the pros and cons of introducing a set of cyber hygiene obligations that is based on industry standards and best practices.

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-22.pdf

Refers to Protective Security Policy Framework (PSPF) & AS 4811 - Employment Screening

Standards Australia
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-90.pdf

... develop the local Cybersecurity Industry - in the same way that we have a local Defence Industry to support Defence projects around the country.

[DISP includes personnel security assessments for non-security cleared staff].
AVA Group
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-103.pdf

Q. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities? A. Lack of security professionals with the correct clearance levels. Pathway for security professionals who are not working in the public sector, to receive levels of clearance commensurate with information they need to receive to inform their organisations of risk.

REA GROUP
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-51.pdf

Recommends AS 4811 - Employment Screening & the Protective Security Policy Framework.

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-158.pdf

our organisations are only as strong as their weakest link. The latest NDB data breach analysis shows that a high proportion of data breaches were due to human error. Therefore, it is not only about having cyber security technology to mitigate data breaches.

iA Group
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-95.pdf

The essential feature of a well-conceived assessment of cyber risk incorporates a whole-of-government and a whole-of-society response. The risk is society-wide and so must be the response.

[comment: three Royal Commission are reflecting society's standards for trust, which all have recommended enhanced screening for honesty and trustworthiness.]
Flinders University
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-98.pdf

With the increased connectivity and explosion in computing capability, malicious actors of all types –[including] insiders – have more opportunities and greater incentive to identify and exploit vulnerabilities, and employees have more opportunities to make mistakes.

Oracle
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-104.pdf

It is clear that the Government is seeking to gauge the level of support for expansion of its powers to deter, detect and respond to serious cyber threats.

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-112.pdf

Australian Government agencies must act consistently with the policies of the Australian Government, such as the Attorney General's Protective Security Policy Framework.

OAIC
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-197.pdf

Improvements could be made for more trusted forums, perhaps with "Chatham House" rules, for industry to safely voice their experiences in.

Transurban
https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-199.pdf

To maintain trust from the Australian community, we recommend that the government ensure there is some form of declaration that all workers with any access to personal information must sign to say that states that neither they, nor any member of their family, or any close friend or associate of theirs:
** has had any allegations of sexual or family violence made against them**
** have never had an intervention order taken out against them.**
** are not on the sexual offenders register**
** have never been charged with any form of sexual violence or family violence**

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-11.pdf

Providing a free inspection service to SMEs. A one-day audit of their actual operational processes and a vulnerability scan of their systems. 70% of data breaches occur from human factors, accidental or malicious.

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-strategy-2020/submission-6.pdf