

17 November 2021

Committee Secretary
Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity
PO Box 6100
Parliament House
Canberra ACT 2600

Phone: +61 2 6277 3419

Fax: +61 2 6277 5809

aclei.committee@aph.gov.au

**Re: Response to Inquiry into the Expansion of ACLEI's Jurisdiction and the Corruption
Vulnerabilities of Law Enforcement Agencies' Contracted Services**

Thank you for the opportunity to provide a submission to this inquiry. Veritas Engineering Pty Ltd (Veritas) provides services to the general public as an accredited body to programs that are managed by agencies that fall within the jurisdiction of the Australian Commission for Law Enforcement Integrity (ACLEI).

These agencies include:

- Department of Home Affairs (multiple accreditations since 2006)
- Australian Criminal Intelligence Commission (ACIC) (accredited since 2014)
- Australian Federal Police (accredited since 2017)

Over the past 15 years, Veritas has provided identity and background checking services and solutions in support of thousands of organisations in every state and territory across Australia to support key industries' ability to operate effectively, securely, and efficiently while achieving Regulatory compliance. Key industries supported include:

- Agriculture
- Aviation
- Education
- Health Services
- Maritime
- Mining and Resources
- Offshore
- Pharmaceutical Product Manufacturing
- Professional Services
- Transport & Logistics

Within these programs, Veritas typically works as an interface between the public seeking credentials and the federal law enforcement agency. For example, in the case of the issuance of Nationally Coordinated Criminal History Checks (NCCHC) obtained through access of the ACIC's National Police Checking Service (NPCS), Veritas:

- Obtains informed consent from the applicant;
- Collects identity documentation and verifies the applicant's identity;
- Submits the necessary information into the ACIC system using the authorised means;
- Issues results to the applicant in the prescribed manner and formats.

In the above example, Veritas is commercially bound to operate within the terms and conditions set forth by the ACIC. In other programs, Veritas is governed by the relevant Acts or Regulations under which the programs fall (e.g. Aviation Transport and Maritime Transport and Offshore Facilities Security Acts and Regulations).

Veritas is of the view that the relevant terms, Acts or Regulations under which it operates as an external service provider to law enforcement agencies does not create increased corruption vulnerabilities (i.e. more vulnerabilities than if the law enforcement agencies undertook those same functions).

Within each of the programs it participates, Veritas understands that it must operate within environments whereby the government agencies are responsible for ensuring the governance of their systems, structures and approaches, are consistent with any applicable legislation.

Veritas offers the following considerations that could be undertaken within the existing governance frameworks to minimise risks of corruption vulnerabilities. These include:

1. Increase the transparency of actions undertaken by external service providers to increase the level of governance on the delivery of services and operations by external providers.

Quality Assurance programs establish and maintain set requirements for developing, manufacturing, or delivering reliable products and services. A quality assurance system focuses on increasing customer confidence and an organisation's credibility, while also improving work processes and efficiency, to ensure the deliverables meet the program purposes.

The Australian National Audit Office (ANAO) maintains a key strategic planning document¹ to ensure that its Quality Assurance Framework supports delivery of the appropriate standards and applicable legal and regulatory requirements and reports.

Requiring industry participants to achieve accreditation to international standards for Quality Assurance would assist government by putting in place the appropriate controls to deliver against the ANAO's performance requirements. In collaboration with the ANAO, developing audit quality indicators that measure external providers' target benchmarks against the ANAO's target benchmarks could provide transparency with respect to the processes, policies and procedures that support relevant elements of the ANAO Quality Assurance Framework.

The following three standards are applicable as to external providers and could assist in reducing vulnerabilities to corruption:

- **ISO 9001:2015 (Quality Management Systems)** is an internationally recognised standard that specifies requirements for a quality management system. By demonstrating accreditation to this standard, organisations can be independently assessed as demonstrating the ability to consistently provide products and services that meet customer and regulatory requirements.
- **ISO 27001:2013 (Information Security Management Systems)** is the international standard for information security. This accreditation sets out the specification for an information security management system. The standard includes "Segregation of duties"² as a risk mitigation strategy.
- **ISO 37001:2016 (Anti-bribery Management Systems)** is the international standard that allows organisations of all types to prevent, detect and address bribery by adopting an anti-bribery policy, appointing a person to oversee anti-bribery compliance, training, risk assessments and due diligence on projects and business associates, implementing financial and commercial controls, and instituting reporting and investigation procedures.

¹ <https://www.anao.gov.au/work/corporate/quality-assurance-framework-and-plan-2020-21>

² ISO27001 Annex A.6.1.2 "Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets."

2. Increase the vetting of external service providers to ensure appropriate levels of capability of can be delivered to meet the expected outcomes.

Veritas is involved in several programs as an external service provider to government agencies for the verification of identity and background checking services. In these programs, external participants exchange data electronically with the government agencies.

Governance frameworks can be used to structure and delineate levels of authority for participants. Frameworks support the setting of rules, procedures, and other informational guidelines as well as define, guide, and provide for enforcement of these processes.

ISO 31000:2018 provides guidelines on managing risk faced by organisations. A standard approach to risk management, consists of three main phases: risk identification, risk analysis, and risk evaluation.

By taking a risk-based approach, government agencies could assess external service providers' ability to meet the agencies' program objectives which in turn are mapped to external service provider requirements and reduce vulnerabilities to corruption from external service providers.

3. Government's changing of the norms to balance legal and behavioural approaches.

In 2015, the 13th United Nations Congress on Crime Prevention and Criminal Justice developed practical teaching guides ³ that provide concrete actions to advance responses addressing crime prevention, strengthening criminal justice and promoting the rule of law and international cooperation.

This Congress agreed that as governments around the world change the legal anti-corruption norms for companies, this in turn incentivises businesses to adopt ethics and compliance programs that in turn contribute to detecting and preventing corruption to avoid sanctions and reputational damage.

Implementing such a solution requires a multi-faceted approach which involves both government and the business community. This approach includes legislating stricter and more nuanced laws that incentivise companies to strengthen compliance while promoting the importance of corporate values which in turn contribute to building an ethical culture.

³ <https://www.unodc.org/e4j/en/anti-corruption/module-5/key-issues/preventing-private-sector-corruption.html>

Ultimately, developing an effective compliance program that goes beyond mere compliance and includes ethical business practices should include internal, external and collective measures. These might include:

- Holding business leaders personally accountable for their actions and those actions of their organisations. Ethical behaviour is everyone's responsibility; this acknowledges that Leadership is driven from the top.
- Ensuring that guiding values and commitments make sense and are clearly communicated at every appropriate opportunity. This might include promotion of this approach via industry bodies to foster acceptable and appropriate codes of ethics and guidelines. This might include licensing.
- Incorporation of risk assessments to monitor and understand how limited resources are managed as effectively as possible to mitigate vulnerability risks.
- Fostering of working groups to bring government agencies and the external providers closer together. Example: the sharing of the impacts of legislative changes on day-to-day business challenges which in turn can lead to difficult situations and grey areas.
- Promotion of internal controls and channels for enabling the reporting of unethical behaviours or issues (e.g. protect and encourage whistleblowing).

When government and industry work in partnership, this approach incentivises corporate stakeholders which include staff and customers, shareholders, business partners, and the wider community to achieve even higher standards of integrity and ethical business practices than the imposition of mere rules can enforce. The failure of not achieving this can significantly impact the ethical standing of businesses in the community in lightning speeds.

4. Balancing Risks of Corruption: Efficiency Gains and Cost Savings to Government.

It is a legitimate question to ask whether the risk of corruption increases as a result of contracting services or functions by law enforcement agencies to external service providers particularly when balancing the efficiency gains and cost savings to government. Certainly, government should evaluate each program on its own merits and risks.

A pertinent example is the case of Veritas providing the interface with those persons/organisations seeking identity verification and/or background checks. Over its nearly two decades of involvement in this industry, Veritas has developed considerable technology an intellectual property for streamlining productivity and yielding efficiency and cost gains for both individuals, organisations, and government.

In its experience, the number of external service providers participating in programs has risen in some cases and declined in others. What has emerged as a consistent theme and in

turn directly impacts levels of program participation are the audit requirements (from both government and independent auditors on behalf of external service providers). As the levels of oversight and compliance increase, program participation from external service providers has decreased. Veritas is of the view that this has had a positive impact on program compliance.

What is perhaps unknown is the degree to which industry has contributed to positive acceptance of programs requiring high levels of engagement with persons. Finding the optimal level of program participation by external service providers should therefore be considered by government.

Alternatively, should government choose to minimise the “contracting” of services to industry, understanding how this may impact public sentiment for each program should be considered.

In drawing on a recent example of a similar, albeit not directly related, recent government initiative, it can be noted that in establishing the Trusted Digital Identity Framework, the Australian Government “agreed to work across government **and with the private sector** to develop a Trusted Digital Identity Framework to support the Government’s Digital Transformation Agenda” (emphasis added). A key reason for doing so was to “streamline people’s interactions with government and provide efficiency improvements.”⁴

Balancing Risks of Corruption: Industry Development.

Similar to the example above, the public will hold similar expectations of government and industry organisations working together in the delivery of identity services. Engaging industry to deliver portions of the process contributes to the development of local industry development. In the case of Veritas, this might be seen in terms of IT and emerging technologies including biometrics, artificial intelligence, cyber security, etc.

An approach similar to that of a Public-Private Partnership can yield positive results for all parties. Delivery of improved services and better value for money can be achieved through appropriate risk transfer, encouraging innovation, greater asset utilisation and an integrated whole-of-life management underpinned by private financing.

Given the nature of the services Veritas currently delivers as an external service provider to law enforcement agencies, enhancing the accountability framework can help to minimise vulnerabilities for corruption. This framework could consider:

⁴ Digital transformation Agency – TDIF: 02 - Overview

- Improving the quality and frequency of engagement by the government and independent agencies;
- Expanding oversight and safeguards for critical issues such as Privacy and Cyber Security;
- Increasing the capabilities to audit provide depth to audits;
- Developing greater transparency.

From a high-level perspective, the outputs provided in these identity/background check programs (e.g. identification cards, reports, etc.) whether produced by government or industry use commercially available (albeit high-end) production systems to minimise costs.

Government and industry should share the responsibility to minimise security risks and minimise corruption vulnerabilities. This can best be achieved through the raising of the levels of security protection across the security categories of governance, personnel security, physical security, information and cyber security.

Reducing the level of security in one or fewer categories without the inclusion of both government and industry, can risk leading to the achievement of suboptimal results.

In summary, as an industry participant, Veritas believes that the decentralising of service provisions encourages industry and public ownership for addressing issues regarding both national security and crime and corruption.

Furthermore, Veritas is of the view that the “contracting” of services or functions (for which Veritas is accredited to be involved in) by law enforcement agencies to external service providers need not create an increased corruption vulnerability. Governance, oversight and quality assurance measures should be applied across all participants, both public and private.

Please feel free to contact me direct for any questions or comments relating to this submission on

[REDACTED]

Regards,

[REDACTED]

Stephen Inouye CPEng GAICD
Managing Director