CPNI
Centre for the Protection of National Infrastructure

# THE SECURE PROCUREMENT OF CONTRACTING STAFF

## A GOOD PRACTICE GUIDE FOR THE OIL AND GAS INDUSTRY

APRIL 2011

**Disclaimer**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

This guidance does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with this guidance does not itself confer immunity from legal obligation. CPNI recommends that organisations seek professional advice, especially on employment law, when implementing or amending their procurement procedures.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Oil & Gas UK
the voice of the offshore industry

UKpia

DEPARTMENT OF ENERGY & CLIMATE CHANGE

# Contents

# Foreword

Oil and gas play an important part in the UK's energy mix and will have a key role in our transition to a low carbon economy. They underpin the delivery of essential services to households and industry, and enable economic growth. Furthermore, supporting over 400,000 jobs, the oil and gas industry continues to make a major contribution to the nation's finances.

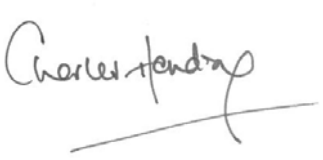
The Department of Energy and Climate Change has responsibilities for energy security. These include working in partnership with the Centre for the Protection of National Infrastructure (CPNI) and industry to ensure that the UK's critical energy infrastructure is secure and resilient to all hazards and threats, including terrorism. Ensuring the security and resilience of the oil and gas industry is a priority for the industry itself and for Government.

The Government's National Security Strategy identified the threat of international terrorism as one of the greatest facing the UK. The threat is relevant to the energy sector: there have been several attacks on energy installations in the Middle East. It is important to ensure that the oil and gas industry is alert to the risk and well informed as to how their assets and networks can best be prepared in order to reduce this risk.

Considerable efforts are being undertaken to manage this risk. It is understood that the implementation of physical and cyber security measures will help reduce the risks to key sites, systems and equipment. It is, however, equally important for all operators to take proportionate steps, through the adoption of appropriate policies and procedures, to manage the risk of staff and contractors exploiting their legitimate access to sensitive assets, information and people.

The benefits of robust personnel security extend beyond counter-terrorism because any workers who use their legitimate access for unauthorised purposes could cause significant financial or reputational damage to a business or other organisations. It is, therefore, important for all operators to incorporate effective personnel security measures into their management procedures and ensure that the relevant parts of business (Human Resources, Procurement, IT and Security) work together to manage these risks.

I am grateful to CPNI for producing this document and thank Oil & Gas UK and the UK Petroleum Industry Association for their valuable input. I hope the guidance this document contains will make a positive contribution to improving the security and resilience of some of this country's key energy assets.



DEPARTMENT OF ENERGY & CLIMATE CHANGE

# Executive summary

**Why is this guidance important?**

Every year, organisations suffer significant financial and reputational losses as a direct consequence of staff misusing their access and privileges. 'Insider' activity ranges from fraud and theft of intellectual property to the sabotage of key sites, systems and equipment. Such unauthorised activities may be carried out by disaffected individuals, single-issue groups, competitors or those with links to organised crime or terrorism. The potential ramifications of insider activity on the safety and security of the workforce are therefore serious.

Organisations within the oil and gas community are regularly obliged to allow a significant number of workers, who are not company employees, to have legitimate access to some of their most sensitive assets. Whilst the engagement of contracting staff is vital to business operations, it can increase the risk of insider activity. Contractors may not necessarily have the same sense of loyalty, nor have been screened by their own company or agency to the same standard as employees of the engaging organisation, nor be managed in ways which enable identification of potential problems before they arise.

This guidance seeks to outline the personnel security provisions which organisations need to put in place with the companies and agencies supplying contract staff in order to reduce exposure to intentional and unintentional insider acts by this section of the workforce.

**Who is accountable and who should read this guidance?**

A number of departments - Human Resources, Security, Legal, Supply Chain or Procurement - may play a role in the engagement of contract staff and these departments should therefore consult the guidance. It is advisable, however, for a single business department to be responsible for the secure procurement of contracting staff.

**How will this guidance benefit my organisation?**

This guidance outlines some practical personnel security measures which organisations can implement to:

- Identify and assess the 'insider' risks posed to an organisation by the engagement of a contractor(s). The proposed model provides a transparent mechanism that promotes proportionate decision-making on subsequent security mitigations;
- Ensure that only trustworthy and competent contracting staff are engaged to work for the organisation;
- Close down opportunities for contracting staff to abuse the organisation's assets once on site;
- Audit and encourage compliance with security provisions throughout the contracting chain.

**Acknowledgements**

The following organisations were instrumental in the development of this good practice guidance:

- **BP**
- **Shell UK**
- **Nexen Petroleum UK Limited**
- **ExxonMobil**
- **Centrica plc**
- **ConocoPhillips UK**
- **Total UK Ltd**
- **AMEC**
- **National Grid**

Wider comments by other parties were also invited by UKPIA and Oil & Gas UK. The expert contributions from organisations and individuals consulted in the development of the guidance are gratefully acknowledged.

# Introduction

This document has been developed by the Centre for the Protection of National Infrastructure (CPNI) in collaboration with Oil & Gas UK, The United Kingdom Petroleum Industries Association (UKPIA) and the Department for Energy and Climate Change (DECC).

### Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

### The National Infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life:

- Communications
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Transport
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

### Oil & Gas UK

Oil & Gas UK (The United Kingdom Offshore Oil & Gas Industry Association Limited) is the leading representative body for the UK offshore oil and gas industry. Membership of Oil & Gas UK comprises companies active in the UK continental shelf. The aim of Oil & Gas UK is to strengthen the long-term health of the offshore oil and gas industry in the United Kingdom. It does this by working closely with companies across the sector, governments and all other stakeholders to raise the profile of the UK offshore oil and gas industry. The organisation promotes open dialogue within and across all sectors of the industry on topics that influence activities, including technical, fiscal, safety, environmental and skills issues, and brokers solutions by developing and delivering industry-wide initiatives and programmes.

**UKPIA**

The UK Petroleum Industry Association (UKPIA) is the trade association which represents the interests of, and speaks for, nine companies involved in the UK downstream oil industry, whose activities cover refining, storage and distribution, and marketing of petroleum products. Its member companies include: BP Oil UK, Chevron, ConocoPhillips, INEOS Refining, Esso Petroleum, Murco Petroleum, Petroplus Refining & Marketing, Shell UK and Total UK.

The nature of these businesses is extremely varied with activities ranging from large, capital-intensive and complex refineries, through storage and distribution to forecourts retailing fuel.

UKPIA's representation focuses on common issues relating to these activities, in non-competitive areas. An important element of UKPIA's role is to inform its members of proposed legislation and related developments, the technical and other impacts, and to help form and advocate the industry's position on these and other issues likely to affect it. UKPIA and its members are also committed to taking a lead role in the delivery of Process Safety standards within the downstream industry.

UKPIA is also responsible for the co-ordination of downstream emergency response in liaison with member companies and Government.

**Department of Energy and Climate Change (DECC)**

The Department for Energy and Climate Change (DECC) is the Government department responsible for all aspects of UK energy policy, including working in partnership with Industry to ensure the UK's critical energy infrastructure is, and remains, secure from disruption either from natural hazards or other threats, including acts of terrorism.

DECC sets the overall approach to protective security, including personnel security, across the energy sector, working closely with the Centre for the Protection of Critical National Infrastructure (CPNI) and the asset owners/operators.

The Governments approach to National Security incorporates the principles of protecting national infrastructure upon which normal daily life in the UK depends. This scope includes the Energy sector, where the most important sites/assets, whose loss would have a substantial impact on the delivery of essential services (electricity, gas and fuel), are deemed to be part of the Critical National Infrastructure (CNI).

The Government has a longstanding programme of work to protect CNI from the threat of international terrorism. This programme is underpinned by the National Security Strategy which identified the threat of terrorism as one of the greatest risks facing the UK.

# Overview: personnel security & secure contracting

## Why is personnel security important for contract staff?

The potential damage that can be caused to an organisation from an 'insider' within their workforce who uses their legitimate access for unauthorised purposes is well documented. Organisations have suffered significant financial and reputational losses as a direct result of such activity, ranging from fraud and unauthorised disclosures of sensitive company information, to malicious sabotage of key sites, systems and equipment.

Every year, however, companies within the oil and gas community must necessarily allow legitimate access to some of their most sensitive assets, sites, information and personnel to a significant number of workers who are not company employees. The use of contractors is common place in the oil and gas industry, providing vital skills and expertise that cannot be developed internally for the same cost or within the same timescales.

**In November 2001, Vitek Boden was sentenced to two years in prison for releasing up to one million litres of sewage into a river and the coastal waters of Maroochydore in Queensland, Australia.**

**Boden had previously worked on the Maroochydore water project as a consultant but had been refused a full-time job by the Maroochy Shire government. He used the internet, a wireless radio, stolen control software and his inside knowledge to carry out the attack on the SCADA system.**

***Press reporting, 2001***

The use of contractors can however also result in an increased personnel security risk, as a contractor's primary loyalty may not be to the organisation that engages them and their commitment to the organisation's security culture may be diminished as a consequence. It is therefore essential that companies put in place effective personnel security policies and procedures that manage the insider risks posed by contractors.

## The definition of 'contractor' and the scope of this guidance

A contractor is defined as an individual who is not an employee of the company, but who has a direct or indirect contractual relationship to provide services to the end user (i.e. the hiring company, referred to in this document as 'the contracting authority'). A contractor may therefore be an individual worker engaged by the contracting authority directly under a contract for services or an individual worker engaged to work for the contracting authority through an agency. Additionally, in large or complex projects, a contracting authority may engage a third party company, as opposed to an individual, to complete a project or supply services. This company will supply their own staff and may in turn recruit further levels of subcontractor or workers.

The provisions of this guidance are aimed towards engagement of a contracting workforce via an agency or engagement of a company which then supplies the 'contractors' to complete the work. Where an individual is directly engaged by the contracting authority under a contract for services, the general principles within this guidance regarding risk assessment, pre-engagement screening levels and ongoing measures do apply. However, it is recognised that the majority of these provisions such as pre-engagement screening will be undertaken or managed in-house by the relevant business area.

## What is personnel security?

Personnel security is a system of policies and procedures designed to manage the risk of staff or contractors exploiting their legitimate access to an organisation's assets or premises for unauthorised purposes.

An effective personnel security regime for contracting staff should therefore cover the entire 'lifecycle' of a contracting worker, providing assurance that:

- Personnel security measures have been applied in a way that is proportionate to the risks, and reduce those risks to an acceptable level;
- The personal information provided by the contractor is genuine;
- Only personnel who are unlikely to present a security concern are allowed to work on the contract;
- The opportunity for the contractor to abuse their access to the organisations assets has been limited as far as possible;
- Measures are in place to detect if a contractor becomes a security concern and processes are in place to manage this accordingly.

## The insider threat, personnel security and the duty of care

There are many individuals and groups who may wish to act as or utilise, an insider within the oil and gas industry, including disaffected employees, single issue groups (such as environmental activists), journalists, commercial competitors, terrorists and hostile intelligence services.

The ramifications of insider activity on the safety and security of the workforce can be

**As organisations implement increasingly sophisticated physical and IT security measures to protect their assets from external threats, the recruitment of 'somebody on the inside' becomes a more attractive option. Insider threat assessments following the imprisonment of five men in 2007 connected with a plot to undertake a bombing campaign in the UK suggest that Al Qaida and associated groups have also recognised the potential value of insiders with appropriate skills and access in the organisations which make up the national infrastructure.**

serious. Companies owe a duty of care to provide a safe place and system of work, to recruit competent personnel and to take reasonable care not to expose employees or workers to unnecessary risk. A breach of this duty could result in criminal sanctions under health and safety legislation and/or civil proceedings.This duty arguably extends to the insider risk and therefore encompasses the engagement and activities of contracting staff.

By carrying out personnel security risk assessments, and embedding personnel security measures into the contractor relationship, companies should have a greater level of assurance about the credentials and integrity of the contracting workforce and thereby be less vulnerable to claims the duty of care in this respect has been breached.

## Who should be involved and who should be accountable?

A number of individuals, groups or departments within an organisation are likely to be involved in the procurement of contracting staff. The most likely departments are Procurement, Human Resources, Security, Legal, Supply Chain, and the relevant business owners/management. These areas are likely to have competing interests with regard to balancing the project costs or the need for swift staff recruitment versus security. It is therefore advisable to make one department responsible and accountable for the personnel security arrangements for contracting staff and for a senior member of staff within that department to be identified to lead the process and work with all relevant parts of the organisation and the contractors to ensure compliance.

## The ‘lifecycle’ of the contractor

The procurement process for the engagement of contractors will differ between organisations, however as a general guide the flow-diagram in figure 1 on the following page illustrates where contracting authorities should be considering personnel security provisions as part of the procurement process for contracting staff.

# Personnel security in the contract cycle

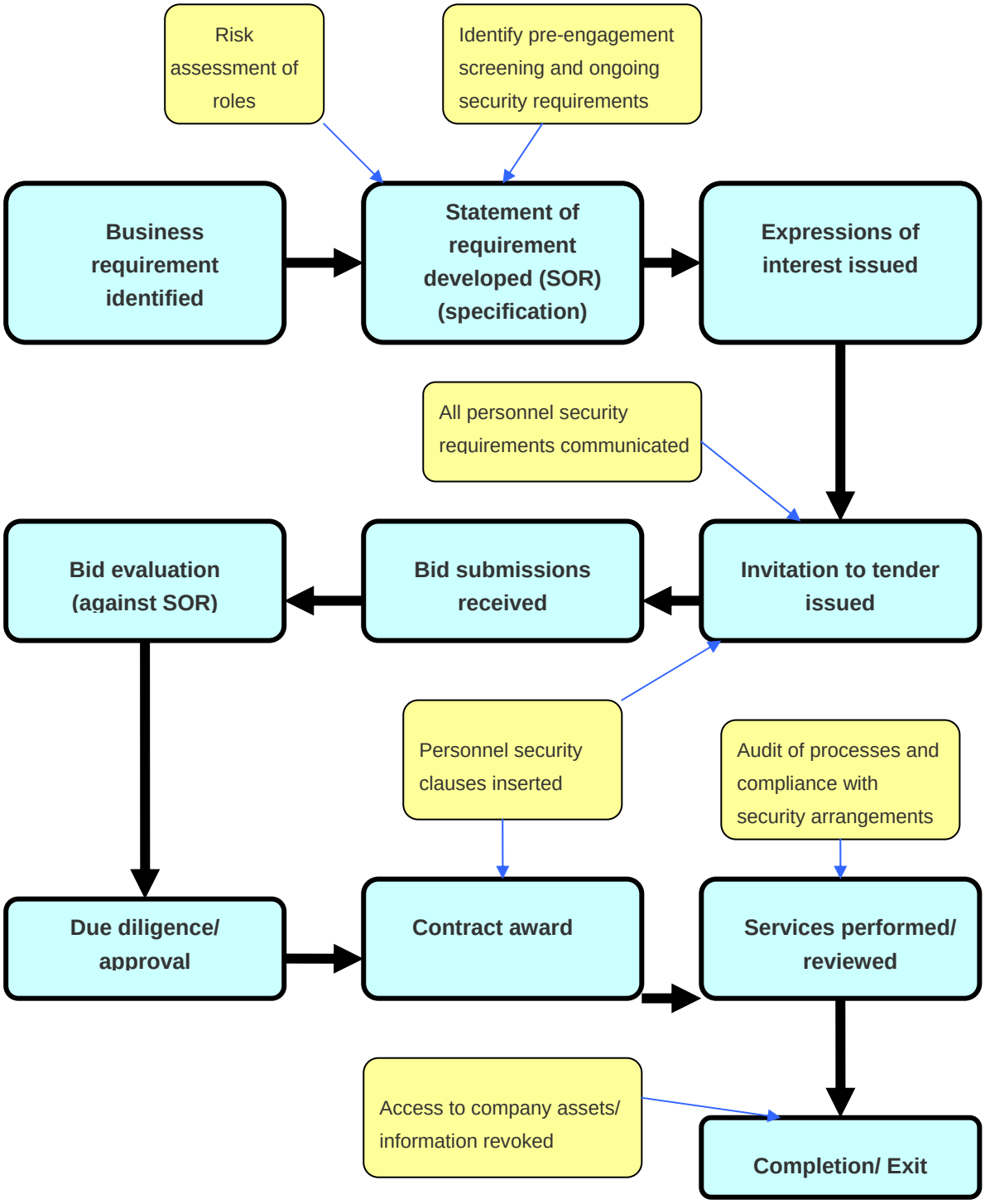


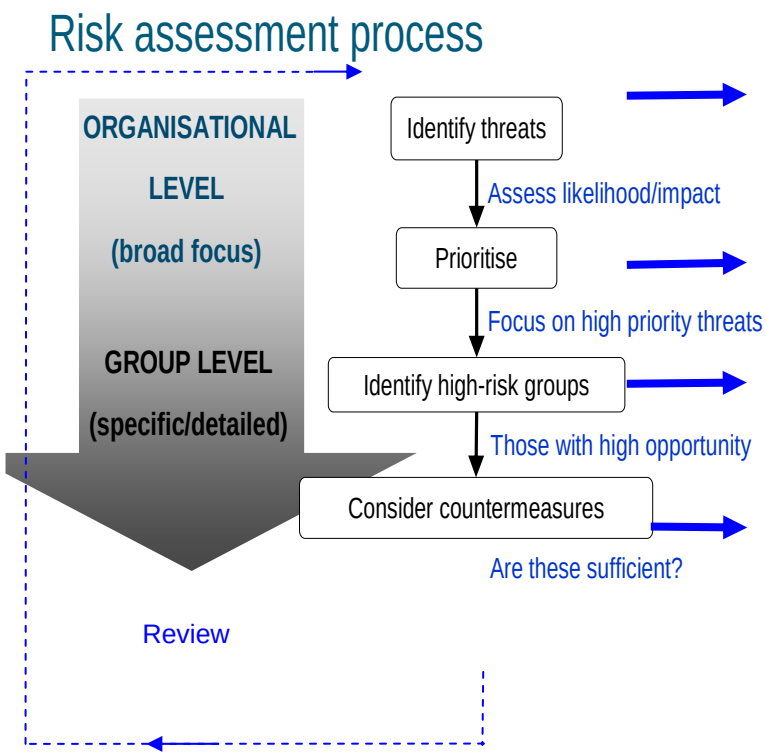

*Figure 1: Personnel security in the contract cycle*

## Step 1 - Risk assessment

Prior to the engagement of any contracting staff, a personnel security risk assessment should be undertaken to determine the level of insider risk posed to the organisation due to the access to information/assets the contractor(s) role will afford. The risk assessment process should mirror that used for permanent employees and consider the sufficiency of the personnel security countermeasures in place. In particular, the risk assessment should ensure that the level of pre-engagement screening associated with the contractor(s) reflects the level of access/responsibility associated with the role and that of an employee undertaking a similar role. In the event that this is not possible or workable in the timeframe, then a suite of other personnel security countermeasures should be deployed to manage the risk, such as restricted or monitored access (see the section *Ongoing measures* in step 4).

The suggested approach to ensure a transparent and consistent mechanism for achieving this is to adopt the CPNI personnel security risk assessment model. This process is outlined in figure 2 below. Organisations can use the outcome of assessments under this model to determine a proportionate personnel security regime for employees, contractors and workers.

*Figure 2: Risk assessment process*




**Identify** all the potential threats an insider could pose within the organisation (this may be broken down into individual business areas/sites).

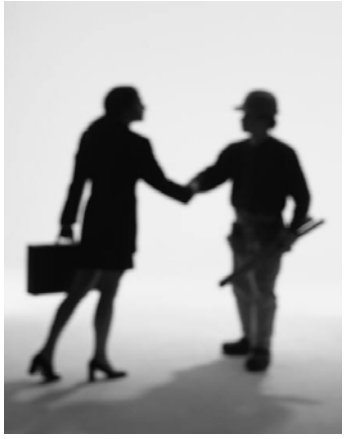
**Prioritise** these according to the impact these acts could have on the organisation and the likelihood of them taking place. Prioritisation will ensure you develop a personnel regime that is proportionate to the risk.

**Understand** which groups of employees/workers/**and contractors** have the necessary access and permissions to make these threats a reality.

**Consider** what countermeasures are in place and should be in place to reduce the vulnerability of the organisation to these threats. This should form the basis for pre-employment/engagement screening requirements and ongoing personnel security regime for employees, workers and contractors.

A suggested risk assessment matrix can be found in Annex A. For further information/ guidance on the risk assessment process see CPNI guidance: *Risk assessment for personnel security: a guide* available at www.cpni.gov.uk.

## Step 2 - Pre-engagement screening: determining the appropriate level of screening



The purpose of pre-engagement screening (also known as background checking, or in the instance of employees, as pre-employment screening) is to gain an appropriate level of assurance as to the competency, trustworthiness, integrity and probable reliability of the contractor as well as to confirm they are legally permitted to work in the UK. Once a personnel security risk assessment has determined the level of risk posed to the contracting authority by the contractor(s), the next stage is to define the appropriate amount of pre-engagement screening that is commensurate to this risk.

The contracting authority should, where possible, ensure contracting staff are subject to the same level of screening as permanent employees if they have the same access and privileges. These levels should be defined as a requirement in the tender process. The contracting authority should also define ahead of the tender process if the contracting authority will undertake the pre-engagement screening in-house, if the contracting company/agency will be responsible for the checks, or if a pre-determined third party screening company will be used.

Figure 3 outlines incremental levels of pre-engagement screening. These are recommended for use in conjunction with the risk assessment to set the screening requirements for contractors. Completion of these checks should be made a condition of working on the contract.

*Figure 3: Recommended pre-engagement screening levels*

**MINIMUM (All contractors should be cleared to this level)**

- Proof of identity
- Proof of residency
- Verification of right to work in the UK
- Self declaration of criminal records
- Relevant qualifications

**BASIC**

- All minimum checks +
- Employment/education history – 3 years (any gaps must be satisfactorily accounted for)
- Checks to include overseas information if relevant

**MEDIUM**

- All minimum and basic checks +
- Employment/education history – 5 years (any gaps must be satisfactorily accounted for)
- Basic criminal record disclosure to verify self declaration

**HIGH**

- All minimum, basic and medium checks +
- Employment/education history – 5-10 years (any gaps must be satisfactorily accounted for)
- All academic qualifications
- All professional qualifications
- *Additional measures if relevant**

*Additional measures*

- Financial enquiries if relevant to the role
- Standard/enhanced criminal record check if relevant to the role
- Security interview (optional interview to verify information from the screening process)
- National Security Vetting (see page 16)

## Criminal Record checks

Under the Rehabilitation of Offenders Act 1974 (ROA) a person is not normally required to disclose **spent** convictions when applying for a job. There are some roles in the oil and gas industry where convictions deemed to have been 'spent' can still be taken into account. These roles are outlined in ROA 1974 (Exceptions) Order 1975 and the ROA (Exceptions) Order (Northern Ireland) 1979. In these instances, companies can apply for Standard and Enhanced Disclosures which can be obtained from Disclosure Scotland, The Criminal Records Bureau and Access NI.

The ROA 1974 does however also state that it is reasonable for an employer to ask individuals for details of any unspent criminal convictions and can take the relevance of these convictions into account when considering employment/engagement. It is therefore advisable to obtain this information as part of the pre-employment screening process in-house, as well as a pre-engagement requirement for contracting staff.

**Engaging contractors who declare unspent convictions**

Information on a contractor's unspent criminal convictions can be obtained through either a self declaration (see Annex B) or a basic criminal record disclosure available from Disclosure Scotland or Access NI (the latter for those based in Northern Ireland).

The disclosure of a conviction should not necessarily be a bar to engagement. However, companies should indicate as far as possible, the types of unspent convictions that are likely to be unacceptable for a given post (there is likely to be significant variation between posts). We would advise - for all posts - that companies consider the situation carefully before allowing on site contracted staff who are:

- On probation (in a legal sense);
- Under a suspended prison sentence;
- Released from prison on parole;
- Still under a conditional discharge;
- Subject to a Control Order.

When engaging individual independent contractors, it is likely that the results of any disclosed convictions will be considered in-house by the contracting authority and the contracting authority's own criteria will indicate whether a declared unspent conviction is acceptable or not. In more complex cases a range of factors will need to be considered when making a judgement on engaging the individual - such as the seriousness of the offence; whether the offence casts doubt on the integrity of the individual or affects the ability of the individual to undertake the job; the relevance of the conviction to the post; the nature of the offence and the length of time since the offence occurred.

When contracting a company for services or engaging agency staff, clear criteria should be communicated to the recruiting organisation (as part of the pre-engagement screening requirements) to indicate whether a declared unspent conviction is likely to be acceptable or not. In more complex cases, an appropriate communication method needs to be put in place to enable appropriate discussion ahead of the engagement of the individual onto the contract.

**Overseas criminal record checks**

In some circumstances it may be prudent for the contracting authority to stipulate confirmation of criminal convictions in another country.

Further guidance on obtaining this information can be found in CPNI's *Pre-employment screening: a good practice guide* and *Disclosure of criminal records in overseas jurisdictions,* both available from www.cpni.gov.uk.

**National Security Vetting**

This guidance focuses on the pre-employment/engagement screening resources that are available to organisations as part of their in-house screening arrangements. In certain exceptional cases, the individual may also be required to hold a national security clearance (in addition to the screening levels detailed on page 14). National Security Vetting (NSV) seeks to determine an individual's suitability to hold posts with long-term, frequent and uncontrolled access to SECRET and TOP SECRET assets, or for posts involving access to individuals, establishments, assets or information assessed to be at risk from or of value to terrorists. These exceptional cases are defined by government policy and should be discussed with the Department for Energy and Climate Change (DECC).

## Additional Guidance:

**General**
CPNI: *Pre-employment screening: A good practice guide* (3rd ed) – www.cpni.gov.uk

**Criminal Record disclosure**
Disclosure Scotland – www.disclosurescotland.co.uk
Access NI – www.accessni.gov.uk

Criminal Record Bureau – the CRB no longer have a website, however information on criminal record checks with this body can be found at www.direct.gov.uk, www.businesslink.gov.uk and www.homeoffice.gov.uk

**Employing personnel with criminal records**
*Employing people with criminal records* (a Chartered Institute of Personnel and Development (CIPD) fact sheet) - www.cipd.co.uk

*Employing ex-offenders - a practical guide* (Assessing the relevance of criminal records) – (a joint CIPD and CRB publication) – www.cipd.co.uk

*Recruiting ex-offenders: the employers' perspective* - NACRO guidance, www.nacro.org.uk

*Guide to recruiting people with criminal records* – NACRO, www.nacro.org.uk

**National Security Vetting**
*Cabinet Office Security policy framework* - www.cabinetoffice.gov.uk

## Step 3 - Communicating the required standard of pre-engagement screening

### Embed pre-engagement screening in contracts

Contracts should outline the checks required for each post and detail how the checks are to be performed. Guidance on how to conduct pre-engagement screening can be found in CPNI's *Pre-employment screening: a good practice guide* available at www.cpni.gov.uk. One oil and gas organisation chose to attach a copy of this guidance to the contractual document and required the contract company to ensure that adequate pre-employment screening was carried out using the standard specified within this document. As the contracting authority you may wish to follow this example; you may chose to specifically embed your required standard into the contract, or you may wish to attach your own organisation's pre-employment screening policy as a schedule to the contract. You should of course always seek guidance from an employment lawyer in this process.

Regardless of the chosen embedding mechanism, the following standards should be observed as a minimum:

- An original (not photocopy) of one of the following documents should be checked:

  - Current signed full passport;
  - Current photo-card current driving licence and paper counterpart;
  - Current biometric residence permit (formerly known as identity card for foreign nationals);
  - Current EU/EEA identity card.

- A visual check should be performed to verify the applicant is identical to the individual in the identification documentation.

- In the absence of photographic documentation (or in addition to), identity should be established using two or more of the following original (not photocopy) documents:

  - Current full UK driving licence (old version);
  - Full birth certificate (sometimes referred to as the long birth certificate issued within 6 weeks of birth);
  - Current benefit book or card or original notification from the Department for Work and Pensions (DWP) confirming right to benefit;
  - Adoption certificate;
  - Marriage/civil partnership certificate;
  - Building industry sub-contractor's certificate issued by Her Majesty's Revenue & Customs (HMRC);

- Recent HMRC tax notification;
- Current firearms certificate;
- Police registration document.

- For applicants from overseas (or who have spent a considerable time overseas) the contracting company should seek to obtain the same information as that of a UK applicant.

- In the limited instances when photographic identity is not available, a photograph vouched with the signature of a 'person of standing' within the community such as a magistrate, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager or civil servant, who has known the individual for at least three years should be required to verify identity. The signatory should also be contacted to check that he or she did, in fact, sign the photograph.

- One of the following original (not photocopy) documents should be obtained to verify the applicant's current address. The document must be less than three months old and contain the applicant's full name and address:

  - Proof of residence from a financial institution
  - Record of home visit
  - Confirmation from an electoral register search that a person of that name lives at that address (electronic check)
  - Relevant utility bill or certificate from a company confirming the arrangement to pay for the services at a fixed address on pre-payment terms
  - Local authority tax bill (valid for current year)
  - Bank, building society or credit union statement or passbook containing current address
  - Recent mortgage statement from a recognised lender
  - Current local council rent card or tenancy agreement
  - Court order

- The relevant contracting company should be satisfied the identity documents are genuine – for guidance see CPNI's *A good practice guide on pre-employment screening: document verification* at www.cpni.gov.uk.

- Right to work should be verified in accordance with the UK Asylum and Nationality Act 2006 and the UK Border Agency code of practice.

- Applicants are required to account for periods of time or residence not explained in their CV (one month +).

- References (where applicable) are confirmed to be genuine through a structured process e.g. follow-up telephone calls (landline number not mobile), requests for headed paper, independent internet verification.

- Employment/Education references require detailed information for the whole period of employment/education: dates and positions held/verification of job title and salary. For education references this should cover the course dates, title of course and grade awarded.

- Original copies of qualification certificates are inspected and copies retained.

**Dealing with adverse pre-engagement screening information with contractors**

The contracting authority should put in place a process with the contracting company/agency for dealing with adverse pre-employment screening information, stating where possible the threshold for refusal of an individual to work for the organisation as part of the contract. This should also consider the disclosure of criminal convictions where appropriate. It is also advisable to put in place a process to enable the contractor company/agency to refer the decision making process (in particular for border-line cases) back to the contracting authority ahead of any decision to go ahead and engage the individual.

## Case study

One major oil and gas company has set thresholds for adverse pre-engagement checks as follows:

*Instances where an individual should not be utilised on the contract:*

- The contractor refuses to give their consent or provide information for legitimately requested screening purposes to their employer;
- The contractor has not been able to adequately confirm their identity to their employer or where the contractor has attempted to mislead their employer as to their identity;
- The contractor has not been able to confirm to their employer they have a right to work in the UK, where they do not have a right to work in the UK or where the employee has attempted to mislead their employer over their right to work;
- The contractor fails to achieve security vetting clearance where the contract requires that National Security clearance (NSV) is obtained;
- Previous employment within the Company that resulted in an unsatisfactory termination or where they were previously removed from working on any contracts to perform work for the Company.

*Instances where acceptance of the person must be discussed and agreed with the Company contract manager:*

- Any gaps in employment or address history greater than one month where a reasonable explanation cannot be provided;
- Any unspent criminal conviction.

**Managing the unanticipated procurement of contractors**

The contracting authority **should not** allow contractors onto site until pre-engagement screening has been completed. There may however be emergency situations where an individual must be brought onto site ahead of the completion of pre-engagement screening, or instances where it is not feasible to screen a contractor to the same level as an existing employee even if they are to have the same access rights. In these situations a process **should** be in place between the contracting company/agency and the procuring company to ensure the risks are mitigated through other means for example the use of an escort or restricting access (see ongoing personnel security in the next section of this guidance).

## Step 4 - Embedding ongoing personnel security into contracts and practice

The personnel security risk assessment will inform decisions about ongoing personnel security countermeasures, helping to ensure that they are proportionate to the risk of contractors acting maliciously in post. Once on site, contractors are usually given access to the same organisational assets as permanent employees in similar roles and as such can have the same impact if they use this access for illegitimate means. It is rational, therefore, to subject them to the same ongoing personnel security measures as their permanent counterparts.

Contracting authorities may wish to attach their own security policies as a schedule to the contract to ensure compliance, or draft specific security requirements into the contract. Regardless of the mechanism of delivery the following approach/regime should be observed:

**In January 2008, Emir Hysenaj was found guilty along with five others for the £53 million robbery of the Securitas depot in Kent in 2006. Mr Hysenaj, an agency worker based at the depot, had reportedly undergone some limited pre-engagement screening. He was on a low wage, but had extensive access to a facility that dealt with hundreds of millions of pounds in cash. Mr Hysenaj was accused of providing information to the criminal network ahead of the raid, using a hidden camera to film the inside of the deport. It was only after the event that colleagues purportedly recollected Hysenaj's heightened interest in the security arrangements at the depot.**

***Press reporting*.**

**1. Have a system in place to confirm the person who arrives for work is the person the agency/contract company supplied and 'screened' to work for you.**

An effective mechanism is the exchange of photographs and names between the agency/contracting company and the contracting authority to enable verification at the gate/door. Industry-recognised arrangements such as the Vantage system, the Energy Utilities Skills Register Card, or the Construction Skills Certification Scheme could also be used as an additional verification check as part of this process (though not as a replacement for pre-engagement screening). For individual independent contractors, it is suggested

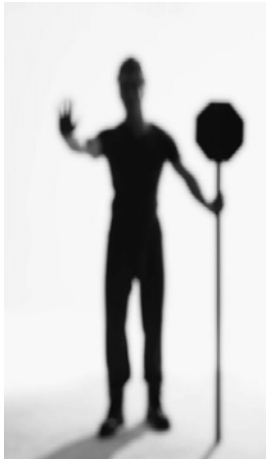
document verification takes place in-house to verify identity (see CPNI guidance: *Pre-employment screening, a good practice guide* at www.cpni.gov.uk.)

**2. Control Access**

Where possible, contractor access should be limited physically by zoned/controlled access and contractors should be issued with a separate, distinguishable pass to permanent staff and be distinguishable from permanent staff through other means (such as different coloured hats, overalls or tabards etc). Contractor passes should be programmed to automatically expire on a daily basis or when the contractor is no longer required on site. It is advisable to configure contractor passes to detect any attempted unauthorised activity. A process should also be put in place to manage the security of any site keys held by contractors.

To compliment this, a challenge culture for non-compliance with the access policy should be followed and promoted on site.

**3. Consider escorted access**



In instances where contractors have access to sensitive assets or information and have not been screened to the same standard as permanent staff, companies should escort them whilst on site or implement additional controls such as physical measures to restrict unfettered access (for a range of protective security measures see www.cpni.gov.uk).

**4. Control IT security**

Sensitive IT systems should be restricted to those who require legitimate access. Contracts should be drafted requiring mandatory adherence to the principles of the contracting authority's IT policies, including the prohibition of unauthorised use of the organisation's IT systems. The contract should also include a stated right for the contracting authority to monitor/revoke user activity. IT rights should also be revoked automatically when the contractor leaves. The contracting authority may choose to achieve this by attaching their own company policies as a schedule to the contract or by creating contractor-specific policies (for guidance on protective electronic security measures see www.cpni.gov.uk).

**5. Have a clear process of ongoing security management for contractors**

It is advisable that the contract outlines the following personnel security provisions:

- The pre-engagement screening requirements (see pages 13-20);
- Where any work should be carried out and who should have access to specific material (i.e. named individuals);

- Details or reference to the arrangements for dealing with security incidents/breaches (e.g. reporting, notifying and investigating);
- A requirement for contract staff to protect the organisation's assets (including restrictions on copying and disclosing company/customer information);
- Access control arrangements (physical and electronic access);
- An obligation to inform the organisation if an individual is no longer employed by the agency/contracting company, has been dismissed, is undergoing any disciplinary procedures or has been arrested;
- A requirement that the contracting company/agency must disclose any incident of expulsion from any relevant accrediting body;
- A clause requiring the contractor to disclose any work being undertaken concurrently for a competitor organisation and providing for immediate termination of the contract if there is thought to be a conflict of interest;
- Details of who is responsible for any lapse in security. It is advisable to name an identified individual (single point of contact) within the contracting company/agency that ensures individuals comply with company security requirements;
- A clause that the contracting company/agency will be liable for financial penalties if it is discovered that the security provisions have not been adhered to (including pre-engagement screening).

Any standards of behaviour which a permanent employee is expected to observe should be included as a normal part of the contractual agreement. For example, contractors should be expected to commit to policies governing acceptable use of email and the internet, obligations towards data protection, security policies, and the organisation's gift policy. Some organisations include a premium in the contractor's fee that can be deducted if they fail to comply with these requirements.

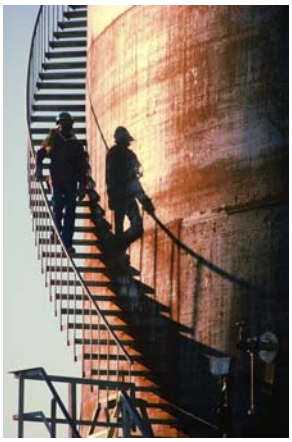
**6. Include a security briefing as part of the site induction**

Oil and gas companies will not issue a site pass to contractors without completion of a health and safety induction. By expanding this to ensure contractor awareness of health, safety **and security** requirements you can help foster a more effective security culture on site.

**7. Have a process in place with the contracting company/agency to manage the substitution of a temporary member of staff when the usual contract staff member is absent**

These arrangements should be included in the contractual agreement, and the engaging organisation will need to decide what additional personnel security measures to implement (if required) – for example, restricted or supervised access when the replacement contractor is on site.

**8. Put in place effective exit/off-boarding procedures**



These arrangements should include provisions for revoking physical access to site/buildings, return of passes and keys, return of any equipment, return of any documents (physical or electronic), removal of IT access and any remote access. Most organisations find it beneficial to have an exit checklist to ensure nothing is overlooked.

**9. Consider re-engagement provisions**

When a contractor is engaged on more than one occasion in the same organisation, it is important not to assume that their circumstances have remained unchanged between periods of engagement. Steps should therefore be taken, at the beginning of each period of re-engagement, to ensure as far as possible that the contractor poses no greater threat to the organisation than previously. Depending on the time elapsed, the nature of the organisation and the sensitivity of the role, this could range from a short series of questions confirming that contractors' circumstance gives no greater cause for concern than during the initial period of engagement, to a repeat of the entire pre-engagement screening process. This requirement should be stipulated in the contract.

**Further guidance**

**For further guidance on ongoing personnel security see CPNI *Ongoing personnel security: a good practice guide* www.cpni.gov.uk.**

## Step 5 - Audit

Contracting authorities should quality assure compliance by the contracting company / agency with their pre-engagement screening and ongoing security requirements through regular audit (a suggested checklist to assist with this process can be found in Annex 2).

Companies should ensure that the right to audit is specified in their contractual documentation and contains sufficient compensatory terms (such as a termination clause) if the contracting company is found to be in breach of this requirement.

It is sometimes useful to determine in advance which company will bear the costs of audit requirements, particularly in the event that the activity is likely to be outsourced. If possible to do so, this should be outlined within the contract, noting any circumstances in which this might differ.

Companies should also consider outlining their expectations for readily available records to be held in accordance with the requirements of the Data Protection Act and other legislation, which could be referred to in an audit scenario.

The contract should make provision for the company to be able to examine the records or perform an audit with reasonable notice (and ideally to define the minimum notice to be provided).

**The audit process**

The audit process itself should be as transparent and as independent as possible. Ideally the terms of reference should be agreed with the contracting company / agency before commencing the audit to ensure that the purpose and scope of the audit is clear. Maintaining a collaborative approach will help to ensure that the relevant documentation and personnel are available for the duration of the audit. The terms of reference should include the expected duration of the audit, which records and access to key staff will be required, and where the results will be reported at the end of the audit.

There may be some instances which require an urgent audit into the arrangements for pre-engagement screening, for example, where it is perceived that a breakdown in the process may have contributed to a security breach. In this case, the terms of reference should still be defined, and the audit conducted in a similar way, although the minimum notice as defined in the contract can be used to gain access more quickly if required.

The audit is likely to include two aspects; the framework and process deployed by the contracting company to deliver effective background checking, and a review of a sample to validate that checks have been completed to the required standard.

**Framework / process review – guidance checklist:**

**Audit Objective:** assurance to be obtained through interviews with key staff and review of procedural documentation.

- What processes and procedures do the contracting company have in place for pre-engagement screening?
  - Obtain copies and assess whether these are aligned with the company's requirements and policy for background checking of contractors?
  - What happens if the processes are not in place?
- Is there a structured process in place for confirming references and legitimacy of documentation?
- Is there a process to handle overseas validation of references and documentation?
- How do they ensure the checks are consistently applied?
- What controls do the contracting company have in place to ensure checks are completed?
  - For example – supervisory checks / oversight
  - Signed checklist for the person completing the checks
- What process is being used to handle exceptions?
  - Who decides?
  - Who takes on board the risk?
  - Has the company defined parameters around exceptions?
  - Has the company defined parameters for the contracting firm to work within?
  - Is there a contact within the business who they can contact if they are not sure?
- What process do they have in place to deal with ongoing personnel security issues which may arise?

### Sample check and/or observation of live process

**Audit Objective:**

Assurance to be obtained through observing live process and sample check of paperwork:

- Observe live process if possible to do so -
  - Select a number of checks to observe taking place from start of the process through to the end.
- Review the paperwork or documentation to confirm that the relevant checks have been carried out (a checklist to assist with this element of the audit can be found in annex C) -
  - Sample size – the sample size should be proportionate to the number of checks carried out, and could be determined by establishing an average number of checks that have been completed during a typical month.
  - Review the records (individual records or checklists) to ensure that the relevant checks have been carried out and results documented in accordance with the Data Protection Act.
- If Management Information is routinely gathered as part of the assurance process, validate a sample of this to the extent that it is possible to do so.
- Validation of some of the records held to ensure that checks have been completed.

## Subcontractors

For very large or complex projects, organisations may engage a company rather than an individual as a contractor, and that company may need to engage others in order to complete the project. When contractors recruit subcontractors, who may in turn recruit further levels of subcontractor, there is potential for the organisation's security standards to become confused or diluted.

To mitigate against this risk as far possible, the contract between the contracting authority and the first contracted company must be absolutely explicit about:

- The security controls (both pre-engagement and ongoing) demanded by the organisation, and the need for these to be upheld throughout the entire contracting chain;
- Who is responsible for any lapse in security;
- The right of the organisation to approve any subsequent choice of subcontractor;
- The right of the organisation to audit the implementation of the security standards at any point in the contracting chain.

## Secure procurement of contracting staff checklist

- A risk assessment has been conducted to determine the level of insider risk posed to the contracting authority due to the access to information/assets the contractor(s) role will afford.
- Proportionate pre-engagement screening levels(s) have been agreed that are commensurate to the risk.
- The level and standard of screening has been formally communicated to the contractor, agency or contracting company (including a mechanism to deal with any adverse information uncovered during recruitment).
- Appropriate ongoing security arrangements and policies have been drafted into the contract with clear lines of communication and defined responsibilities outlined (personnel, IT, information and physical).
- Agreed access arrangements have been put in place.
- A system has been put in place to confirm that the contractor who arrives to work is identical to the individual who has been supplied and 'screened' to work on the contract.
- A process has been put in place with the contracting company/agency to manage the substitution of a temporary member of staff when the usual contract staff member is absent.
- An effective off-boarding process has been put in place to ensure that the contractor's access to assets and information has been revoked when it is not longer necessary.
- An appropriate audit mechanism has been put in place to monitor compliance with the required security arrangements of the contract (including pre-engagement screening).
- The security controls (both pre-engagement and ongoing) demanded by the contracting authority have been cascaded throughout the entire (sub)contracting chain.

## Annex A: Example risk assessment matrix

| Threat No. | Threat | Likelihood scale 1-5 | Likelihood assumptions | Impact scale (1-5) | Impact assumptions | Risk priority (1-4) | Group with highest opportunity | Reasons | Countermeasures | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Existing | Sufficient? | New |
| 1 | e.g. Employee carries out a Denial of Service (DoS) attack on an IT system | 2 | Lack of technical knowledge<br><br>Technical information available to enable this to be carried out<br><br>Back up services | 2 | System loss for 24 hours<br><br>Reputational impact<br><br>Minimal loss of customers | (Score dependent on impact and likelihood scores.) | IT staff [100]<br><br>IT staff in the last two years [75] | Staff have the skills, opportunity & knowledge | CCTV<br><br>Supervision and natural surveillance by colleagues.<br><br>Back up system in place. | CCTV coverage not effective on key locations.<br><br>No security appraisals / whistle-blowing systems to flag concerns.<br><br>No automatic removal of IT access on exit. | Two man rule in IT server room.<br><br>Initiate whistle-blowing system.<br><br>Brief staff on need to extend personnel security to ex-IT personnel.<br><br>Automate the removal of IT access on exit. |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |

# Annex B: Example criminal record self-declaration form

**Note:** If you are appointed, a check against the National Collection of Criminal Records may be undertaken and documentary evidence sought to confirm your answers.

Surname:……..

Full Forenames:…….....

Full permanent address:…….....

……

……..

Date of birth:……

1. Have you ever been convicted or found guilty by a Court of any offence in any country (excluding parking but including all motoring offences even where a spot fine has been administered by the police) or have you ever been put on probation (probation orders are now called community rehabilitation orders) or absolutely/conditionally discharged or bound over after being charged with any offence or is there any action pending against you? You need not declare convictions which are 'spent'* under the Rehabilitation of Offenders Act (1974).

YES / NO (delete whichever is not appropriate) (*If yes, please give details overleaf)*

2. Have you ever been convicted by a Court Martial or sentenced to detention or dismissal whilst serving in the Armed Forces of the UK or any Commonwealth or foreign country? You need not declare convictions which are 'spent' under the Rehabilitation of Offenders Act (1974).

YES / NO (delete whichever is not appropriate) (*If yes, please give details overleaf)*

3. Do you know of any other matters in your background which might cause your reliability or suitability to have access to government assets to be called into question?

YES / NO (delete whichever is not appropriate) (*If yes, please give details overleaf)*

* The way in which a conviction becomes spent under the ROA 1974 will depend on the sentence received for the offence, and the rehabilitation period that applies to that offence sentence. If a person has been convicted of an offence for which a sentence of more than 2.5 years was imposed then the conviction can never be spent. Free independent legal advice in this area can be sought from NACRO.

If you answered ‘YES’ to any of the questions on this form, please give details below.

I declare that the information I have given on this form is true and complete to the best of my knowledge and belief. In addition, I understand that any false information or deliberate omission in the information I have given on this form may disqualify me for employment.

Signature:…….

Date:…….

The information you have given above will be treated in strict confidence. You do not need to show the completed form to any representative of the company.

**Important: Data Protection Act (1998).** This form asks you to supply ‘personal’ data as defined by the Data Protection Act 1998. You will be supplying this data to the appropriate HR or Security authority where it may be processed exclusively for the purpose of a check against the National Collection of Criminal Records. The HR or Security authority will protect the information which you provide and will ensure that it is not passed to anyone who is not authorised to see it.

By signing the declaration on this form, you are explicitly consenting for the data you provide to be processed in the manner described above. If you have any concerns, about any of the questions or what we will do with the information you provide, please contact the person who issued this form for further information.

Name and address of sponsoring company:……..

…….

…….

## Annex C: Example secure procurement of contracting staff audit checklist (pre-engagement screening)

| | | Yes/No/NA | Comments |
|---|---|---|---|
| **1** | The organisation has a copy of the pre-engagement screening policy detailing different levels of background checks required for all new contractors | | |
| **2** | The following credentials are confirmed about all new applicants **prior** to the proposed start date: | | |
| **2.1** | Identity is established by checking the original (not photocopy) of one or more of the following: | | |
| | **a)** Current signed full passport | | |
| | **b)** Current photo-card driving licence and paper counterpart | | |
| | **c)** Current biometric residence permit | | |
| | **d)** Current EEA identity card | | |
| **2.11** | A visual check is performed to verify the applicant is identical to the individual in the identification documentation | | |
| **2.2** | If photographic identity documentation is not available, identity is verified through two or more of the following types of original (not photocopied) documents: | | |
| | **a)** Current full UK driving licence (old version) | | |
| | **b)** Full birth certificate (issued within 6 weeks of birth) | | |
| | **c)** Current benefit book or card or original notification letter from the Department for Work and Pensions (DWP) confirming right to benefit | | |
| | **d)** Adoption certificate | | |
| | **e)** Marriage / civil partnership certificate | | |

| | | Yes/No/NA | Comments |
|---|---|---|---|
| | **f)** Building industry sub-contractor's certificate issued by Her Majesty's Revenue & Customs (HMRC) | | |
| | **g)** Recent HMRC tax notification | | |
| | **h)** Current firearms certificate | | |
| | **i)** Police registration document | | |
| | **j)** None of the above, they only check a current full signed passport, photo driving licence or photo identity card | | |
| **2.3** | In the event that photographic identification is not available, a photograph vouched with the signature of an upstanding member of the community is used to verify identity | | |
| **2.4** | One of the following original (not photocopy) forms is used to verify the applicant's address | | |
| | **a)** Proof of residence from a financial institution | | |
| | **b)** Record of home visit | | |
| | **c)** Confirmation from an Electoral Register search that a person of that name lives at that address | | |
| | **d)** Recent original utility bill or certificate from a company confirming the arrangement to pay for the services at a fixed address on pre-payment terms | | |
| | **e)** Local authority tax bill (valid for current year) | | |
| | **f)** Bank, building society or credit union statement or passbook containing current address | | |
| | **g)** Recent original mortgage statement from a recognised lender | | |
| | **h)** Current local council rent card or tenancy agreement | | |
| | **i)** Court order | | |
| | **j)** None of the above (supply details) | | |
| **2.41** | Only documents that are less than 3 months old are accepted | | |

| | | Yes/No/NA | Comments |
|---|---|---|---|
| **2.5** | The organisation complies with the requirements under the Immigration and Asylum Nationality Act 2006 and the UKBA code of practice in ascertaining the right of an individual to work in the UK | | |
| **2.6** | All applicants complete a self declaration of *unspent* criminal convictions | | |
| **3** | When required, contractors always undergo the relevant criminal record disclosure to identify any unspent convictions | | |
| **4** | If required, a minimum of three years previous employment history is verified for all employment/education references | | |
| **5** | When stipulated, previous employment history is verified for 5-10 years in line with required level | | |
| **6** | References are confirmed to be genuine through a structured process e.g. follow up telephone calls, requests for headed paper, independent internet verification | | |
| **7** | Employment references require information for the whole period of employment | | |
| **8** | When an employer's reference cannot be provided, references from other responsible people are obtained (education/character references) | | |
| **9** | The organisation requires candidates to produce original qualification certificates for inspection *(e.g. educational, health and safety)* | | |
| **10** | The organisation retains copies of qualification certificates | | |
| **11** | If relevant to the post, financial checks are always carried out to identify serious debt | | |
| **12** | For applicants from overseas (or who have spent a considerable time overseas) the same information as that of a UK applicant is sought | | |

| | | Yes/No/NA | Comments |
|---|---|---|---|
| **13** | Applicants are required to account for periods of time or residence not explained in their CV | | |
| **14** | Personal Data is maintained in accordance with the Data Protection Act 1998 | | |