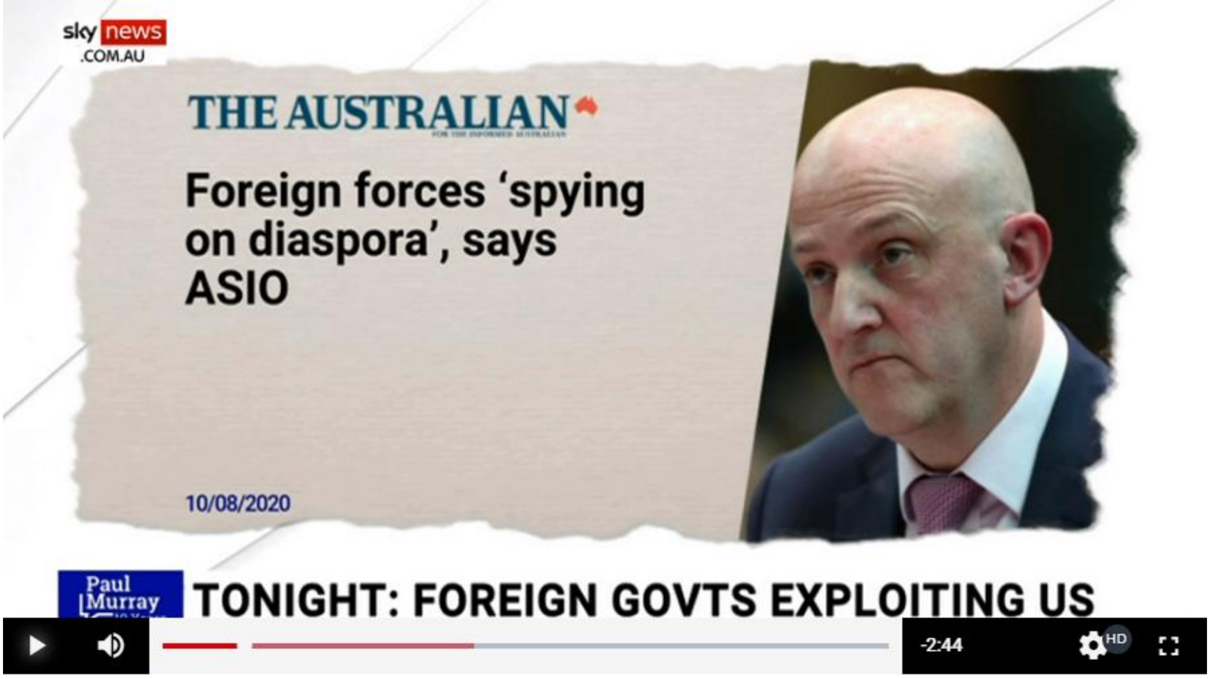
Critical Infrastructure Protection: How to mitigate sabotage, espionage and coercion and other personnel risks, guided by the principles of simplicity, transparency, accuracy and stability.

A range of hazards have the potential to significantly compromise the supply of essential services across Australia and **personnel** and cyber security are increasingly interrelated. Australia's critical systems are facing a worsening threat environment and the nation also needs to address vulnerabilities in the supply chain.

Crown Vetting has been a commonwealth panel member providing national security clearance services (Baselines to PVs) for more than ten years. We will limit our comments to our expertise, personnel security. We note that more than 12% of the Cyber Strategy 2020 submissions explicitly mention personnel risks, yet the final Cyber Strategy 2020 Report did not consider the **insider threat** as an 'actor' or a 'problem' (see page 50 for a list of identified problems). Also see the selected quotes on last two pages of this submission.

Screening people for associations with (for example) state-based actors is common-sense. To probe deep enough to consider if a worker is vulnerable to coercion is extremely important – both from a detection and deterrent point of view. In terms of cyber, IBM & Verizon research note that **malicious** (not fat finger, or clicking on a wrong link) **trusted insiders** contribute to 1:4 of all data breaches, costing millions of dollars of damage per breach and this could expose Australia to a catastrophic loss in the critical infrastructure sector.

Australia is announcing the danger and risks surrounding personnel security publicly:



THE AUSTRALIAN

Foreign forces 'spying on diaspora', says ASIO

10/08/2020

TONIGHT: FOREIGN GOVTS EXPLOITING US

An official Baseline clearance does **not** include an ASIO Assessment, but our government understands how important PERSEC is in our protecting our (Defence Industry) infrastructure. For example, last year:

*"[ASIO] have emphasised the need to act early to protect the industry, which the government has been told will become one of the nation's top targets for foreign espionage. Measures will include ******security screening******* for thousands of new employees and supply-chain network security."*
https://www.reddit.com/r/IntelligenceNews/comments/alzsjr/article_in_comments_cashedup_asio_hunting_spies/

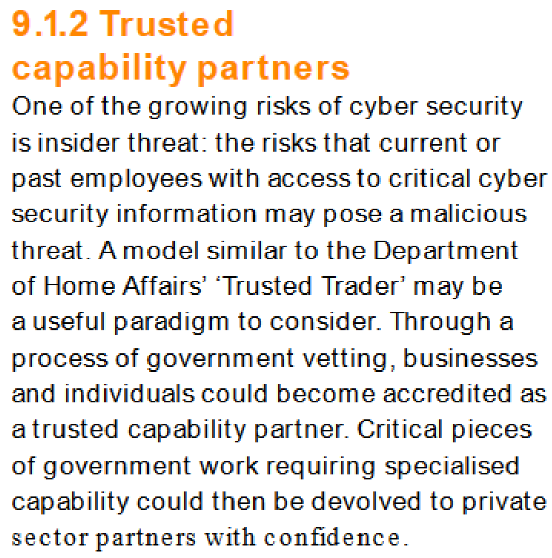
As a Defence Industry Security Program member and a people risk organisation, we appreciate that the consultation paper highlighted personnel security risk and its role to identify and understand various types of risks and then mitigate them, as pursuant to the principles-based outcomes.

> pg 20. **Personnel security.** Critical infrastructure entities will implement policies and procedures which seek to mitigate the risk of employees (insider threats) exploiting their legitimate access to an organisation's assets for unauthorised purposes. This may include:
> • Ensuring only **suitable** employees and contractors access the entity's resources
> • Assessing and managing the ongoing **suitability** of its personnel

The Security of Critical Infrastructure Act 2018 was in place before the Attorney General's October 2018 revised Protective Security Policy Framework (PSPF) was released. PSPF12 relates to personnel security and it is very clear that all personnel and contractors who have access to government resources, information, people, assets must be **suitability** cleared. PSPF13 relates to the ongoing suitability of its personnel. This is not a *'may'*, but a *'must'*. Mandatory. Of particular relevance, it could be argued that by extension, critical infrastructure owners and operators access government resources – even at non-national security level – and therefore the PSPF is applicable.

Is **suitability** defined in the PSPF? Yes. Honesty, Trustworthy, Tolerance, Maturity, Loyalty and Resilience.
Can *suitability* be determined by a $50 police check or a referee check? No.

Accenture's Cyber Strategy 2020 submission offered an important concept that relates to insiders:



9.1.2 Trusted capability partners

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. Critical pieces of government work requiring specialised capability could then be devolved to private sector partners with confidence.

We would suggest the phrase "Through a process of government vetting" be adjusted to "through a fast, standard vetting process and a favourable outcome of a PSPF-compliant suitability assessment, individuals could become trusted capability partners." Note that Accenture recommends individual vetting – not simply company vetting.

ICAC NSW in their Employment Screening Handbook note that "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 & Personnel Security Protocol."

In the context of **ongoing** suitability (PSPF13) be it periodic reviews (official Baseline is 15 years) or modern continuous vetting, understanding the background risks of employees and contractors offers the Entity knowledge to find aggregated weaknesses in their workforce security to then address, remediate and mitigate it: it could be by not hiring the unsuitable person, or by monitoring staff member's computer activities with greater scrutiny, or by altering the drug use policy, or establishing an employee assistance program, or enhanced security awareness training or cyber-awareness training or assisting with how to identify and how to handle suspicious, ongoing, unusual, persistent contact from a friend or stranger who may or may not be working for another government and so on. This is good security hygiene and a proper cyber posture which can't be done well without understanding the personnel risk topography.

Crown Vetting's sister company, Cleard Life Vetting Agency has in many ways democratised security vetting and created the ability for infrastructure owners and operators to easily and simply access a PSPF-compliant suitability check at the Baseline *equivalent*, as fast as "next day" - via through the AI-engine and vetting-as-a-service (VAAS) platform.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Yes. Mitigate trusted insider risks by assuring their suitability.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

Page 21, Figure 2, Point 5 of the Regulatory Model states "Industry complies with relevant sector specific standards, thus satisfying the Commonwealth obligations". If Regulators adopt the PSPF for PERSEC as the obligatory standard, then a PSPF-compliant suitability clearance (audited by Regulators) should naturally be deemed acceptable. Industry-specific screening can also be augmented and customised with the inclusion of an agreed sectoral (or even organisational) suitability assessment template.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

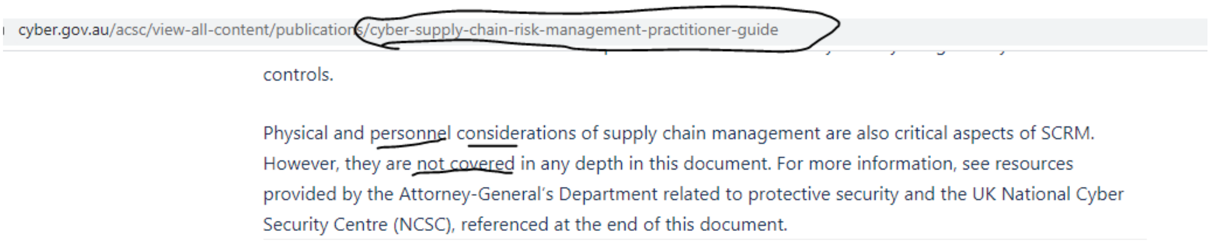
Identifying and understanding personnel security risks is rare. Unless organisations have 100% of their staff requiring security clearances, then the answer would generally be a no, not in any formal, standardised way. Also, not many PSPF-compliant suitability assessments are done by non-commonwealth Entities. The Home Affair's Trusted Trader program doesn't do vetting at the individual level, nor is it designed to be PSPF compliant. For example, the membership application asks if their organisation's HR policy includes conducting a police check. Furthermore, the PSPF12 'recommends' that a suitability assessment occurs **prior** to the employment contract offer. Not many, if any Entities, reach that lofty standard (unless the candidate has a gone through an official clearance previously). PSPF, non-national security clearance screening is not done even at the commonwealth level. At the state-level it might be worse: a recent Victorian Audit Office Report indicated that 60% of contractors did not even have a $50 police check done before commencing employment – meaning more than 3,500 workers in the Victoria public service have not been checked for any criminal history.(That report was published before the Victorian COVID security contractor fiasco). Furthermore, given the expertise that is required to vet properly, many would find it difficult to know what to ask for and if they do, they might not have the skills to make consistent and fair determinations. 1:4 complaints to the Human Rights Commissioner are due to criminal history discrimination.

13. What costs would organisations take on to meet these new obligations?

An official Baseline costs more than $700 and from the start of an e-pack to a grant notice can take 30-60 days, which degrades onboarding & recruitment. The ANAO stated that a complex Baseline cases take on average 145 days after receiving the pack. As mentioned previously, there is a commercially available PSPF-compliant, vetting-as-a-service platform that is able to complete Baseline-equivalent suitability assessments ‘next day’ at a fraction of the cost, $135. The VAAS has an REST API, so that HR departments are able to initiate an assessment inside their HR Information System or Applicant Tracking System. When triggered a text message is immediately sent to the candidate to commence the suitability process. The discreet result returns to the employer a green, amber or red light which enhances decision making capabilities for the Hiring &/or Security Managers.

Page 20. **Supply chain security.** Critical infrastructure entities will protect their operations by understanding supply chain risk. Supply chains can be compromised or disrupted from a variety of **man-made** activities. (Australian Cyber Security Centre’s Cyber Supply Chain Risk Management Practitioner Guide (2020) provide **clear** guidance on best practice supply chain management.)

The Cyber Supply Chain Risk Management Practitioner Guide unfortunately does **not** provide **clear** guidance on best practice as they relate to personnel considerations and refers the reader, we expect, to the PSPF:



cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management-practitioner-guide

controls.

Physical and personnel considerations of supply chain management are also critical aspects of SCRM. However, they are not covered in any depth in this document. For more information, see resources provided by the Attorney-General’s Department related to protective security and the UK National Cyber Security Centre (NCSC), referenced at the end of this document.

Managing third-party risks can be resolved by applying the same vetting practices and standards to contractors. It could be achieved through obligatory contractual agreements or via due diligence tender evaluations, or initial assessments for workers via vendor management systems. Glassdoor research indicates that by screening candidates you can achieve a 70% increase in the quality of your workforce – something most employers should be amenable towards – no-one likes to be betrayed and no-one wants to be responsible for letting in a ‘bad apple’.

Conclusion:

Be it for pre-employment personnel security risk measures (PSPF12), or for ongoing suitability (PSPF13) obligations or to conduct a one-time risk assessment or a cyber audit – it will go a long way to understand the hidden risks present in the critical infrastructure company’s current workforce, contractor and supply chains.

We believe that an enhanced, fast, reliable, standardised personnel security measure is not only appropriate but essential for sovereign resiliency. This element needs can be included into the risk assessment of critical infrastructure, its framework, and any legislation adjustments.

We would be pleased to assist you further.

A sample of the Cyber Strategy 2020 submissions:

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 Commissions (including banking/financial Infrastructure sector] are reflecting society's standards for trust, whereby all Commissioners have recommended enhanced integrity 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