National Fraud Authority

Procurement Fraud in the Public Sector

October 2011

CONTENTS

1. EXECUTIVE SUMMARY 3

2. INTRODUCTION 6

3. THE NATURE OF PROCUREMENT FRAUD 7
Fraud in the pre-contract award phase 7
Fraud in the post-contract award phase 9

4. CHALLENGES WITH TACKLING PROCUREMENT FRAUD 12
Difficulty in detecting procurement fraud 12
Difficulty in measuring procurement fraud 12
Lack of consistent and proactive risk assessment 13
Absence of a procurement fraud strategy 13

5. THE RESPONSE 14
Immediate interventions 14
Spend and recovery audits 14
Procurement fraud training 14
Changes to Government procurement policy 15
Centralisation of procurement 15
Transparency 16
Lean procurement 17
The medium term strategy 18
A counter fraud culture in public procurement 18
Fraud risk assessments 18
Data analytics 19
Whistle-blowing and fraud reporting 20
Measurement of procurement fraud 21
Sharing information and intelligence 21

ANNEX A – TfL approach to preventing procurement fraud in Crossrail 23

ANNEX B – Acknowledgements 26

1. EXECUTIVE SUMMARY

1.1 Procurement fraud is a complex problem. It covers a wide range of illegal activities from bid rigging during the pre-contract award phase through to false invoicing in the post-contract award phase. It can be perpetrated by those inside and outside an organisation. Procurement fraud is difficult to detect; cases are rarely reported and subsequently it is difficult to measure the extent of the problem. Where fraud is detected, resource is generally channelled into investigation and prosecution which is expensive and rarely ends in a conviction or the recovery of losses. The existing approach to tackling the problem must change, with greater focus placed on preventing this type of fraud.

1.2 Savings can be made now, with little or no cost to the Government. Work undertaken by the Home Office and Department for Transport (DfT) to detect and recover overpayments to suppliers demonstrates an immediate opportunity for other departments and the wider public sector to undertake a similar exercise. Like the Home Office and DfT, commissioning the exercise on a 'payment by results' basis presents a further opportunity of achieving efficiency savings alongside preventing fraud.

1.3 Changes to Government procurement policy and process present a golden opportunity to design fraud risk out of procurement. Centralisation, lean procurement and greater transparency in public spending can all be implemented in such a way as to reduce the fraud risk whilst making the processes quicker and simpler. Designing fraud risk out of procurement processes at an early stage will leave a counter fraud legacy in public procurement.

1.4 The immediate roll out of counter fraud training for procurement specialists and all those involved in the procure-to-pay process presents a third opportunity to make an impact. The experience of the 'Procurement Fraud Taskforce' in the United States demonstrates that fraud awareness training has been an effective intervention. Procurement fraud training should be aligned with the Government's continued drive for professionalism in public sector procurement.

1.5 In the medium term, Government departments and the wider public sector must take a holistic *fraud risk management* approach to understanding and tackling the problem. A counter fraud culture must be embedded amongst procurement specialists, building on the recommended procurement fraud training. Fraud risk assessments should be undertaken to identify and mitigate fraud before embarking on procurement, and the power of data analytics must be harnessed to improve detection of procurement fraud. There needs to be clear and easy ways for staff and the public to raise suspicions of procurement fraud without fear of reprisal on the person reporting their suspicions. Information and intelligence on fraud and fraudsters should also be shared across the entire public sector.

1.6 In summary, this report makes three recommendations for immediate action and a further set of recommendations for the adoption of a holistic strategy in the medium-term.

Immediate action

1. Government departments, agencies and non-departmental public bodies should undertake a spend-and-recovery audit on their accounts payable system to detect overpayments to suppliers. This is a matter of urgency for organisations which will shortly be closing or merging.

2. The Chartered Institute of Purchasing and Supply (CiPS) should work with the Government to develop and deliver a procurement fraud training module for new and existing procurement specialists in the public sector. Consideration should also be given to providing procurement fraud training to staff who audit or assure procurement processes.

3. The Efficiency and Reform Group (ERG) in the Cabinet Office should ensure fraud risk is designed out of processes underpinning policies on transparency, lean procurement and centralised procurement. ERG should consider utilising an independent panel of fraud experts to support this undertaking.

Medium-term action

4. Government departments and other public sector bodies should develop and adopt a holistic approach to tackling procurement fraud:

    a) Procurement fraud training should provide a basis for embedding a counter fraud culture amongst procurement specialists and those involved in the procurement process.

b) Fraud risk assessments should be undertaken to identify and mitigate fraud. In central Government, this should form part of Starting Gate and Gateway reviews on major projects, with the independent panel of fraud experts playing an advisory role. Public bodies should use the Chartered Institute of Public Finance and Accountancy (CIPFA) Contract Audit Toolkit as a framework.

c) Data analytics should be deployed to detect anomalous behaviour. Consideration should be given to adapting analytical techniques to detect insider-enabled procurement fraud.

d) A cross-Government fraud reporting service should be created so that suspicions of procurement fraud can be reported by staff and members of the public. This service should be linked to the National Fraud Intelligence Bureau (NFIB), in order for investigation to be targeted and lessons learned to be properly disseminated to public bodies.

e) Government departments and the wider public sector should assist the National Fraud Authority (NFA) and Cabinet Office in developing the methodology for measuring and reporting procurement fraud in the public sector. Departments should use this as a basis for completing their Quarterly Data Summary.

f) In order to understand the broader picture of procurement fraud, information and intelligence on procurement fraud must be shared with and analysed by the NFIB. Findings must be disseminated to the wider counter-fraud community in order to improve the response to procurement fraud.

2. INTRODUCTION

2.1 Procurement is the process of acquiring goods or services in order to satisfy the needs of a person, group or organisation. In the UK, public sector procurement ranges from purchasing small commodities such as stationery or one-off services such as new street lighting; through to large scale specialist goods such as defence equipment or long-term services such as waste management.

2.2 In 2009-10, central and local Government spent £236bn procuring goods and services. At £150bn, central Government expenditure on procurement was almost a quarter of all Government expenditure during the same period[1].

2.3 In the UK, ERG[2] sets policy and standards for public sector procurement in order to promote fair, open and transparent competition for business. Where the value of procurement is over a certain monetary threshold, public bodies must follow European Union (EU) procurement directives[3].

2.4 Domestic and EU procurement policy provides a framework for mitigating the risk of fraud and other unlawful procurement activities. However, cases of procurement fraud continue to emerge in all areas of public service.

2.5 This report presents research undertaken by the cross-Government Procurement Fraud Working Group (PFWG)[4] to understand how and why procurement fraud occurs in the public sector. It recognises the complexities around detecting and measuring procurement fraud and recommends cross-Government options for tackling the problem.

[1] Source: Government Combined Online Information System (COINS)
[2] Formerly the Office of Government Commerce
[3] Thresholds vary according to the nature of the procurement. More information is available here: http://ec.europa.eu/internal_market/publicprocurement/index_en.htm
[4] A list of members is available in Annex B

3. THE NATURE OF PROCUREMENT FRAUD

3.1 Procurement fraud is a deliberate deception intended to influence any stage of the procure-to-pay lifecycle in order to make a financial gain or cause a loss. It can be perpetrated by contractors or sub-contractors external to the organisation, as well as staff within the organisation.

3.2 The nature of procurement fraud differs between the two core stages of the procurement lifecycle; pre-contract award and post-contract award. Fraud in the pre-contract award phase is complex, often enabled by a lack of compliance with policy, but also involving activity such as collusion and corruption which can be difficult to detect.

3.3 Fraud in the post-contract stage is considerably different. As contracts are already in place, most cases of fraud tend to involve overpayments to contractors, through false or duplicate invoicing, and payments for substandard work or work not completed under contract terms. Sharp practice and unlawful activity can also be present in the margins of post-contract award fraud. Examples of this includes overpricing for goods or services.

Fraud in the pre-contract award phase

3.4 The pre-contract award phase generally involves the core stages of pre-tendering – defining the requirement, developing the specification, producing a business case and tendering – market engagement, bidder selection and bidder evaluation. This phase ends in the award of a contract.

3.5 Fraud during this phase can be complex and difficult to detect. Much of the fraud occurs in an organisation's external environment, either with or without the knowledge of those involved in the procurement process. Examples include price fixing between suppliers to secure business and maximise profit margins and bid-rigging, and 'cover pricing' where suppliers submit false bids to secure who gets business. Such cases have been prevalent in the UK construction and healthcare industries.

Case Study – Supplier 'cartels' and 'cover pricing'

In 2009, the Office of Fair Trading (OFT) imposed fines totalling £129m on 103 construction firms in England. These firms were found to have colluded with competitors to agree over-inflated bids for building contracts with, amongst other organisations, the NHS and schools. This activity is known as 'cover pricing'.

Cover pricing is where one or more bidders in a tender process obtain an artificially high price from a competitor. Cover bids are priced so as not to win the contract but are submitted as genuine bids, which give a misleading impression to clients as to the real extent of competition. This distorts the tender process and makes it less likely that other potentially cheaper firms are invited to tender.

The OFT also found six instances where successful bidders had paid an agreed sum of money to the unsuccessful bidder (known as a 'compensation payment'). These payments of between £2,500 and £60,000 were facilitated by the raising of false invoices.

Case Study – NHS Price Fixing

In the late 1990s, NHS trusts saw a sharp rise in the price of dozens of generic drugs. Generic drugs are up to a fifth cheaper than those under patent. The NHS filed a £150m claim against seven manufacturers accusing them of collusion in order to set artificially high prices for these drugs.

Assisted by a whistle-blower claiming to have attended secret meetings between the suppliers, an investigation was subsequently launched by the NHS and Serious Fraud Office,

No criminal charges have ever been brought, but three of the seven firms have settled out of court without admitting liability.

3.6 A host of domestic and EU policy and guidelines underpin the pre-contract award phase. Public sector procurement specialists and other staff involved in the process are required to follow these in order to promote fair and transparent competition. Over time, the push for continuous improvement has seen the number of policies and procedures grow. This has added a level of complexity to the procurement process, making it somewhat onerous and leading to situations where shortcuts have been taken which lead to the bypassing of fraud controls. PFWG members cited numerous cases of fraud being enabled through a lack of compliance with local or national procurement policy, which suggests that where procurement policy was once a framework for mitigating fraud, it has now, paradoxically, become an enabler to fraud. The Government's efforts to simplify public procurement presents an opportunity for fresh thinking, but care needs to be taken to ensure that important fraud controls are not discarded.

Fraud in the post-contract award phase

3.7 The nature of fraud in the post-contract award phase focuses firmly on contract management, specifically on payments made on contracts. Most public bodies use an electronic accounts payable system, with key controls around separation of duties between requisition, ordering, checking receipt of goods and services and authorising payment.

3.8 Similar to cases in pre-contract award, PFWG members identified cases where these controls were bypassed which enabled fraud to occur. Notable examples involved overpayments to suppliers through the fraudulent submission of duplicate or false invoices which had been unknowingly paid by finance teams. More seriously, there were also cases where staff had colluded with suppliers to raise and process false invoices, often receiving bribes or 'kickbacks' in the process. The following case illustrates an example:

Case Study – Bogus invoicing on existing supplier contract

An Engineer in an NHS Trust colluded with a supplier to submit bogus orders for equipment, supposedly for Trust use. In return for procuring the items under false pretences, the Engineer received items for personal use from the supplier.

An investigation by NHS Protect found that legitimate requisitions had been altered and false orders were found to be valued at £80,000. At the trial, the hospital engineer received a 2.5 year custodial sentence for obtaining property by deception.

A number of weaknesses were identified, the most noticeable being that Requisitioning Officers had too much freedom in choosing a preferred supplier and that authorised requisitions were returned straight to the Requisitioning Officer following authorisation rather than being sent to the supplies department. Finally, goods/equipment received was being booked in by the requisitioning officer, not by an independent person.

3.9 A further example demonstrates how poor controls around the accounts payable system can enable payment fraud to go undetected for some time:

Case Study – False invoicing

A member of the Finance team in a Government department created invoices for a non-existent supplier quoting a virtual office address and fictitious Companies House and VAT registrations. The employee created eight invoices for the supplier, five of which were paid. The employee was a registered approver of invoices and a senior member of the finance management team.

The fraud came to light when the bank to which the funds had been diverted, contacted the department to notify them of unusually high funds and subsequent transactions passing through the individual's bank account. In total, the employee diverted £246,000 to his own bank account.

An investigation ensued and found weaknesses in processes within the department relating to supplier set-up. New suppliers were found to be automatically set up on the payment system simply for submitting an invoice, with no checks being undertaken on the validity of the invoice and company.

The department put in place new controls including a process whereby new suppliers are only placed on the payment system when a member of the procurement team and finance team had approved this. All new suppliers are now approved by the Chief Accountant in the department.

3.10 The key difference with these examples from pre-contract award is the ability to detect fraud, albeit after it has taken place. Most public bodies use an electronic payments system, meaning structured data is produced which can be tracked and audited. With the right analytical approach, fraud can be detected, measured and appropriate action taken.

4. CHALLENGES WITH TACKLING PROCUREMENT FRAUD

Difficulty in detecting fraud

4.1 The complex and diverse nature of procurement fraud means it is difficult to detect. Between 2006 and 2009, Government departments only reported 58 cases of fraud totalling £889,800 during the pre-contract award phase, compared to 246 cases totalling £6,523,200 during post-contract award[5].

4.2 The cases presented in the previous section were detected through non-automated means such as staff identifying anomalies in behaviour and reporting suspicions. This highlights the importance of whistle-blowing as a service for staff and members of the public to report suspicions of fraud.

Difficulty in measuring procurement fraud

4.3 Given the challenges of detecting procurement fraud, there can be little confidence that detected cases reflect the true extent of the threat. In both the public and private sector, accurate losses to procurement fraud remain unknown.

4.4 In January 2011 the NFA published an indicative estimate of £2.4 billion of losses to procurement fraud in the public sector. This estimate is made up of losses of £1.5bn to central Government and £855m to local Government[6]. The figure was calculated by applying a one per cent fraud loss estimate to the procurement spend figure across Government, which was based on an 'at risk' figure used by Ministry of Defence Police to estimate procurement fraud within their 2009 defence expenditure. While it is a useful starting point, extrapolating an estimate from undetected fraud losses remains unreliable.

4.5 As with other fraud, procurement fraud goes undetected, unreported, and therefore unmeasured. The challenge remains to gain an accurate measure of procurement fraud losses in the public sector.

[5] Source: HM Treasury (2006 – 2009) 'An analysis of fraud in Government departments'
[6] Due to rounding, these figures do not total £2.4bn exactly

Lack of consistent and proactive risk assessment

4.6 Awareness and understanding of the nature of procurement fraud forms the basis of preventing this type of fraud. PFWG members highlighted an absence of awareness and understanding amongst procurement specialists as well as the supplier market. Risks are considered, but these are mainly focused on the ability to deliver the project to time, cost and quality, rather than specifically identifying and mitigating fraud risks.

4.7 A lack of awareness and understanding creates an environment where procurement fraud can flourish. If public bodies are not considering the risk of fraud before they embark on procurement, then procurement fraud can go undetected.

Absence of procurement fraud strategy

4.8 Where procurement fraud is tackled in the public sector, it is generally through a traditional enforcement model of investigation, prosecution and sanction. While it is important to punish fraudsters, this approach is time consuming, expensive and often does not result in conviction or recovery of lost funds.

4.9 What is required is a consistent and comprehensive strategy involving all elements of a counter fraud response including prevention, detection, disruption, investigation and sanction.

5. THE RESPONSE

5.1 Going forward, there are three immediate opportunities for intervention, which can save money *and* help design fraud risk out of future Government procurement policy. In the medium term, a holistic 'fraud risk management' approach must be adopted.

IMMEDIATE INTERVENTIONS

Spend and recovery audits

5.2 In 2009, the Home Office commissioned a 'spend and recovery' audit on the organisation's accounts payable system to detect overpayments to suppliers. The provider examined six years of external expenditure and to date has detected and recovered £4m in overpayments on behalf of the department. The Department for Transport (DfT) has since commissioned the same provider to review payments made over six years across the entire DfT family accounts payable systems. Analysis of 2009/10 expenditure has already identified almost £0.5m in overpayments for recovery. The provider expects to identify £8m once the audit is complete on all DfT family systems over six years of spend data.

Recommendation 1

Government departments, agencies and non-departmental public bodies should undertake a spend-and-recovery audit on their accounts payable system, to detect overpayments to suppliers. This is a matter of urgency for organisations which will shortly be closing.

Procurement fraud training

5.3 Since 2006, the US Procurement Fraud Taskforce has trained 36,000 procurement specialists, auditors and prosecutors to tackle procurement fraud. They view procurement fraud training as crucial to detecting, investigating and prosecuting fraudsters.

5.4 The British Airports Authority (BAA) take the same view, and run fraud awareness training programmes with forensic auditors which all procurement staff attend. BAA also publicises fraud cases, which it believes has a positive impact on supplier behaviour.

5.5 In the UK, the Chartered Institute of Purchasing and Supply (CiPS) is ideally positioned to develop and deliver such a programme of training. CiPS provides training and qualifications for procurement professionals across all sectors and the Government remains committed to a professional, skilled procurement workforce in the public sector. Such training would raise the awareness of fraud risk amongst procurement specialists and help establish a counter fraud culture in the specialism.

Recommendation 2

CiPS should work with the Government to develop and deliver a procurement fraud training module for new and existing public sector procurement specialists. Consideration should also be given to providing procurement fraud training to staff who audit or assure procurement processes.

Changes to Government procurement policy

Centralisation of procurement

5.6 In 2010, Sir Philip Green undertook a review of the efficiency of Government spending. The Green Review highlighted a number of inefficiencies in public procurement, some of which were due to departmental autonomy over purchasing. He recommended that the Government should leverage its purchasing power by seizing opportunities to procure as a single entity.

5.7 The Green Review has prompted a number of changes to Government procurement which are currently being led by ERG. Spending on ICT contracts above £5m now require central approval and the new Major Projects Authority (MPA) oversees large-scale projects which will be centrally funded and managed. Nine categories of common goods and services will be procured centrally from October 2011.

5.8 The transition to these new processes and systems creates a significant opportunity to design processes and procedures that reduce the risk of fraud. Centralised procurement will mean fewer contracts to process but these contracts are likely to be more significant in size and value. Therefore, should fraud occur, the losses will significantly increase. Conversely if the policy environment and internal controls are robust they will protect a larger segment of the Government procurement spend. This shows the importance of performing a risk assessment of the new processes at the outset, which achieves the right balance between efficiency and fraud control.

5.9 This presents an opportunity for a new independent panel of counter fraud experts to advise the MPA on designing fraud risk out of the transition to centralised procurement and the resultant crown contracts.

Transparency

5.10 Since early 2011, Local Authorities have been encouraged to publish all spending activity over £500. Central Government departments now publish all spending activity over £25,000. This push for greater transparency over public spending is a positive step in efforts to disrupt and deter procurement fraud. In the OFT case, cartels operated effectively because they were aware of the lack of transparency around public procurement. If the public can see who public bodies are contracting with and how they are spending public money, then an additional layer of detection and disruption can be added.

5.11 However, the introduction of transparency requirements on public bodies has had the unintended consequence of allowing fraudsters to exploit weaknesses in the control environment. The publication of public spending data has also seen a rise in fraudulent requests to change the details of supplier bank accounts. As public bodies have published spending activity on their websites, fraudsters have used this information to exploit weaknesses in protocols. Central Government departments, Local Authorities and Universities have all fallen foul of the fraud. If a fraud risk assessment had been conducted before implementing the policy, the risk could have been identified and steps taken to mitigate the risk, such as refresher training for staff on ensuring requests to change bank details are properly verified before authorisation.

5.12 For local Government, the National Anti Fraud Network (NAFN) acts a hub for the collection, collation and circulation of intelligence alerts on fraud against Local Authorities. Local Authorities were quickly made aware of the 'request to change bank details' fraud by such an alert. If a cross-Government alert system had been in place at an earlier stage then departments could have been forewarned about the multiple attacks being perpetrated by fraudsters. Such intelligence sharing is vital to ensure future attacks are spotted at an early stage and communicated to all other departments. Using a case of post-contract award fraud against a Government department, a similar system of fraud alerts has since been piloted with Counter Fraud Champions in central Government.

Lean procurement

5.13 The outcome of the Green Review has also prompted a re-evaluation of current procurement processes in Government. Typically, Government procurement can take more than 350 days to complete, which is time consuming and expensive for both the procuring body and prospective suppliers. Following a review in 2010, the Government is currently piloting 'lean' procurement principles on a number of procurement exercises in central Government.

5.14 Lean principles present an opportunity for the myriad of policies and procedures currently dominating public procurement to be rationalised and prompt positive behaviour from procurement specialists who will now have no need to bypass existing bureaucracy.

5.15 Lean procurement pilots present an opportunity to assess the risk of fraud and we believe the independent panel of fraud experts should be deployed to help design out fraud.

Recommendation 3

The Cabinet Office Efficiency and Reform Group (ERG) should ensure fraud risk is designed out of processes underpinning policies on transparency, lean procurement and centralised procurement. The independent panel of fraud experts should support ERG in this undertaking.

THE MEDIUM TERM STRATEGY

In the medium term, the public sector should take a more holistic approach to preventing procurement fraud.

A counter fraud culture in public procurement

5.16 A counter fraud culture amongst procurement specialists is important in disrupting and preventing procurement fraud. The complexities around detecting and preventing procurement fraud, particularly in the pre-contract award phase, mean improving the awareness and understanding of the problem amongst procurement specialists must be the first step. Elements of an effective counter fraud culture include awareness of the problem, an understanding of how and why the problem should be mitigated, and the creation of suitable incentives to prevent, detect and report suspicions of fraud. Procurement fraud training will provide a basis for embedding a counter fraud culture.

Fraud risk assessments

5.17 The key to establishing a holistic approach is to ensure fraud risk assessments are undertaken before embarking on procurement. Risk assessments work in two ways. Firstly, they must be undertaken before the procurement process is underway, in order to identify and mitigate fraud risk. Secondly, assessments must be undertaken by auditors once the procurement process is complete – the aim being to detect fraud and take appropriate action.

5.18 In central Government, the Starting Gate and Gateway Review processes for major projects provides a framework in which fraud risk assessment can take place. Starting Gate reviews are undertaken before major projects begin (thus before procurement). If fraud risks are considered at this early stage, the risk can be designed out of the project and subsequent procurement. Once the project is underway, fraud risk assessments can be subsumed within Gateway Reviews, to audit the success of efforts to design fraud out of projects as well as identify new risks which may have arisen along the way.

5.19 In 2010, the Chartered Institute of Public Finance and Accounting (CIPFA), together with Transport for London (TfL), published the *Contract Audit Toolkit*. The Toolkit is designed to assist auditors in detecting and mitigating risks during their audits of procurement and contract management. The Toolkit contains specific measures for identifying fraud in the entire procure-to-pay lifecycle. Since

2009, TfL has used this approach to identify and mitigate fraud risk in the Crossrail programme. An outline of the approach can be found in Annex A.

Recommendation 4

Fraud risk assessments should be undertaken to identify and mitigate fraud. In central Government, this should form part of Starting Gate and Gateway reviews on major projects, with the new independent panel of fraud experts playing an advisory role. Public bodies should use the CIPFA Contract Audit Toolkit as a framework.

Data analytics

5.20 Where structured data on procurement is available, data analytics must be deployed to detect and subsequently prevent fraud. The British Airports Authority (BAA) place data analytics at the forefront of their strategy to prevent procurement fraud. BAA use a forensic auditor to undertake holistic contract audits, which identify areas of efficiency savings as well as potential fraud. On average, the audit identifies eight per cent of potential savings through greater efficiencies and preventing potential fraud.

5.21 Analytics can also go beyond payments and detect links between employees in organisations and criminal networks. The UK Border Agency (UKBA) has used analytical software to identify links between UKBA staff and breaches of immigration controls. Over a period of 18 months, the exercise has detected three cases of serious organised crime, generated 70 cases for investigation by UKBA and led to the reopening of two investigations which had previously been closed. The software has the potential to be adapted to different working environments, and to detect links between employees involved in the procurement process and conflicts of interest within companies or links to wider criminal networks. The software could also be used to identify anomalous behaviours, such as one member of staff regularly authorising payments to the same supplier. Given the presence of insiders across the pre and post-contract award phases, this technology must be exploited further.

Recommendation 5

Data analytics should be deployed to detect anomalous behaviour. Consideration should be given to adapting analytical techniques to detect insider-enabled procurement fraud.

Whistle-blowing and fraud reporting

5.22 Where risk assessments and the use of analytics detect suspected fraud, it is crucial that suspicions are reported and properly investigated. Many public bodies run in-house whistle-blowing services for staff. While this is useful, n-house services sometimes lacks the anonymity necessary to give staff and other persons the confidence to report their suspicions. The NFA's insider-enabled fraud scoping study report identified a need to improve cross-Government fraud reporting mechanisms. Specifically, this includes a single, integrated fraud reporting service for Government where suspicions of procurement fraud can be reported anonymously. Reports should be collated and analysed centrally, in order to understand the extent of the problem and target action. Similar services operate in the NHS and help build a single intelligence picture on which to target investigation.

Recommendation 6

A cross-Government fraud reporting service should be created, so that suspicions of procurement fraud can be reported by staff and members of the public. This service should be linked to the National Fraud Intelligence Bureau (NFIB).

Measurement of procurement fraud

5.23 Where risk assessments are undertaken and data analytics is used more widely, information and data must be used to improve the measurement of procurement fraud losses. Using analytics and risks assessments for fraud prevention purposes also has the potential to generate a measure of prevented losses in procurement.

5.24 In 2011/12, departments will begin recording fraud, error and debt losses via their Quarterly Data Summary. Procurement fraud losses will be one area of fraud loss to be measured and reported upon.

Recommendation 7

Government departments and the wider public sector should assist the NFA and Cabinet Office in developing the methodology for measuring and reporting procurement fraud in the public sector. Departments should use this as a basis for completing their Quarterly Data Summary.

Sharing information and intelligence

5.25 Undertaking risks assessments, using data analytics to prevent and detect fraud, and having an integrated fraud reporting service will generate better information and intelligence on which to understand the full extent of procurement fraud. It is crucial that this is analysed in a single place so that the clearest possible picture of procurement fraud against public services can be generated. In the UK, the NFIB is best placed to receive and analyse data on procurement fraud and public bodies should make every effort to share information and intelligence through NFIB.

Recommendation 8

In order to understand the broader picture of procurement fraud, information and intelligence must be shared with and analysed by the NFIB. Findings must be disseminated to the wider counter-fraud community in order to improve the response to procurement fraud.

ANNEX A – TFL APPROACH TO PREVENTING PROCUREMENT FRAUD IN CROSSRAIL

Background

Crossrail is Europe's largest civil engineering project. It will run for 118 km from Maidenhead and Heathrow in the West, through new twin-bore 21 km tunnels under central London to Shenfield and Abbey Wood in the East. It will bring an additional 1.5 million people within 45 minutes commuting distance of London's key business districts.

Scheduled to open in late 2018, Crossrail will provide an increase of ten per cent in London's public transport capacity with up to 24 trains per hour between Paddington and Whitechapel during the peak. The total funding envelope available to deliver Crossrail is £14.8 billion.

Crossrail is being delivered by Crossrail Limited which is a wholly owned subsidiary of Transport for London (TfL).

TfL has experience of major construction projects and the type of frauds risk associated with such projects. It was assessed that Crossrail would be a very attractive target for fraudsters, particularly organised criminal gangs. Thus it was decided to implement a counter fraud strategy at Crossrail at a very early stage.

Initial Assessments

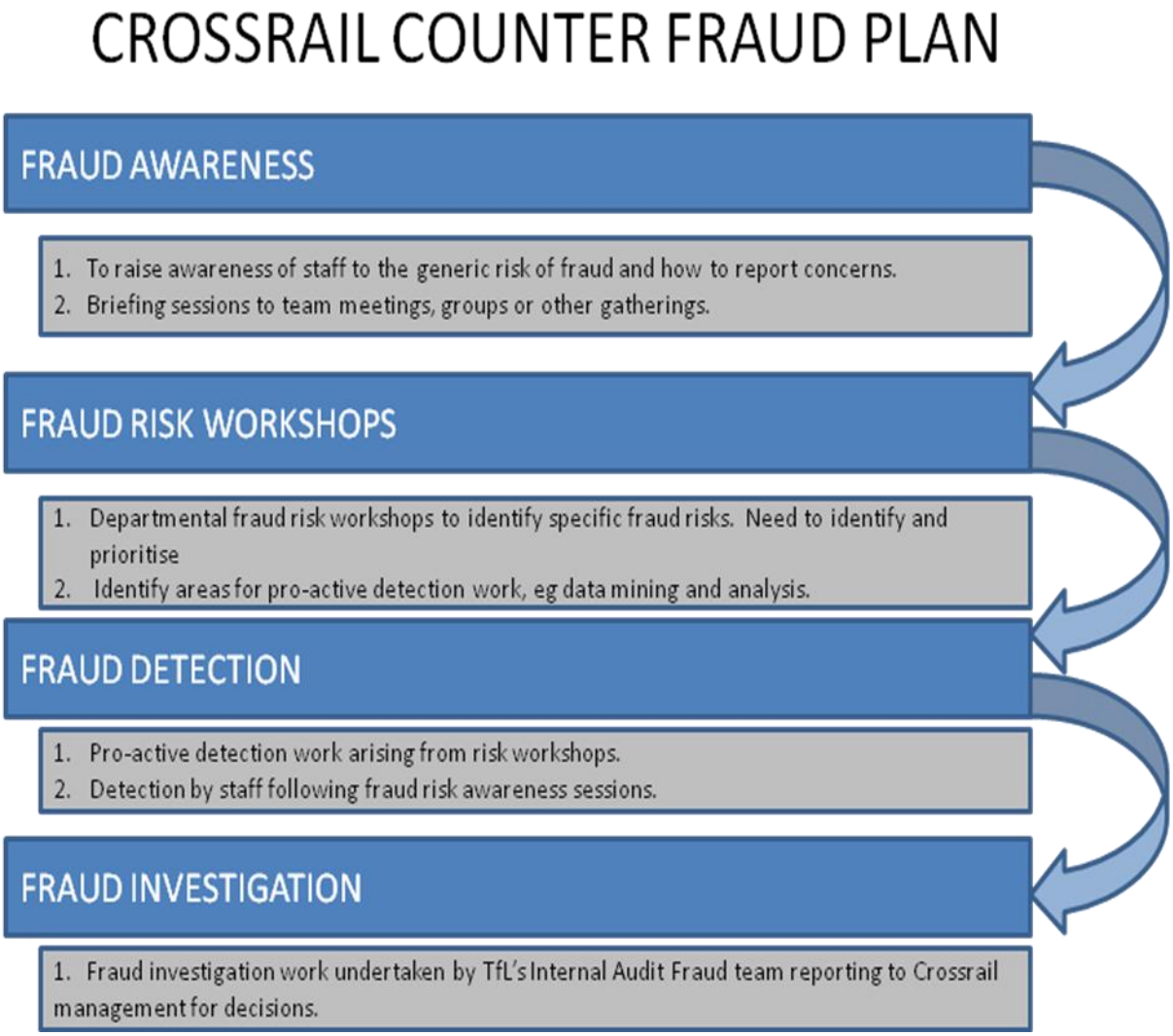
TfL provides fraud prevention, detection and investigation services for and behalf of Crossrail, although the management activities to prevent fraud remain with Crossrail.

A briefing was presented to the Crossrail Executive Committee and fraud was accepted as a strategic risk. It was agreed that the first stage of the approach was to identify the likely frauds that could occur at Crossrail. These were based on the approach used in the production of the Contract Audit Toolkit, produced by TfL and adopted by the Chartered Institute of Public Finance and Accountancy (CIPFA), and were assessed as:

- Contract fraud
- Contractor fraud
- People risks
- Corruption/conflict of interest
- Accounting/financial fraud

Counter Fraud Plan

The Crossrail executive Committee approved the Crossrail Counter Fraud Plan, outlined below:



Initial Action Plan

Using this counter fraud plan as a base, a Crossrail initial action plan was agreed as follows:

Action	Comment/Benefit
Establish a Fraud Risk Assurance Group (FRAG) within Crossrail.	The FRAG would develop and submit for approval to the Executive & Investment Committee (or such other Committee or Sub-committee as appropriate), policies, strategies and procedures to prevent, monitor and report fraud across the Crossrail programme
Promulgate the whistleblowing policy/ process to all staff and contractors.	Demonstrate that Crossrail takes this issue seriously and give staff and contractors the ability to report suspicious activities.
Fraud awareness training / Fraud risk workshops based on the list of fraud risk themes.	The generic assessments above have been supplemented by a series of short workshops with the functional managers to generate risks and controls that are specific to Crossrail. Further workshops and briefings are being rolled out to all staff to raise awareness and develop in-house expertise of fraud risks and the required controls.
Identify areas for proactive detection work, and run analyses based on the output from the risk workshops.	These are being conducted on a regular basis. Analysis is being done initially by the TfL Forensic Data Analyst team with the intention to create reports that can be run by the business area on a regular basis.
Conduct Fraud Risk Management Internal Audit.	Provide independent assurance to the Audit Committee and the Executive that anti-fraud processes are effective, particularly in relation to procurement and payment validation.

ANNEX B – ACKNOWLEDGEMENTS

PROCUREMENT FRAUD WORKING GROUP

- Efficiency and Reform Group, Cabinet Office
- Transport for London
- Audit Commission
- Ministry of Justice
- Home Office
- Chartered Institute of Purchasing and Supply
- Department for Work and Pensions
- NHS Protect
- Westminster City Council (RSM Tenon)
- Department for Education
- Department for Communities and Local Government
- Foreign and Commonwealth Office
- Department for Business, Innovation and Skills
- Ministry of Defence
- Department for Environment, Food and Rural Affairs
- National Audit Office
- Department for Transport
- Her Majesty's Revenue and Customs

OTHER CONTRIBUTORS

- US Procurement Fraud Taskforce
- Metropolitan Police
- British Airports Authority
- Sellafield Ltd.