



INTELLIGENCE ASSESSMENT

EMPLOYEE AND CONTRACTOR FRAUD PRACTICES:
COLLABORATION BETWEEN 'TRUSTED INSIDER' AND ICT SERVICE
PROVIDERS IN THE COMMONWEALTH GOVERNMENT

Date: 13 March 2020

PROMIS # 10333354

Information current at: 13 March 2020

Summary

A review by Australian Federal Police (AFP) Intelligence of recent referrals to the AFP reveals a fraud practice currently posing a risk to the Australian Government. The fraud methodology has been identified within government agencies that access AusTender panel providers¹ for recruitment services specific to the recruitment of Information and Communications Technology (ICT) contractor services. The fraud is achieved by overcharging the government agency for the true value of ICT contractor services. (For Official Use Only)

The fraud relies on a series of deconstructed interdependencies, commencing with a government employee in the role of 'Trusted Insider' who manipulates a recruitment process. The fraud involves employment of a low-skilled ICT contractor being paid at high-skilled services rates. The contractor does not receive the full value of the high-skills payments, as excess funds are skimmed off and paid back to a third party during payment processes. The Trusted Insider² will likely have influence in selection and recruitment, and remain connected to oversight of the contractor's employment i.e. time-recording and overtime claims. The multiple movement of payments from the government agency, to recruitment provider, then a Payroll Services Provider (PSP)³, and finally to the contractor allow the fraud to be obfuscated. The Trusted Insider is the principal of the fraud and the PSP facilitates the fraud. The contractor may be unaware of the excessive amounts claimed in the fraud. (FOUO)

Common administrative constructs⁴ used by contractors to service the Australian Government, make it likely that this methodology is being shared and replicated in the ICT contractor cohort. It is unlikely that existing fraud activity is being identified through standard audit or performance reviews. (FOUO)

¹ AusTender Australian Government panel service providers – Department of Finance www.tender.gov.au

² Current referrals identify Trusted Insiders as Executive Level permanent fulltime employee in Australian Public Service.

³ Provides payroll services to the contractor. Holds an Australian Business or Company Number (ABN/ACN).

⁴ Training environments, payroll service providers, independent specialist recruitment providers and/or sub-contract providers.

This document is the property of the Australian Federal Police (AFP). It may not be copied or disseminated to any third party without prior AFP approval. To arrange approval, please contact the AFP [redacted] This information must be stored, accessed and handled in accordance with the Australian Government PSPF information security management protocol and guidelines.

Scope

This intelligence assessment outlines fraud methodology within Australian Government agencies. The assessment specifically describes fraudulent activity, occurring alongside the legitimate service provision process used to engage ICT contractors for government. The assessment does not identify individuals or entities. (FOUO)

The purpose of the assessment is to inform the Australian Government of identified methodology, in order to support disruption of current activity and deterrence of future fraud opportunity. This assessment outlines fraud methodology in order to connect risk, threat, costs and resource implications, corrupt internal environments and adverse consequences for ICT project delivery in the Australian public sector. The assessment considers the role of the Trusted Insider, the role of facilitators and various mitigation strategies currently available. The assessment considers adverse impacts but does not design a proposed solution. (FOUO)

The fraud methodology may perform similarly in other specialist service provision context, but these contexts are neither identified nor considered in this assessment. (FOUO)

Background

The AFP received two fraud referrals in 2018-2019, in which methodology was recognised as having previously been used in ICT procurement contractor fraud against a government agency during 2017-2018. The AFP anticipate receiving a future referral in 2020. The frauds are perpetrated against Australian Government agencies at work locations in Canberra. The identified ICT contractors have each been sourced through a Canberra office of a recruitment provider that is an authorised AusTender panel supplier. (FOUO)

Financial loss to the Commonwealth - from identified fraud using this methodology during 2017-2019 - is conservatively estimated to exceed \$1.5million in fraudulent claims and overpayments. (FOUO)

The fraud appears most prevalent in ICT service environments related to Systems, Applications and Products in Data Processing (SAP). SAP is an enterprise resource planning software commonly used throughout Australian Government. It is not known how many ICT environments may be affected by this fraud type. (FOUO)

Due to the subtle nature of the fraud - which makes it difficult to identify - no reports are known to have been generated by an internal audit, compliance area or performance review mechanism. Reports of fraud, particular to this methodology, have been made by an observant employee manager or conversely from a disenfranchised employee making a public interest disclosure.⁵ (FOUO)

⁵ *Public Interest Disclosure Act 2013*

Environmental Context: Common Procurement Elements

The following elements form the basis of a standard ICT contractor procurement process:

ICT contractors are recruited to work in a government agency through **recruitment providers** that are registered members of an **AusTender procurement panel**. The panels are administered under the Department of Finance, and members of a panel are approved, under this arrangement, to act as a supplier of services to government. Specialist panels are used to fulfil various services to the Australian Government; for example recruitment, electrical and building maintenance. Individual business entities act as suppliers to the panel. The supplier must first be approved and qualified, before being accepted on the panel, and will be limited by the panel description as to what goods and services they can provide. Suppliers cannot abridge panels – they must submit a separate application for each panel they wish to join. The purpose of panel providers is to negate bureaucratic delays, avoid procurements duplication across agencies and facilitate access to common services required by government. A supplier of recruitment services receives a fee, and ongoing commission payments, from the government agency when their proposed candidate is selected. (Unclassified)

Contractors commonly use a **Payroll Services Provider (PSP)** to provide employment support services. These may be services provided to an individual or group arrangement. The PSP will hold an Australian Company Number (ACN) or an Australian Business Number (ABN) which the contractor uses to supply services to government. The primary function of a PSP is to manage employment income for the contractor, who is their client. Within the contractor environment, a PSP acts as intermediary between the government agency, recruitment provider and the contractor. The PSP receives payments on behalf of the contractor whilst also making disbursements such as superannuation and taxation. The PSP may arrange other services including insurances or work cover. The PSP is likely to provide similar services to many contractors for which the PSP is paid a commission fee – usually a percentage deducted from gross payment. PSP is a legitimate service commonly used by individual contractors who do not have an ACN/ABN. The contractor is responsible for paying their own PSP fees. (U)

A PSP may also operate as a **labour hire company** (recruitment services). Labour hire services and payroll services may exist in the same business environment such as a 'one-stop shop' for contractors, but the services provided by each function are separate and distinct. (U)

A **contractor** is an entity who has agreed to provide services under contract, or through a contracted arrangement. A contractor may be an individual or company, but must have access to the ACN/ABN to be able to invoice supplier services to government, and receive payments for those services. A contractor is not classified as an employee for the purpose of paid salary, superannuation, taxation or work cover. Individual contractors are required to manage their own salary arrangements and typically this is why individuals employ a PSP. Each contractor, or employee of a contractor, is subject to APS conditions of employment such as adhere to the Australian Public Service (APS) Code of Conduct and maintain a valid security clearance. (U)

The Australian Government Security Vetting Agency (AGSVA)⁶ provide security clearance vetting services to government agencies for employees and contractors who require a clearance for working with the Australian Government. During any period of employment, a government agency will perform the role of sponsor to the security clearance holder. The clearance remains valid only while it is sponsored. There are reporting obligations for the holder of an AGSVA security clearance, which include reporting changes of personal circumstances and major financial transactions such as inheritances or buying or selling of assets. The security clearance holder must declare all conflicts of interest, secondary employment, income streams and business interest arrangements. This is known as self-reporting. Failure to self-report can result in a security clearance be down-graded or withdrawn by AGSVA. Where the contractor is a company, each individual employee of the contractor must have a security clearance. (U)

AGSVA will accept **third-party reporting** at any time from the sponsor, either during or after the employment term. A third-party report contains information or intelligence about the security clearance holder. When an employee or contractor ceases employment, the Agency is required to notify AGSVA that they no longer function in the role of sponsor. The sponsor is expected to notify AGSVA of any adverse behaviours during the period of employment in order to inform future risk assessments which may affect suitability for employment. AGSVA do not suspend a clearance unless notified by the sponsor. When notified of employment cessation, AGSVA place the security clearance into a hiatus phase until it expires or is enlivened by a new sponsor. (U)

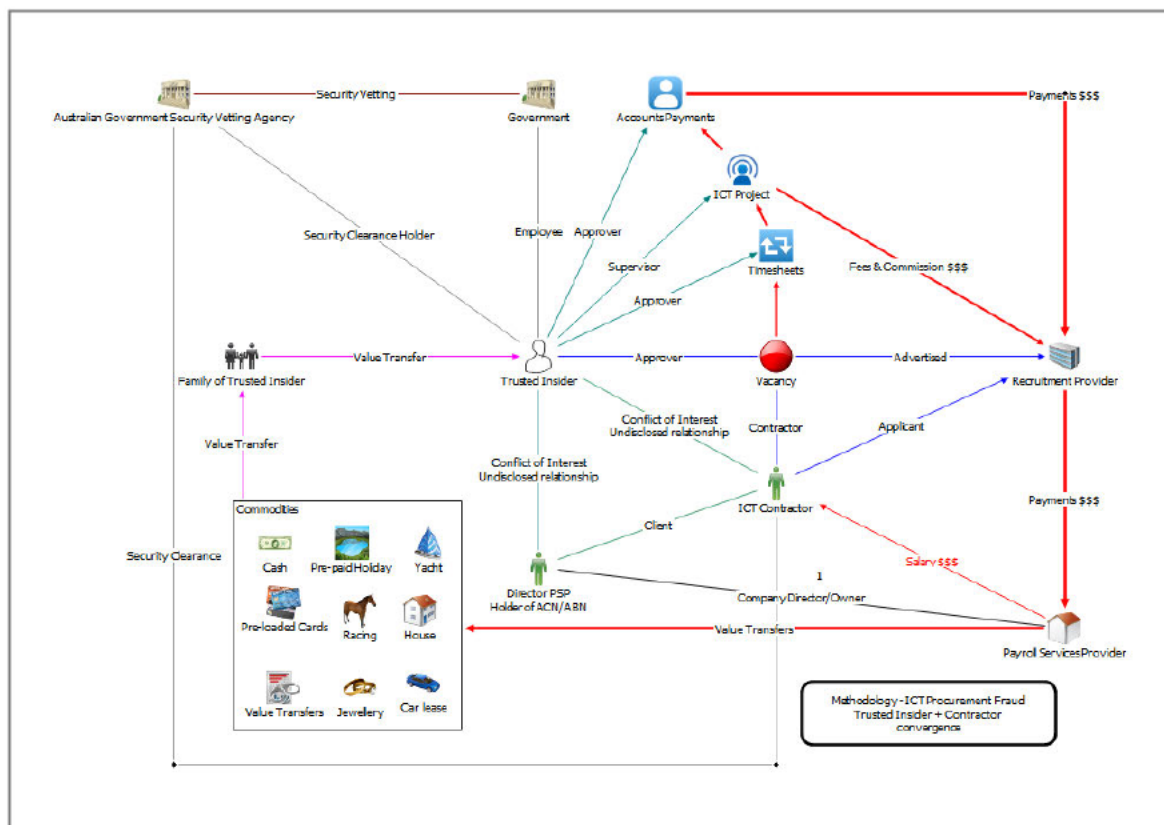
AGSVA accept third-party intelligence and information reports beyond those from the sponsor. They can come from a variety of sources such as an independent person, a government agency, a law enforcement agency, a court, a family member, a neighbour, an employee or a colleague. A third-party report might describe knowledge of situations, events, dubious behaviours or suspicious circumstances which are related to the security clearance holder. AGSVA use a variety of methods to capture third-party reports as part of ongoing monitoring, security and risk assessments. Third-party reports are anonymous. (U)

⁶ *Understanding Security Clearances*, Department of Defence, www.beta.defence.gov.au

Fraud Methodology: Key Enablers

The fraud referrals received by AFP contain the following essential elements:

- A. A Trusted Insider in a position of influence or authority connected to an ICT work project within an Australian Government agency;
- B. A contractor employee who has unverified or low skills, fake academic credentials and/or manufactured employment history and who uses the services of a PSP;
- C. A corrupt PSP, or similar behaving entity, with a registered ACN/ABN who provides employment service to the contractor. The PSP has an undisclosed relationship with the Trusted Insider;
- D. A legitimate recruitment provider that is an authorised supplier on an AusTender panel; and
- E. An advertised vacancy for an ICT contractor position, being managed through a legitimate recruitment provider and where the Australian Government agency is the client. The Australian Government agency is represented and/or the process is influenced by the Trusted Insider. (FOUO)



Simplified depiction of ICT procurement fraud methodology (FOUO)

This document is the property of the Australian Federal Police (AFP). It may not be copied or disseminated to any third party without prior AFP approval. To arrange approval, please contact the AFP [redacted]. This information must be stored, accessed and handled in accordance with the Australian Government PSPF information security management protocol and guidelines.

Fraud Methodology: Production

1. The Trusted Insider and PSP have an undisclosed relationship known only to themselves;
2. The contractor has a connection, prior to employment, to the Trusted Insider and/or the PSP ;
3. The contractor has prior knowledge – either by Trusted Insider or PSP - of an anticipated ICT vacancy and knowledge of which recruitment provider will advertise the vacancy;
4. The contractor acts on the prior knowledge, and registers with the nominated recruitment provider;
5. The vacancy is advertised through one, or more, recruitment providers, who perform the usual service of bidding and putting forward proposed candidates in a selection process to the government agency;
6. Targeted recruitment of the contractor is enacted by the Trusted Insider in progressing the recruitment of the contractor, on a high-skills salary despite the contractor being a low-skills candidate. The Trusted Insider might provide coaching to the contractor; supply answers to candidate interview questions; request the contractor by name or reputation; submit a request for specialist or unusual skills base which are unnecessary for the position, but which are skills specific to the contractor;
7. The Trusted Insider will insist on recruiting the contractor, even where other more suitable candidates are available, and pursue the recruitment despite advice from the recruitment provider that the contractor is unsuitable;
8. The contractor is ultimately employed in a position rated above their skills and experience and, probably unbeknown to the contractor, at a very high-skills salary rate;
9. The Trusted Insider has influence in the recruitment process, knowledge of the salary rates and fees and ongoing involvement in approvals, timesheets and payment claims related to the contractor;
10. The Trusted Insider recommends the PSP as a preferred payroll services provider and subsequently, salary payments are made to the contractor via the PSP;
11. The Trusted Insider, the recruitment provider and the PSP each know the total value of the contract arrangement, but are unable to see individual transactions or money-flow;
12. The recruitment provider receives ongoing commission and fees for sourcing the contractor and managing the employment contract to the government agency;
13. The recruitment provider knows the value totals paid to the PSP, but does not have oversight of final values paid to the contractor. This is because the payments are received and adjusted by the PSP;
14. The PSP makes lower value payments to the contractor; and
15. The PSP retains the difference between high-value receipts and low-value payments. The PSP then returns a benefit to the Trusted Insider through various forms of value transfer⁷. (FOUO)

⁷ Cash, shares transfer, high-value goods, pre-loaded credit cards, pre-paid holiday, school fees, rent, hire and/or lease payments.

Fraud Methodology: Detection

The identified frauds are each cleverly constructed, managed and difficult to detect. It is not likely that they are being identified through either internal audit or compliance reviews. (FOUO)

The known frauds have been identified by a government agency when:

- A contractor realised that there was a larger financial gain being made beyond the contractor's current payment. Being disgruntled by this, the contractor made a public interest disclosure, revealing the fraud and naming both the trusted insider and PSP; or
- An observant manager came to an empty workplace on a weekend. The next week that same manager received ICT contractor overtime claims. The manager queried the overtime claims, and reviewed other claims that had come before, and unravelled the fraud. (FOUO)

Analysis

The key element to the fraud is the role of the Trusted Insider and facilitation of the fraud by the PSP. The fraud success is dependent on obfuscation of payment flows where public and private contracts converge, and where there is no oversight by either the government agency or the recruitment provider. (FOUO)

Fraud constructed using this methodology is difficult to identify. The fraud is likely to go unnoticed for an extended period of time resulting in high costs, low quality production, expanded project time frames and subsequently the delayed delivery of goods and services to the Australian Government. The broader implications are the germination of corrupted work environments, cronyism, nepotism and opportunities to further influence and perpetuate fraudulent behaviours among the ICT contractor cohort. The behaviour and methodology may migrate to - and be adopted by - other government contractor cohorts. (FOUO)

The described fraud is highly likely to generate inflated costs and delayed project delivery when there are multiple low-skills level contractors employed on a significant work project. This is most likely to occur in large departments, or when a highly skilled labour force is necessary to deliver whole-of-government programs. In order to deliver a large work project with replacement low-skilled employees, the Trusted Insider must, by necessity, extend the project time-period in order to achieve outcomes. Alternatively, they can use existing high-skills labour more intensively, which also results in large overtime claims and payments. In either case, it is to the financial benefit of the Trusted Insider to have multiple low-skills contractors working on an extended work project timeline, in order to maximise financial gains made on each contractor through the fraudulent arrangements. (FOUO)

It is highly probable that any involved employees and contractors could not be considered 'fit and proper persons' for ongoing employment in the Australian Government. The fraud is perpetuated, in part, through manipulation

and exploitation of control mechanisms which are set in place expressly for the purpose of mitigating corrupt practices in the Australian Government. The persons of interest within these frauds have failed to disclose significant financial dealings, conflict of interest or significant business relationships to either the agency or to AGSVA as required under security reporting obligations. The actions of all parties breach the APS Code of Conduct, *Public Governance, Performance and Accountability* (PGPA) Act and the criminal code.⁸ (FOUO)

It is highly probable that a corrupt PSP will provide companion criminal services in support of committing fraud against the Australian Government, not limited to the ICT environment, and which may include cartel behaviours and money laundering. The PSP demonstrates knowledge of the procurement and supplier environment and likely has multiple clients operating under Trusted Insider arrangements. The Australian Government promotes the use of free market supply to government procurement from the panel providers. The fraud participants in this scenario exploit the 'blind-spots' where public sector and private enterprise intersect. The PSP facilitator is clearly aware of these intersections and traverses them to obfuscate fraud. (FOUO)

Conclusion

ICT Procurement is an expensive and ongoing investment in progressive technology upon which government is heavily reliant⁹ to deliver services. The fraud described in this assessment is highly likely to affect Australian Government service delivery with negative consequence for the delivery of large scale ICT infrastructure projects. Immediately apparent is the criminal element of the behaviour, alongside the increased financial impost on agencies who are being defrauded. The Australian Government may be unknowingly reliant on low-skills workers delivering important services and projects across a wide range of ventures. (FOUO)

Egregious behaviours are highly likely to be adjunct in a corrupted workplace such as theft, dishonesty, cronyism, nepotism, bullying, corruption, unauthorised access to government information, honest services fraud, approved delivery of sub-standard services, and cartel behaviours such as market manipulation and price-fixing. (FOUO)

Agencies may find, upon review of previous internal fraud reporting, indications that this methodology and any participants have already been reported under the agency internal fraud reporting mechanism.¹⁰ (FOUO)

Agencies will likely find that working environments and culture are being adversely effected by this fraud, in particular where fraud has been detected but not reported. Legitimate employees receive benefit without being a party to fraud, such as overtime opportunities; simply because they provide the labour skillset required to competently complete a work project. Complicit actions are contributory to normalising a fraud culture and may explain low reports. (FOUO)

⁸ *Criminal Code Act 1995* (Cth), *Criminal Code Amendment* (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth)

⁹ Queensland Crime and Corruption Commission, *ICT Procurement what are the corruption risks?*, Prevention in Focus, August 2018.

¹⁰ Fraud & Corruption Control Plan, Fraud Control Framework, PGPA Act 2013, Attorney-General's Department Canberra 2017

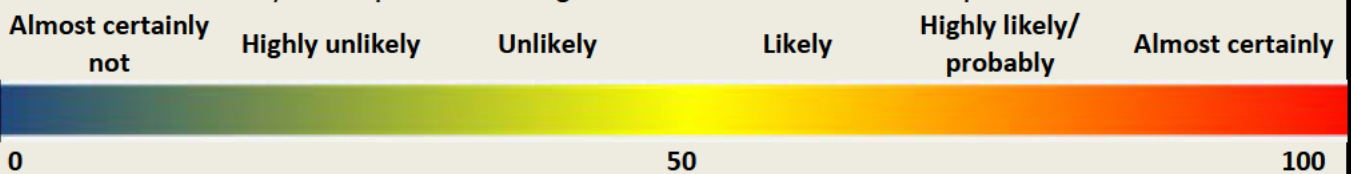
Fraud and other 'white-collar crimes' are generally considered 'victimless crime', however, workplace environments should assess the broader effect where fraud has been found to occur. Legitimate workers may be subject to unfair and harsh treatment under the auspices of a Trusted Insider. These workers may be limited in their ability to progress, because their natural promotion path is blocked by corrupt employment practice. Alternatively, they might have been required to provide unreasonable support to low-skills employee contractors, or threatened by job loss, and been functioning in a fraught work environment where their position is more valuable to the Trusted Insider if it is vacated so as to be occupied by a low-skilled worker. (FOUO)

AFP Intelligence would recommend that:

- Agencies review this fraud methodology and recognise indicators in their environment;
- Agency staff are familiar with third-party reporting to AGSVA and practice rigour in security vetting and reporting so as to prevent the movement of bad actors between government agencies (disruption);
- Agencies who identify fraud or corruption take action in reporting to AGSVA against security clearance holders including withdrawal or cancellation of sponsorship; and
- This assessment be referred to the Attorney-General Department for attention and awareness of the Commonwealth Fraud Prevention Centre. (FOUO)

Estimative Language

Certain words used in this assessment convey confidence and analytical judgement regarding the probability of a development of event occurring. Assessments are often based on incomplete or fragmented information and are not necessarily fact or proof. The image below describes the relationship of the terms to each other.



This document is the property of the Australian Federal Police (AFP). It may not be copied or disseminated to any third party without prior AFP approval. To arrange approval, please contact the AFP [redacted]. This information must be stored, accessed and handled in accordance with the Australian Government PSPF information security management protocol and guidelines.

External Distribution *(list all external domestic and international agency names)*

- Attorney General's Department
- Services Australia
- Department of Finance
- Australian Criminal Intelligence Commission
- Queensland Crime & Corruption Commission
- Australian Government Security Vetting Agency