Cabinet Office

HMG Baseline Personnel Security Standard

GUIDANCE ON THE PRE-EMPLOYMENT SCREENING OF CIVIL SERVANTS, MEMBERS OF THE ARMED FORCES, TEMPORARY STAFF AND GOVERNMENT CONTRACTORS

Version 6.0 – May 2018

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
1.0	1.0	Dec 2008	N/A
2.0	2.0	1 May 2009	Version 2.0 of the guidance reflects the Official Committee on Security, Sub-Committee on Personnel Security (SO(PS)) decision that full implementation of the BPSS (including application of the 'unspent' criminal record check on all recruits) is a core mandatory requirement of the SPF (MR23). Additional references to expert advice on immigration, nationality and right to work legislation and overseas criminal record checks have been incorporated.
3.0	2.1	Oct 2009	Version 2.1 of this guidance makes more explicit reference to Mandatory Requirement 23 and the removal of the reference to the document 'Identity Fraud – The UK Manual.' This version also advises that as a **pre-employment** screening process, we do not expect the BPSS to be applied retrospectively where assurances have already been obtained or are in place to allow for access to government assets.
5.0	3.0	February 2011	Version 3.0 of this guidance amends an erroneous reference to the List X 'Approval for Access' process and has been amended to reflect recent policy changes to reviews and renewals of the BPSS. Reference is also made to the Home Office's plans to review the Notifiable Occupation Scheme.
8.0	3.1	April 2012	Change to HMRC's address in Part II, paragraph 36 for checks on an employment record.
10.0	3.2	April 2013	Minor changes to format and branding. Updated links and contact details.
11.0	3.3	October 2013	Minor changes to formatting. Reference to HMRC Record Check removed and replaced with Civil Service Resourcing Employment History Check. National Insurance Number (NINO) Prefix list removed.
N/A	4.0	April 2014	Version 4.0 has been aligned to the new government classification policy for implementation in April 2014. Minor updates (e.g. to website links) are also included. The reference to the BPSS CD-Rom has been removed, as the content is out of date.
N/A	5.0	January 2018	Version 5.0 reflects the introduction of the Disclosure Barring Service taking over from Disclosure Scotland for conducting unspent

			criminal record checks in England and Wales.
1.1	6.0	May 2018	Changes in data protection legislation reflected.

Contents

HMG BASELINE PERSONNEL SECURITY STANDARD

PART I – INTRODUCTION AND BACKGROUND

The HMG Baseline Personnel Security Standard (or 'BPSS') describes the pre-employment controls for all civil servants, members of the Armed Forces, temporary staff and government contractors generally. Its rigorous and consistent application also underpins national security vetting.

The personnel security controls described in this document **must** be applied to any individual who, in the course of their work, has access to government assets. Every effort **must** be made to complete the BPSS, but where it cannot be applied this **must** be risk-managed and the details recorded for audit purposes.

This document reflects the application of the BPSS in government and, as such, there are common references to "departments and agencies." This should be borne in mind when applied to those outside of government (e.g. List X, Civil Nuclear Industry etc).

Introduction

1. The most important asset in any organisation is its people. The application of the BPSS should ensure that organisations are employing people entitled to work in the UK and with the honesty, integrity and values needed for government-related work.

2. The BPSS and supporting guidance describe the mandatory pre-employment controls required to address the problems of identity fraud, illegal working and deception generally. As well as posing serious risks to reputation, integrity and financial assets they may also be indicators of more serious national security concerns. Failure to address these issues could lead to reputational or more serious damage to the business of government. It should be remembered that without adequate confirmation of identity any subsequent National Security Vetting (NSV) offers no assurance.

Responsibilities

3. Generally, the responsibility for applying the BPSS rests with HR divisions. However, it is strongly encouraged that HR and Security units work closely together to ensure the effective and consistent application of the guidance. Other stakeholders (e.g. legal advisers and procurement staff) should also be involved where appropriate.

Pre-employment Security Controls

4. As part of a holistic security regime, which includes physical and IT security measures, departments and agencies **must** have in place appropriate personnel security controls before and during employment to reduce the risk of damage, loss or compromise of government assets.

5. As a minimum requirement, all staff **must** be subject to the BPSS. Full implementation of the BPSS, including a 100% application of the 'unspent' criminal record check, is explicitly mandated as part of the Security Policy Framework (SPF). **Mandatory Requirement 13** states that:

Departments and Agencies must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and proportionate and robust personnel security regime that determines what other checks (e.g. National Security Vetting) and ongoing personnel security controls should be applied.[ao]
OI,
The BPSS describes the pre-employment screening controls for government and therefore there is no requirement for these checks to be applied retrospectively where assurances have already been obtained or are in place to allow for access to government assets.

For more sensitive posts there are an additional range of security controls, collectively referred to as National Security Vetting (NSV). These controls are not a substitute for the BPSS (which, apart from the unspent criminal record check, should be carried out beforehand) and **must only** be applied where they are necessary, proportionate and add real value.

6. The purpose of conducting rigorous pre-appointment checks is to:

- Ensure that all new, directly recruited staff are entitled to undertake the employment in question and, where appropriate, meet nationality rules for government service.
- Guard against the employment of anyone posing as a prospective employee for commercial or personal gain.
- Provide a sound basis for any subsequent NSV requirement.

7. Although implementation of the BPSS is mandatory there may be occasions when it is not possible to carry out all of its checks (e.g. for high numbers of short-term contractors or overseas workers). It is recognised, too, that monitoring compliance becomes increasingly difficult for departments the further away from their centre the business goes (e.g. to contractors and sub-contractors, etc). However such instances must be appropriately risk-managed and the reasons for not applying the BPSS in full recorded for audit purposes.

8. Where staff are appointed in posts overseas (e.g. staff engaged locally by the FCO, DFID, etc), and the BPSS cannot be applied, all possible related verification checks **must** be carried out as part of the recruitment process.

Baseline Personnel Security Standard

9. The BPSS is one of four levels of personnel security controls currently available to departments and agencies depending on the level of assurance required. The others are the Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). The BPSS is not a security clearance whereas the CTC, SC and DV are all formal security clearances obtained through the NSV process.

National Security Vetting (NSV)

In <u>all</u> cases, verification of identity and the individual's entitlement to undertake the work in question <u>must</u> be carried out before NSV. The other elements of the BPSS (excluding the criminal record check) must be completed as soon as practicable and certainly within three months.

10. Other than in exceptional circumstances NSV **<u>must not</u>** be undertaken before the BPSS' controls have been applied. However, it is recognised that, on some occasions, elements of NSV will have to be carried out in parallel. These occasions should be entered into by departments and agencies, on a case-by-case basis, with full acceptance of the risk, and with close liaison between those responsible for applying the BPSS and those carrying out NSV.

'Need to know' principle

11. The dissemination of sensitive information and assets should be no wider than is necessary for the efficient conduct of an organisation's business and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. This 'need to know' principle is fundamental to the protection of sensitive government assets. It applies both within a department or agency and when dealing with individuals outside of it.

Access

12. The BPSS allows for access to HMG assets on a need to know basis, the BPSS is sufficient to allow an individual:

- Access to OFFICIAL assets of UK origin.
- Occasional access to SECRET assets of UK origin in the normal course of business or during conferences or courses or briefings.
- Custody of a small quantity of SECRET assets.
- Entry to areas where SECRET assets are stored.
- To work in areas where SECRET and TOP SECRET information might be overheard.
- To use equipment capable of handling SECRET information, provided that access controls are in place.
- User access to the Public Services Network (PSN).

The BPSS is not sufficient for an individual working in a post in which they could obtain a comprehensive picture of a SECRET plan, policy or project. In this case a formal security clearance would be required.

13. The BPSS does not allow:

- Access to, or knowledge or custody of, assets classified CONFIDENTIAL or above, belonging to another country or international organisation (e.g. NATO).
- An overseas agent[1] for a contractor to have access to, or knowledge or custody of, assets classified SECRET or above, in which case a Security Check (SC) is required.
- Access to a restricted site[2] during an overseas visit.
- Access to any SECRET codeword material or TOP SECRET material.
- Logical access to the Public Services Network (PSN) (e.g. administrators who have the capability and opportunity to attack the system).

14. In these circumstances, depending on the level of access required, a formal security clearance will be required. This may also be necessary where a department or agency considers the risk of access to even a small amount of SECRET assets is unacceptable.

15. The judgement on access and risk will depend on the scope for introducing appropriate risk management measures. Rigorous application of the BPSS seeks to manage the risk of staff or contractors exploiting their legitimate access to government assets for unauthorised purposes.

The Centre for the Protection of the National Infrastructure provides guidance on carrying out a risk assessment for personnel security at:
http://www.cpni.gov.uk/advice/Personnel-security1/

Data protection in recruitment and selection

16. Data protection legislation applies to the processing of personal data about individuals. Applying the BPSS will involve such processing and must be carried out in compliance with the data protection principles that data must be:

- Fairly and lawfully processed.
- Obtained for specified and lawful purposes.
- Adequate, relevant and not excessive.
- Accurate and kept up to date.
- Kept for no longer than is necessary.
- Processed in line with the rights of individuals under the legislation.
- Secure.
- Not transferred to countries without adequate protection.

[1] An overseas agent is an individual employed by, or contracted to a UK company to represent its interests outside the UK. The individual would be a foreign national, or exceptionally a British National with permanent overseas residency. The BPSS allows an overseas agent to have occasional access to SECRET on approved UK sites.

[2] A restricted site is either a government, military or industrial facility that is cleared to hold classified material.

17. Data protection legislation does not prevent an employer from carrying out effective recruitment controls, but balances the employer's needs and the applicant's right to respect for their private life. Further information is available from the Code of Practice issued by the Information Commissioner.

The Information Commissioner's Office (http://.ico.org.uk/) provides detailed guidance on data protection and employment practices at:

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/employment/

It is consistent with data protection legislation that an individual's refusal to undergo an essential check where there are no alternatives could lead to a refusal of employment. In such cases, individuals should be made aware that it will not be possible to take them on should they refuse. This is distinct from making a particular check a condition of employment where it may not actually be necessary. From a legal point of view the important considerations are (i) that checks are carried out uniformly on a non-discriminatory basis and (ii) that privacy rights, where relevant, are respected.

Transparency

18. To promote transparency, speed up recruitment and comply with data protection legislation, the requirement for BPSS checks and the purposes for which personal information will be used must be made clear in job advertisements and/or recruitment literature/information packs. This is equally necessary where recruitment agencies are used on behalf of an employer. Departments and agencies must explain to applicants as soon as is reasonably practicable in the recruitment process the nature of the verification process and the methods used to carry it out. The most appropriate way to do this will likely be through a privacy notice provided prior to or as part of the application. A flow chart showing how a recruitment process might look is shown at Annex A. Applicants must be reminded that supplying false information or failing to disclose relevant information could be grounds for refusal/dismissal and could amount to a criminal offence.

Sifting and shortlisting

19. The checks should not be used for sifting applicants and should only be carried out where employment has been offered subject to satisfactory completion of enquiries.

Successful completion of the BPSS is one criterion upon which the decision to employ should be based. It should not conflict with the principle of *'selection on merit on the basis of fair and open competition'* which the Civil Service Commission (CSC) upholds.

20. In general, individuals **must** not start work until the BPSS has been satisfied. Employment **must** not commence until identity and an entitlement to undertake the work in question have been established as a minimum. In exceptional circumstances only (e.g. where delays would have a detrimental effect on the organisation's

business), conditional appointments may be made where they have been risk assessed and the outcome recorded. In all cases, the BPSS **must** be completed as soon as possible thereafter and certainly within three months of the employment commencing.

Contractors, consultants and agency staff

21. It is easy to overlook the fact that contractors, consultants and agency staff working on government premises may not have undergone the same degree of checking as permanent government employees, even though they will often have unsupervised access to both premises and information. This can apply to all levels of staff, from management consultants to cleaners.

22. One option is to ensure that contractors are not left to work unsupervised, but this can be resource intensive and impractical (but may be essential where the opportunity to cause harm is high). An alternative is to build in to any contract for services a requirement that the same checks made for government employees must be applied to any contractor and that the contracting company must be able to demonstrate that the checks have been carried out satisfactorily. Also, that such checks may be audited (even spot-checked) by the contracting organisation.

23. The same applies where staff are provided through an agency. The contract or signed agreement with the agency must clearly specify the agency's responsibilities for checking and the notification procedures they need to follow if checking has not been completed or there is cause for doubt or concern. Contracts for which a service is provided must state clearly the requirement for application of the BPSS.

24. Notwithstanding any employment checks undertaken by the agency, where the contract of employment or contract of services is between the government department and the worker, the department must still undertake document checks in accordance with the Immigration (Restrictions on Employment) Order 2007. Consideration might also be given to the production of confidentiality agreements to be signed by any non-government staff being given access to information as part of their work.

25. To assist departments with the incorporation of the requirements of the BPSS into contractual arrangements, the Crown Commercial Service has developed a range of optional Clauses that take account of the BPSS. These Clauses are specifically drafted to be used in the Crown Commercial Service Framework Agreement procurements. The Crown Commercial Service is content for departments to use these Clauses in their own contracts, with the recommendation that qualified advice is sought on their use and applicability.

26. The Crown Commercial Service has made its guidance available to all its suppliers and buyers via their website; http://ccs.cabinetoffice.gov.uk/.

27. With regard to contractors, departments and agencies **must**:

- Conduct regular monitoring of the contractor's compliance with the contract.

- Ensure contractors provide staff who meets all legal requirements, e.g. security staff hold an appropriate Security Industry Authority (SIA) Licence where required.
- Where appropriate, establish that the contractor is part of a recognised professional scheme for accrediting standards in that industry (e.g. the Security Industry Authority's (SIA) Approved Contractors Scheme for security contractors[3]).
- Agree with the contractor a joint system involving passes, photo ID and staff lists for confirming that any individual working on the contract is indeed the person who turns up (i.e. different colours or types of passes can be issued to staff with access to different areas thus allowing immediate recognition of anyone who has strayed into an area to which they do not have legitimate access. It is important to record the issue of passes, monitor and review their use and to retrieve passes that are no longer required).
- Agree a procedure for substituting temporary replacements when the usual contract staff are away or unavailable.
- Consider a staged approach to an individual's access to privileged information or to large amounts of cash.
- Where practicable, supervise contract staff whenever they are on the premises, or when they have access to particularly sensitive areas.

28. The contract manager will normally have responsibility for monitoring performance against the contract. If it is considered necessary, departments and agencies should nominate a separate member of staff to be responsible in personnel terms for contract and agency staff (i.e. not merely for overseeing delivery of the contract) so that potential security problems such as conflicts of loyalty may be identified and addressed at an early stage.

Agency and contract staff must be subject to the same pre and post appointment checks as permanent staff. Departments and agencies must have in place manageable arrangements for checking these categories of staff. It is ineffective to apply personnel security controls to permanent staff if non-permanent staff are then allowed access to premises and information without the same rigorous checks having been carried out.

Other ways to reduce risk from the 'insider' threat

29. Much of the advice in this document reflects good recruitment and employment practice, but personnel security can raise difficult and sensitive issues for employers and employees alike. It is important to ensure that any measures taken are demonstrably proportionate to the perceived risks and that, as far as possible, staff understand the risks and accept the measures taken to mitigate them.

30. In addition to the measures covered elsewhere in this document, departments and agencies must:

- Operate 'need to know' and 'clear desk' policies where possible, restricting access to sensitive locations, assets or information to those staff who need it.

[3] Where supplying companies can demonstrate that their own pre-employment screening controls provide the same degree of assurance as the rigorous application of the BPSS, there will be no need for departments and agencies to carry out duplicate checks on an individual.

- With appropriate legal advice, consider random searching on entry and exit of staff in particularly sensitive areas, making allowance for the fact that this is intrusive and that staff need to appreciate the reasons for it.

The CPNI provides further guidance on reducing the risk from the 'insider threat' at: http://www.cpni.gov.uk/advice/Personnel-security1/

Departments and agencies must ensure that employees are made fully aware of their personal responsibility to apply the 'need to know' principle within their own area of activity. They should be instructed that if there is any doubt about giving access to sensitive assets to other individuals, or organisations, they should consult their line manager or a member of the organisation's security staff before doing so.

HMG BASELINE PERSONNEL SECURITY STANDARD

PART II – THE VERIFICATION PROCESS

Procedures for the BPSS

1. Departments and agencies are responsible for carrying out the BPSS for their own employees, and for ensuring that non-List X contractors carry out equivalent checks for their employees. For List X contractors and sub-contractors, the Security Controller, or an authorised individual briefed by the Security Controller, is responsible for carrying out the BPSS.

2. The BPSS comprises verification of the following four main elements, which are described below:

- **Identity**
- **Nationality and Immigration Status (including an entitlement to undertake the work in question)**
- **Employment history (past 3 years)**
- **Criminal record (unspent convictions only)**

Additionally, prospective employees are required to give a reasonable account of any significant periods (6 months or more in the past 3 years) of time spent abroad.

Information collected at each stage of the process must be reviewed and assessed, and recorded on the BPSS Verification Record (see Annex B). Refusal by the individual to provide any of the required information should be taken into account in the employment decision.

Verification of identity (paper-based system)

Verification of identity is essential before any individual can begin their employment. Identity can be verified by physically checking a range of appropriate documentation (e.g. passport or other photo ID together with utility bills, bank statements, etc) or by means of a commercially available ID verification service.

3. The increasing availability of good quality false documentation makes establishing identity difficult; particularly so if un-trained and busy line managers are expected to spot sophisticated fraudulent documents. However, unless identity is confirmed, any other checks that might be done become meaningless.

4. During the recruitment process, and in advance of any firm offer of employment, individuals must, as a minimum, be asked to provide:

- Confirmation of name, date of birth and address.
- National insurance number or other unique personal identifying number where appropriate (see paragraph 14).
- Full details of previous employers (name, address and dates), over the past 3 years.
- Confirmation of any necessary qualifications/licences.
- Educational details and/or references when someone is new to the workforce when these are considered necessary.
- Confirmation of permission to work in the UK (a separate verification of nationality and immigration status should still be carried out prior to the commencement of employment and must be undertaken if an excuse against a civil penalty liability is to be obtained by the employer. (Paragraph 17, Immigration and Nationality status).

5. This information must be checked to ensure that there are no obvious gaps and that it is consistent by cross-referencing the data provided.

Useful identifying documents

6. The individual's full name and signature, date of birth and full permanent address should be corroborated using as many of the following qualifying documents as is considered necessary on a case-by-case basis. If, in exercising risk management, the required level of assurance can be obtained by the production of a single document, this must include a photo of the individual. Any photograph or identifying information (such as date of birth indicating age) contained in the corroborating document should be compared with the physical appearance of the individual.

Where a signature has not been provided (e.g. because of an e-application) the individual should be asked to provide it at a later date (e.g. at interview) for checking against relevant documentation. It is also good practice to request the same documentation the subject presented at interview on the first day of employment.

Only original documents should be used for identification purposes. Copies are <u>not</u> appropriate.

- Current signed full passport, travel document National ID Card and/or other documentation relating to immigration status and permission to work (see further guidance in the 'verification of nationality and immigration status' section of this paper).
- Current UK photocard driving licence (www.dvla.gov.uk)
- Current full UK driving licence (old version).
- Current evidence of entitlement to DWP benefits (e.g. Universal Credit)
- Building industry sub-contractor's certificate issued by HMRC.
- Recent HMRC tax notification.
- Current firearms certificate.
- Birth certificate (long version only).

- Adoption certificate.
- Marriage certificate.
- Divorce, dissolution or annulment papers.
- Civil Partnership certificate
- Citizencard (http://www.citizencard.com)
- Gender recognition certificate.
- Police registration document.
- HM Forces identity card.
- Proof of residence from a financial institution.
- Record of an official home visit ***.**
- Confirmation from an Electoral Register search that a person of that name lives at that address *.
- Recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms *.
- Local authority tax bill (valid for current year) *.
- Bank, building society or credit union statement or passbook containing current address *.
- Recent original mortgage statement from a recognised lender *.
- Current local council tenancy agreement *.
- Court order *.

7. There is no definitive list of identifying documents and not all documents are of equal value. The ideal is a document that is issued by a trustworthy and reliable source, is difficult to forge, has been dated and is current, contains the owner's name, photograph and signature, and itself requires some evidence of identity before being issued (e.g. a passport or ID Card). Those marked with an ***** should be recent (at least one should be within the last six months unless there is good reason why not) and should contain the name and address of the registrant.

8. Where individuals do not have photo ID, they should be asked to provide additional identifying documents from the list. Where they are unable to provide adequate identifying documents (e.g. because of age, lack of residence, etc), departments and agencies should exercise discretion taking into account all other material obtained through the recruitment process. Where this appears genuinely to be a problem, the individual should be asked to provide a passport sized photograph of him/herself endorsed on the back with the signature of a person of some standing in the individual's community (e.g. a JP, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager, civil servant, etc) and accompanied by a signed statement, completed by the same person, stating the period of time that the individual has been known to them (minimum 3 years). The statement itself, should always be checked to ensure that the signature matches the one on the back of the photograph and that it contains a legible name, address and telephone number. The signatory should be contacted to confirm their status and check that he or she did, in fact, complete the statement.

In circumstances where verification of identity was not straightforward but a decision is nevertheless taken to employ the individual(s), departments and agencies must accept and record any associated risk.

Verification of identity (at cost via a commercial service)

9. As an alternative to the paper-based system for verifying an individual's identity, departments and agencies may wish to use an electronic identity check system. This involves a fundamentally different approach, which does not rely on any physical assessment of paper documents. Instead, it seeks to assess the likelihood that a given identity exists and that the individual actually owns that identity by checking and cross-referencing information held in large and diverse databases (e.g. Electoral Roll, utility company records, bank records, etc). By searching these databases for records associated with the name, date of birth and address(es) provided by an individual, it is possible to build a picture of that individual's past life.

10. If that picture lacks detail or depth, it is possible the identity is fraudulent. If the picture shows a long history of varied transactions or events, it is more likely the identity is genuine. That is not to say the individual is the rightful owner of that identity, just that it exists – the electronic check should be followed up by testing the individual's knowledge of the information obtained. If a significant amount of information exists about a given identity, but the individual is able to corroborate only a portion of it, further questions might well be justified.

11. There are a number of products on the market which potentially offer significant benefits over the paper-based system by:

- Providing a more objective assessment of the likelihood that an individual is who they say they are.
- Offering significant benefits in terms of speed and convenience.
- Being capable of quick and easy adoption with only minimal training for the staff carrying out this work.

12. If departments and agencies wish to use such a service, they should make their own arrangements with an appropriate service provider through their usual procurement channels.

It is conceivable that some individuals would not appear on such services (e.g. if they opt out of the edited electoral roll, do not hold credit cards and do not have bills held in their own name). In such circumstances, any appointment decision based purely on an automated process must be open to applicants to challenge and to ask for human intervention, as per Article 22 of GDPR 2016/679. Also, in employment and data protection terms, departments and agencies should exercise caution unless fully persuaded of the timeliness and veracity of the information provided.

Further advice and guidance on identity and document verification

13. There are a number of other useful sources of reference material which departments and agencies may wish to draw on when considering identity (the list is not exhaustive)[4]:

[4] This is an illustrative list only – we express no opinion on the quality of service provided by the named suppliers and an Internet search will reveal the names of other suppliers.

- Guidance on ID documentation is available from the Centre for the Protection of the National Infrastructure (CPNI) 2017: https://www.cpni.gov.uk/system/files/documents/f2/0b/pre-employment-screening-document-verification-guidance.pdf

- Further useful key resources providing information on aspects of identity and document fraud are available online:

- http://www.renful.co.uk/index.php?ID=s5
- https://keesingreferencesystems.com
- http://www.dvla.gov.uk/media/pdf/leaflets/inf60x7.pdf
- www.identitytheft.org.uk

National Insurance Number (NINO) Record Check (via HMRC)

14. National Insurance numbers (NINOs) can be acquired fraudulently and cannot be relied upon as a sole means of establishing identity or right to work. Temporary numbers beginning with TN or ending in a letter from E to Z inclusive are not acceptable.

15. Where an individual has provided their NINO as a means of identification, and there is any doubt as to its authenticity, departments and agencies can check against HMRC records. A search in the area of 'Trace National Insurance Number' on the website https://www.gov.uk/government/organisations/hm-revenue-customs will lead to a form (CA6855) which can then be printed off, completed and faxed to 0191 225 7660. Such a check should be made on an exceptional basis only where other documentation already supplied by an individual is insufficient for the need.

Verification of nationality and immigration status (including an entitlement to undertake the work in question)

Nationality and immigration status can be verified by physically checking appropriate documentation or, in exceptional circumstances only, by means of an independent check of UK Visas and Immigration (UKVI) records.

16. Departments must take the necessary steps to ensure that an individual has the right to remain in the United Kingdom and undertake the work in question.

The Immigration, Asylum and Nationality Act 2006

17. Immigration and nationality checks are based on the current provisions on preventing illegal migrant working in the UK as set by the Immigration, Asylum and Nationality Act 2006. These provide that an employer may be liable for a civil penalty by employing someone subject to immigration control aged over 16 who does not have permission to be in the UK or to undertake the work in question. An employer may establish an excuse against this civil penalty liability by undertaking specific documentary checks on the individual before the employment commences in accordance with the Immigration (Restrictions on Employment) Order 2007. Further details can be found at:

https://www.gov.uk/government/collections/sponsorship-information-for-employers-and-educators

18. Whilst government departments and agencies may have no civil penalty liability because of crown immunity, they are still required to undertake all appropriate document checks. Where the individual has a limited entitlement to remain in the UK, the BPSS requires repeat checks to be undertaken not less than twelve months after the previous check was undertaken or, if sooner, before the previous leave has time expired. This will ensure that migrant workers will not be able to continue working in a government department or agency after their leave has expired up until the next annual check. These checks will not be required once the employee can demonstrate that he or she has indefinite leave to be in the UK by producing appropriate documents or the employment comes to an end. Documents that demonstrate that the employer has established an excuse from a liability for employing an illegal migrant worker must be retained during the period of employment and for not less than two years after the employment has come to an end.

Further guidance on immigration can be found at:

https://www.gov.uk/government/organisations/uk-visas-and-immigration

19. The UKVI provides support to employers through its Employer Checking Service. It is recommended that employers read the available online guidance before using these services. Further details can be found at:

https://www.gov.uk/check-an-employees-right-to-work-documents

20. Departments should be aware that the employment of migrants from outside the European Economic Area (EEA) and Switzerland is subject to the points-based system. Further information about the system can be found at:

https://www.gov.uk/uk-visa-sponsorship-employers

21. Checks need to be applied evenly, and employers will need to be aware of their obligations under the Race Relations Act. For example, all individuals should be required to provide this evidence and not just those who appear to be migrants. Individuals should be asked to complete the Nationality and Immigration Status Check Form at **Annex C**, and departments and agencies should corroborate the information against the required document or documents listed in the guidance referred to in paragraph 20. The document(s) should be copied, and the copies retained by the department or agency, as explained above.

Civil Service Nationality Rules

22. In addition to the Asylum and Immigration Act 2006, eligibility for employment in the Civil Service, including the Diplomatic Service, on grounds of nationality is governed by the Civil Service Nationality Rules. About 95% of Civil Service posts are also open to Commonwealth citizens and nationals of any of the member states of the European Economic Area (EEA), Switzerland and Turkey. The remaining posts, which require special allegiance to the state, are *reserved* solely for UK nationals only. Those with dual nationality with one part being British are, in principle, eligible however they may not be eligible for employment in certain reserved posts where additional nationality requirements are imposed.

23. To assess a candidate's eligibility under the nationality rules, a check should be carried out either against a full passport or national identity card or, where this is not available, a Home Office document confirming the individual has the required nationality and immigration status for the post. Care should be taken in carrying out this check. Apart from the obvious potential for the use of forged documents, certain Home Office documents presented in isolation may not definitively establish the person's current status. In many instances, immigration status may change, and it should be checked that the document accurately represents the up-to-date position. Candidates with dual nationality are eligible for appointment to non-reserved posts provided that part or all of their nationality satisfies the appropriate Civil Service nationality rules. Further information on civil service nationality rules can be found at: https://www.gov.uk/government/publications/nationality-rules.

Immigration employment enquiry (via UKVI)

24. Where an individual's nationality and immigration status cannot otherwise be verified or where the check has been carried out and concerns remain, an independent check of UKVI records may be carried out. Such checks should be carried out on an exceptional basis only where other information/documentation already supplied by an individual is insufficient for the need.

25. Where such a check is necessary, departments and agencies should contact UKVI's Employers and education providers' helpline on 0300 123 4699.

- The employer checking service can check an individual's right to work if they have an outstanding application or appeal with UKVI, validate an application registration card or validate a certificate of registration. Further information on the employer checking service and the form required can be found on:

  https://www.gov.uk/check-an-employees-right-to-work-documents

  https://www.gov.uk/government/publications/employer-checking-service-form-check-employees-right-to-work

26. If departments and agencies require further information about an individual following the 'right to work' check, the employer checking service may be able to provide that information. Any further enquires should be made to the employer checking service in the first instance.

Verification of Immigration and Nationality documentation – sources of further guidance

- 'A Guide to the Detection of Passport Fraud' – Advice from the National Document Fraud Unit (part of the Home Office) to help in the detection of forged travel documents. It is a basic introduction to the subject of passport fraud and is aimed at those departments and agencies which are presented with identity documents in the course of their work. The 'Guide' is a Microsoft PowerPoint-based self-managed learning CD Rom which can also be used as the basis of

a trainer-led presentation and is normally available to HMG and some corporate bodies only.

- The Centre for the Protection of the National Infrastructure (CPNI) provides guidance on Document Verification, which can be accessed at:

  http://www.cpni.gov.uk/advice/Personnel-security1/Screening/

  https://www.cpni.gov.uk/system/files/documents/f2/0b/pre-employment-screening-document-verification-guidance.pdf

- The European Union launched in 2007 the PRADO website or Public Register of Authentic Documents Online. It contains images and information relating to passports, visas, residence permits, driving licences and other identity and travel documents issued by EU member states. This includes details of their first level security features and how to check their authenticity. The website is available in all the official languages of the EU and can be accessed at:

  www.consilium.europa.eu/prado/EN/homeIndex.html

  A version for control authorities called iFADO containing a higher level of information on False & Authentic Documents Online is also being rolled out across the government secure internet. Details about this can be obtained from the National Document Fraud Unit.

- The HM Passport Service runs the 'OmniBase Service' which provides a web interface into their database of issued passports. It allows, at cost, verification of an individual's passport and a check of its status. Approved departments and agencies will be able to operate the programme using an internet browser. Further information is available from:

  HM Passport Service
  Globe House, 8th Floor
  89 Ecclestone Square
  London
  SW1V 1PN

https://www.gov.uk/government/organisations/hm-passport-office

Verification of employment history (paper-based system)

Employment history can be verified by checking with previous employers and/or by following up references or by means of a commercially available CV-checking service or, by Civil Service Resourcing Electronic Employment History Check.

27. To ensure that prospective employees are not concealing associations or gaps, employing departments and agencies should, as a minimum, verify recent (past 3 years) employment or academic history. Approaches to a previous and/or current employer should not be made without the individual's prior written permission. For periods of self-employment, evidence should be obtained (e.g. from HMRC, bankers,

accountants, solicitors, trade or client references, etc.), confirming that the individual's business was properly conducted and was terminated satisfactorily.

28. Appropriate references can verify employment history and may also provide an additional means of verifying an individual's identity and integrity. However, there is an increasing reluctance on the part of employers to provide frank and timely comments on an individual's character and suitability for employment because of DPA/FOI concerns, even for internal postings. They can also add severe delays to the recruitment process. So, although departments and agencies may continue to seek suitable references if they wish, they are not required as part of the BPSS. Where references are sought these must be checked by:

- Telephoning the author to confirm they provided the reference. In these circumstances, the telephone number should be ascertained independently. A telephone number supplied by the individual being checked should not be relied upon.
- Checking the existence of the employer (e.g. that it appears in the phone book or relevant business directories).

Where the BPSS is being carried out as the groundwork for national security vetting, employment history should, as a minimum, be verified for the past year. Any employer, academic or personal reference, if required, should cover the same period.

29. Departments and agencies may wish to use the BPSS Employment History Report Form at **Annex D** when seeking verification of employment history. It is designed to help former employers provide relevant information about the individual and minimise the effort involved to prompt a quick response.

30. Otherwise, departments and agencies may wish to email former employers for confirmation of an individual's employment history. In these circumstances, email addresses should be ascertained independently. An email address supplied by the individual being checked should not be relied upon. The telephone can be used to check details already provided (e.g. in writing or by email), but it is not recommended as an initial or sole means of verifying employment history unless it is clear that the person on the other end is who they claim to be. Where the telephone continues to be used for this purpose, the details should still be recorded.

Verification of employment history (CV check) (at cost via a commercial service)

31. Alternatively departments and agencies may wish to use an electronic CV checking system; there are a number of commercially available products on the market. Typically, these companies can provide online confirmation of name and address, date of birth, current and previous employment, qualifications and further education, membership of professional/trade bodies, current and disqualified directorships, employee/character references, etc.

32. It is for departments and agencies to decide whether a commercially available CV checking service is an effective option for them in meeting the BPSS. If departments and agencies wish to use such a service, they should make their own

arrangements with an appropriate service provider through their usual procurement channels.

It is conceivable that some individuals would not appear on such services. In such circumstances, any appointment decision based purely on an automated process must be open to applicants to challenge and to ask for human intervention, as per Article 22 of GDPR 2016/679. Also, in employment and data protection terms, departments and agencies should exercise caution unless fully persuaded of the timeliness and veracity of the information provided.

Government Recruitment Services Electronic Employment History Check

33. Government Recruitment Services can provide Electronic Employment History Checks either as part of their full recruitment service for departments or on a bespoke basis for departments not using the full service. Further information is available from:

Customer Acquisition Team
Government Recruitment Service
BP 2301 Lindisfarne House
Benton Park View
NE99 1ZZ
Tel: 07464 644 895
Email: newbusiness.grs@cabinetoffice.gov.uk

Every effort should be made to check that the individual has held the previous employment he/she claims. Any gaps in employment history (past 3 years) should be investigated.

Verification of criminal record ("unspent" convictions only)

The requirement to verify "unspent" convictions does not apply when the BPSS is being carried out as part of the groundwork for national security vetting, where a full check of criminal records (both "spent" and "unspent") will be made as part of that process.

34. Under the terms of the Rehabilitation of Offenders Act 1974, it is reasonable for employers to ask individuals for details of any "unspent" criminal convictions. The Act states that if an offender remains free of further convictions for a specified period (the "rehabilitation period") the conviction becomes "spent". Where rehabilitation has taken place, an individual must be treated as if the offence had never been committed. Under the Act, a rehabilitated person is not normally required to disclose "spent"

convictions when applying for a job (although there are some exceptions under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 e.g. National Security) and such convictions, or failure to disclose them, are not permissible grounds for exclusion from employment. Special care should be taken when dealing with evidence of convictions to ensure that "spent" convictions are identified and disregarded. (For Northern Ireland, the legislation relevant to rehabilitation is the Rehabilitation of Offenders (Northern Ireland) Order 1978 and the (Exceptions) Order 1979. Rehabilitation periods may vary for Northern Ireland. Legal advice should be sought in cases of doubt).

Further information on the Rehabilitation of Offenders Act can be found at:

www.nacro.org.uk , www.lawontheweb.co.uk

Basic disclosure certificate (at cost via Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland)

35. Disclosure and Barring Service (DBS) and Disclosure Scotland offer checks of 'unspent' criminal records through their Basic Disclosure service. From 1 February 2018, DBS should be used to conduct the check for a job in England and Wales. If the job is in Scotland then Disclosure Scotland should be used to conduct the check. Further information on DBS checks can be found at https://www.gov.uk/government/organisations/disclosure-and-barring-service.

36. Further information on the DBS Basic Disclosure Service can be found at https://www.gov.uk/request-copy-criminal-record

37. Further information on Disclosure Scotland's Basic Disclosure service can be found at https://www.mygov.scot/disclosure-types/?via=http://www.disclosurescotland.co.uk/. The check should be, as far as practicable, confined to applicants whom it is intended to appoint and departments, agencies and List X contractors should avoid requiring all short-listed applicants to obtain a Basic Disclosure.

38. Prior to 1 February 2018, Disclosure Scotland provided the unspent criminal record check not only for people working in Scotland but also in England and Wales. Basic Disclosure Certificates contain details of convictions considered "unspent" under the Rehabilitation of Offenders Act 1974. They are not job specific and are generally only issued to the applicant, but can be provided direct to departments and agencies and List X contractors with the individual's prior approval. It can be used more than once, although for obvious reasons it has a limited shelf-life. You must note that different rehabilitation periods apply to England and Wales to those of Scotland and Northern Ireland. The rehabilitation periods in Scotland are longer than that of England and Wales, so failure to use the correct organisation for basic checks could impact on the content of the certificate and leave employers at risk of legal challenges for accessing information they were not entitled to view.

39.

40. Departments, agencies and List X contractors may also want to consider whether or not they plan to bear the cost of a Basic Disclosure or require new entrants to meet this cost.

41. Where an individual provides his or her own Basic Disclosure, departments should ensure that the certificate matches the identity documents of the individual and

that receipt and retention of this information is in accordance with existing data protection legislation. It is recommended that retention of Basic Disclosures should not exceed 90 days. In summary departments should:

- Record the outcome of the disclosure in the subject's personal file.
- Prepare a suitable risk assessment in the event of a negative outcome. The risk assessment should provide the basis for any ongoing personnel security enquiries.

42. Disclosure Scotland recommends that larger departments and agencies that require a substantial number of Basic Disclosures register as 'Responsible Bodies' with Disclosure Scotland. DBS also provide the same service, where larger departments can register themselves as a Responsible Organisation (RO). The candidate will need to provide identity documents to the RO to support their application.

43. The benefits of registration are: control of applications being submitted and visibility during processing; volume tracking; invoicing facility; and minimal administration.

44. Where departments and agencies need to verify unspent criminal convictions of an individual who resides or has resided in Northern Ireland, a Basic Disclosure service is available from Access Northern Ireland (AccessNI) which has access to both Northern Ireland criminal records and the Police National Computer (PNC). This service can be accessed by individuals or by departments if they register as a responsible body with AccessNI.

Further details can be found on: www.accessni.gov.uk

45. Departments and agencies should not share with other employers the information obtained through a Basic Disclosure. They should also abide by DBS's, Disclosure Scotland's and AccessNI's Codes of Practice in obtaining and handling disclosure information.

46. Where it is not possible to obtain a certificate from DBS, Disclosure Scotland or AccessNI because of a lack of UK residence, departments are advised to take a proportionate risk assessed approach in these instances and consider alternative courses of action. For example, the Security Industry Authority (SIA) offers advice on obtaining overseas police certificates on their website www.the-sia.org.uk. More details on these services can be found in Part III of this guidance.

Criminal record declaration

47. Carrying out criminal record checks via DBS, Disclosure Scotland or AccessNI means that there is no need for individuals to complete a Criminal Record Declaration Form. However, if departments continue to request a declaration of unspent criminal record prior to the provision of a Basic Disclosure Certificate, they should be prepared to manage those instances where the self declaration has omitted details of unspent criminal record and whether or not this was deliberate or a genuine oversight. For reasons of transparency, where departments continue to request self-declaration in addition to the Basic Disclosure, the Criminal Record Declaration Form should make clear that a check of unspent criminal record will be carried out.

Consideration of unspent convictions

48. When "unspent" convictions have been disclosed, departments and agencies will wish to consider:

- Whether the offence would cast doubt on the individual's or organisation's reputation.
- Whether the offence would affect an individual's ability to do the job.
- Whether the conviction is relevant to the particular post (e.g. a fraud related conviction might be relevant to a finance post but may not be a problem in other posts; convictions for protest/extremist acts such as those connected with animal rights may be more of a problem for one organisation than another; etc).
- The length of time since the offence occurred.
- The nature and background of the offence (e.g. violent crime or a history of violence which may impact on an organisation's duty of care to its staff).
- The seriousness of the offence.
- Whether there is a pattern of offences.

49. Departments and agencies will need to decide whether an individual may not be generally reliable and, if so, whether that represents a risk. Particular attention should be given to cases in which two or more adverse factors are combined. Any initial doubts about where an individual is posted should be well recorded so that the point(s) is not missed in the future. It is strongly recommended that departments and agencies seek legal advice where appropriate.

50. A number of guidelines are available on the internet that provide help in making judgements around whether or not to employ somebody with a criminal record:

'Employing people with criminal records" – (a Chartered Institute of Personnel and Development (CIPD) fact sheet: www.cipd.co.uk/subjects/dvse"qul/exoffenders/crimrec.htm?SrchRes=1

"Employing ex-offenders – A practical guide" (Assessing the relevance of criminal records) – a joint CIPD and CRB publication: http://www.unlock.org.uk/userfiles/file/employment/employing%20ex-offenders%20a%20practical%20guide.pdf

NACRO's guidance: 'Recruiting ex-offenders: the employers' perspective' available on the CRB's website: http://www.nacro.org.uk/data/files/nacro-2006070300-216.pdf

NACRO: "Guide to recruiting people with criminal records': http://www.nacro.org.uk/data/files/nacro-2005020104-302.pdf

Reasons for concern and checking documentation

51. In applying the BPSS, there are a number of factors which may, separately or in combination, raise concerns. In these circumstances departments and agencies should consider the risks involved in an offer of employment. These factors include:

- Involvement in illegal activities.
- False or unsubstantiated claims on a CV or application form.
- Unsubstantiated qualifications.
- Relevant "unspent" criminal convictions, particularly if not declared by the individual but only revealed by other sources.
- Unexplained gaps in employment history.
- Bad or false references.
- Questionable documentation (e.g. a lack of supporting paperwork or concern that documents are not genuine).
- Evasiveness or unwillingness to provide information on the part of the individual.

52. If individuals are rejected it is important to be clear about the reasons for rejection, and record these appropriately. There is always the possibility of the failed individual seeking some redress, in which case a comprehensive record of decisions and action taken will be important.

53. The rigorous application of the checks outlined in this document is dependent on effective document verification. Staff carrying out the checks need to ensure that they are completely satisfied with the information that the individual has provided, and know what to do should inconsistencies emerge between that information and what the checks have discovered. In these circumstances, applicants should be allowed an opportunity to explain any discrepancies (they might be genuine errors). It is also important that the process is carried out in as timely a fashion as possible, but it is even more important to be confident of the individual's honesty and integrity.

If discrepancies are found in any documentation or information supplied by the individual, further enquiries should be conducted and the individual given an opportunity to explain.

HMG BASELINE PERSONNEL SECURITY STANDARD

PART III – ADDITIONAL CHECKS

Additional verification

1. In addition to the core checks, where additional verification or assurance is required, departments and agencies may consider applying other checks, some of which are described below. To help comply with data protection legislation, departments and agencies should explain the nature of and sources from which information might be obtained about the applicant in addition to the information supplied directly by the applicant. This might be done, for example, by way of a clear statement on any forms required for the purpose of additional verification.

2. If it is necessary to secure the release of documents or information from another organisation or person, departments and agencies should obtain a signed consent form from the applicant (the forms used as part of the BPSS should provide for this) unless consent to their release has been indicated in some other way. If this is the case, it should be recorded on the BPSS Verification Record (**Annex B**). It should be remembered that misleading another person or organisation into providing personal information about an applicant may be regarded as a criminal offence.

Applicants should not be forced to use their subject access rights to obtain records from another organisation (i.e. by making such a requirement a condition of getting a job).

Internet Check

3. A search of the Internet cannot be relied upon to verify identity; some information may be untrue or out of context, but it can be used on an ad-hoc basis to reinforce current procedures. It must be noted that collecting public domain information on individuals falls under data protection legislation and therefore must be declared, such as via the privacy notice. Some websites/search engines that might be used, for example, are:[5]

http://www.google.co.uk/advanced_search?hl=en

http://dmoz.org/Regional/Europe/United_Kingdom/News_and_Media/Journalists.

http://www.holdthefrontpage.co.uk/peoplesearch/journo_search.asp - people search on journalists. Not good on freelancers.

http://wck2.companieshouse.gov.uk – checks current and solvent companies/ratifies employment history.

[5] This is an illustrative list only – we express no opinion on the quality of service provided by the named suppliers and an Internet search will reveal the names of other suppliers.

http://www.lexis-nexis.com – allows the world-wide research of articles published in newspapers (subscriber).

http://www.proquest.com – media related (subscriber).

http://www.friendsreunited.co.uk – international site used to contact and read information on associates from schools, universities and work places. Site also helps to confirm attendance and other names used.

http://www.iana.org – country email index which can provide confirmation of worldwide email domains.

www.nominet.org.uk – internet registry for querying UK domain names.

www.1837online.com – genealogy searches.

www.linkedin.com – people search.

http://www.yahoo.com - source individual's personal profiles.
http://www.hotmail.com - source individual's personal profiles.
http://www.msn.com - source individual's personal profiles.

4. Internet checks will vary in value, but the few seconds that it takes to carry them out might be worthwhile and provide some additional assurance, particularly if carried out early on in the process.

Overseas Check (where a lack of UK residence requires it)

5. Where it is not possible to carry out meaningful checks in the UK because of a lack of UK residence, prospective employees are required, as part of the BPSS, to give a reasonable account of any significant periods (6 months or more in the past 3 years) of time living abroad. Early notification of the need to provide such evidence is essential to prevent unnecessary delays in the process. This requirement should be included in job adverts/advertising campaigns.

6. Individuals might be asked to provide the alternative (original) documentation shown below. These examples are intended to illustrate how suitable assurance may be established, but should not in themselves be treated as prerequisites for employment:

- Suitable proof of residence for time spent abroad.
- Overseas employee or academic references.
- Character references (e.g. from fellow UK travellers/students), which should be clearly written and quote dates and places of meeting.
- References from UK departments and agencies based overseas (e.g. FCO missions, British Council, non-Government Departments and agencies (NGOs)).
- Where available, official and verifiable overseas police certificates obtained from the country or countries of residence (see paragraphs 9-12 below).

Confirmation of dates should be obtained from passports and work permits by contact with appropriate Embassies, High Commissions and Consulates.

7. A lack of UK residency, in itself, should not be an automatic bar to employment. Where documentary evidence for time spent overseas is not available, departments and agencies should consider what additional assurance may be gained from a face-to-face interview with the individual and the merits of any special aftercare procedures, including early reviews following a period of UK residence. However, it should be recognised that where meaningful background checks cannot be carried out and sufficient assurance cannot be gained by other means, it might not be possible to employ the individual. This may in no way reflect on the honesty and integrity of the individual, just that the required background checks in the country or countries of residence prior to arriving in the UK were simply not possible.

8. Departments may wish to make use of the backgroundchecking.com service provided by Experian, which provides for checks to be made with overseas records, as part of their recruitment process. Further information can be found at:

http://www.experian.co.uk/background-checking/why-background-check.html

Overseas Criminal Record Checks (Security Industry Authority (SIA))

9. The SIA are not able, at present, to offer any direct support to departments and agencies and List X contractors wishing to obtain overseas criminal record certificates. However, they have produced a helpful (alphabetical) guide to obtaining overseas police certificates, which can be found on their website www.the-sia.org.uk (then search e.g. for 'Overseas Residents' or 'Criminal Record Certificates'). The guide is periodically updated, so look out for changes. The SIA's approach centres around UK-based foreign Embassies and High Commissions. Where there is no information about a particular country, the relevant Embassy or High Commission can always be contacted for advice. The SIA also provides advice on the reliability, accuracy and authenticity of the information that can be obtained via this process.

10. The quality of information provided differs from country to country. The SIA do not have a graded list of how any particular country fares against another but it has built up an understanding of the processes involved (to request a check), a stock of verified samples and contacts from various criminal record issuing authorities in case they need to authenticate a document back to source.

11. The key points to note are: the type of 'certificate' issued; the conditions of issue; and how it was obtained. Dealing with foreign countries will undoubtedly throw up many different ways of working but there is a balance to be struck between what is required and what can be obtained. An example is Pakistan, where applicants can, if they wish, apply directly to their regional Police HQs. There is no central body that covers all of Pakistan but the High Commission in London can authenticate 'certificates' back to source thereby confirming that they are genuine and satisfying the SIA's needs.

Overseas Criminal Record Checks

12. The Disclosure and Barring Service, Disclosure Scotland and Access Northern Ireland are unable to access overseas criminal records. You will need to ask the individuals to access their own criminal record abroad. Further information can be found at:

https://www.gov.uk/government/publications/criminal-records-checks-for-overseas-applicants

If you find that a Basic disclosure certificate that you have received contains the details of an overseas criminal record, this will be because it is one of a small number of overseas records that are already held on the Police National Computer.

Animal Rights Extremists

13. A number of government departments and agencies assess themselves to be potential targets for vexatious and extreme animal rights protests.

14. For a range of legal and practical reasons there is no police or government database of individuals involved in extremist animal rights activities. However COGSS are aware of two commercial organisations, Huntingdon Life Sciences (HLS) and Agenda Security Services, who can offer screening for animal rights affiliations. Both organisations gather open source information on individuals involved in extreme and vexatious animal rights campaigns. Other providers may also be available.

Huntingdon Life Sciences and Agenda Security Services can be contacted at:

Pro-Active Security Solutions (Huntingdon Life Sciences)

E-mail - info@pa-ss.com

Address
Security Administration
Pro-Active Security Solutions
BCM Pa-S.S.
London
WC1 3NXX
Tel. 01954-261392
Fax. 01954-261372

Agenda Security Services

E-mail - norman@agenda-rm.co.uk

Address
Norman Mortell, BA (Hons)
Director of Operations
Agenda Security Services
Tel: 08456 445546
www.agenda-security.co.uk

15. Departments will want to carefully consider the circumstances in which they would carry out a check of this nature. Use of these services should be proportionate

to the requirements of the BPSS and, in the interests of transparency, potential employees should be made aware they will be subject to a check of these records. Therefore, it is strongly advised that departments carry out and record a rigorous risk assessment to determine which posts are at risk from vexatious animal rights activists. Also, it should be made clear to individuals about to take up posts designated to be at risk that they will be subject to this extra layer of pre-employment screening in the usual way (e.g. recruitment literature, vacancy notices etc.).

HMG BASELINE PERSONNEL SECURITY STANDARD

PART IV – POST VERIFICATION PROCESS

Recording checks and results of the BPSS

Departments must complete and retain a BPSS Verification Record; this document is the official record of the successful completion of the core checks and when they were conducted. The completed form can provide for transfers between departments and agencies and the basis for any subsequent national security vetting checks (where necessary).

1. BPSS checks carried out must be recorded on a Verification Record **(Annex B)** and reflected in the Security Questionnaire for any subsequent national security vetting. The record should also clearly indicate the immigration status of the employee and whether the immigration status needs to be rechecked as described in Part II of this guidance.

2. The completed verification record must be retained on the individual's personal file. If necessary, to ensure that all necessary checks have been undertaken, the form should be signed by a senior responsible officer, so ensuring a sense of ownership and accountability. Given the increased online delivery of HR services and the use of interactive forms, the electronic recording of checks, results and audit trails are acceptable.

3. Given the potential nature of the information to be recorded, some of which could be sensitive personal data under data protection legislation, it is important that access to such information is restricted to those with a true need to know the information held on such forms.

Transfer of documentation

4. Where an individual transfers from one organisation to another, the receiving department, agency or contractor must satisfy themselves that the BPSS has been met. To help do this, they may request from the supplying department or agency or contractor copies of the completed BPSS Verification Record **(Annex B)** and any associated documentation where this has been retained. Departments, agencies and contractors are reminded of their obligations when sharing personal data. Any response to a request for a BPSS Verification Record and associated documentation must be consistent with the requirements of this document.

5. In industry, receiving Security Controllers must confirm the individual's identity and immigration status and may also seek a suitable reference from the supplying contractor, where appropriate. Providing no more than 1 year has elapsed between

the two periods of List X employment, and the individual has not worked overseas during that period, the receiving contractor need not obtain personal references. Once the receiving contractor's Security Controller is satisfied, the BPSS may be approved and a new company Approved Access Number (AAN see below) allocated. Any additional checks required by the Contracting Authority, must be repeated if more than 10 years has elapsed since the last check. All checks and results must be recorded on a new BPSS Verification Record.

Records retention and disposal

6. Departments and agencies and List X contractors should adhere to established retention periods for recruitment records that are based on a clear business need. They should consider carefully which personal information relating to an application is to be held on the individual's employment record, and ensure that it is securely stored or is destroyed. It is recommended that, for documents relating to the BPSS, the completed BPSS Verification Record (**Annex B**) is kept, in the event that it is required e.g. for national security vetting purposes. However, supporting documentation (e.g. copies of utility bills, etc) should be destroyed within 6 months unless there is a clear business reason for exceeding this period. If there is no need to hold the information for longer, provisions of data protection legislation require that that information no longer be held. Criminal conviction information collected in the course of the recruitment process should also be destroyed unless, in exceptional circumstances, the information is clearly relevant to the on-going employment relationship. ISO17799 (Code of Practice for Information Security Management) provides guidance which, if followed, should address the main security risks of unauthorised access to, accidental loss or destruction of, or damage to employment records.

Approving or refusing the BPSS

7. Departments and agencies should decide who is responsible in their organisation for approving or refusing the BPSS. For List X contractors the HR department and, if necessary in conjunction with Security Controller, may approve the BPSS providing it is satisfied that:

- The necessary identity documents have been produced and verified.
- The appropriate references (where required) have been obtained and there is nothing to suggest reservations about the individual's suitability for employment on sensitive government work.
- The individual's nationality and immigration status allows them to undertake the employment in question.
- The individual has supplied an open criminal record declaration, showing convictions or pending prosecutions for minor offences.
- There is no other information that casts doubt on the individual's suitability for access to sensitive government assets.

8. Where any of these conditions are not met and concerns therefore arise about suitability for access to sensitive government assets, or where security concerns arise from the checks undertaken, the Security Controller must forward a copy of all the

documentation relating to the BPSS to the appropriate Contracting Authority (or where the access required is to defence information, the Defence Business Services) for further assessment. A covering letter should be sent, explaining the reasons for referral.

Post approval action

9. Once the BPSS has been approved, the individual must be briefed on local security procedures and if appropriate, the provisions of the Official Secrets Acts (OSA) 1911-1989.

Renewal of the BPSS

10. In Government, there is no requirement to renew the BPSS once it has been approved. However government departments and agencies must recheck the immigration status of migrant employees before the current leave expires or within twelve months of the previous check, whichever is the sooner. These checks must be repeated until the employee is able to demonstrate that he or she can remain indefinitely in the UK or the employment comes to an end. Government employees are required to report changes in their personal circumstances (e.g. a criminal conviction) under the Civil Service Code.

11. Where an individual, subject to the BPSS, leaves a contractor and is subsequently reemployed by the same contractor within 1 year, the BPSS may be re-established. In all other cases the full BPSS must be initiated. Appropriate immigration status checks must however be repeated in order to retain the excuse from a civil penalty liability for employing an illegal migrant worker. Whilst government departments and agencies may have no civil penalty liability because of crown immunity, they are still required to undertake all appropriate document checks.

Ongoing personnel security management (“aftercare”)

12. The necessary checks at the recruitment stage only offer a snapshot. It is essential that HR Divisions and line managers in departments and agencies, and List X contractors and sub-contractors continue to apply good personnel security management after recruitment to identify any changing or suspicious behavioural patterns in staff that might suggest unreliability or a conflict of interest. Ongoing personnel security is best achieved by creating a culture in which security is important and accepted (i.e. a security aware environment). It should be made easy for staff and managers to discuss their concerns and problems confidentially and informally, and to voice any concerns they may have about others.

13. Although in many organisations the focus in the circumstances described below would probably be more on the welfare of the individual rather than on security issues, it should be recognised that all staff can be vulnerable to circumstances that might compromise their attitudes and behaviour regardless of their professional standing and previous reliability. This can be the result of a wide range of life events from stressful personal or working circumstances to deliberate targeting and recruitment by malicious

third parties. Circumstances leading to vulnerability might be subtle and difficult to recognise but could include:

- Ill health in the individual or family.
- Financial difficulty.
- Peer, family or extended group pressure.
- Perceptions of unfairness at work.

14. In this regard, a list of behaviours that might merit closer attention is shown below. This is not a comprehensive list. Individual cases will have unique features and it may take a combination of factors to warrant further concern. (It is important to note that some of these signs may be the result of ill-health and departments should allow for this in any consideration of them.)

- Drug or alcohol abuse.
- Expressions of support for extremist views, actions or incidents, particularly when violence is advocated.
- Major unexplained changes in lifestyle or expenditure.
- Sudden loss of interest in work or overreaction or prolonged response to career changes or disappointments.
- Unusual interest in security measures, or areas of work outside the normal remit.
- Signs of stress such as excessively emotional behaviour.
- Changes in working patterns (e.g. frequently working alone or at unusual hours, and reluctance to take holidays).
- Frequent unexplained absences.
- Repeated failure to follow recognised procedures.
- Unusual travel abroad.
- Relationships with or support for individuals or institutions that are generally regarded as professionally suspect or substandard.
- Sudden or marked change of religious, political or social affiliation or practice that has an adverse impact on the individual's performance of their job or attitude to security.

15. In Government, where doubt arises as to the behaviour and/or continuing suitability of an individual, a report should be made to the Departmental Security Officer. In industry, Security Controllers should be informed who, in turn, should report to the Security Adviser or Contracting Authority. Where this is necessary, the process should be managed to ensure that the appropriate data protection safeguards are in place (i.e. that access to such information is restricted to as few people as possible and certainly only to those with a true need to know).

16. Further advice on ongoing personnel security, including advice on online social networking can be found at: http://www.cpni.gov.uk/advice/Personnel-security1/Ongoing-measures/

It is recommended that departments and agencies develop their own strategies for ongoing personnel security management consulting closely with key stakeholders (DSOs and legal advisers etc.).

Notifiable Occupations Scheme[6]

17. The Notifiable Occupations Scheme can be used as tool for managing ongoing personnel security arrangements. The scheme relates to professions or occupations which carry special trust or responsibility, in which the public interest in the disclosure of conviction and other information by the police generally outweighs the normal duty of confidentiality owed to the individual.

While there is no statutory requirement for the police to share conviction or other information about individuals with third parties, other than in the context of Disclosure and Barring Service Disclosures under Part V of the Police Act 1997, there is a common law power for the police to share information for the purpose of the prevention and detection of crime (each case being considered on its own individual circumstances).

18. The general position is that the police should maintain the confidentiality of personal information, but legal opinion supports the view that in cases invoking substantial public interest considerations a presumption to disclose conviction and other information to relevant parties, unless there are exceptional reasons not to do so, is considered lawful.

19. As part of these arrangements, police forces are requested to notify the appropriate Government department, professional regulatory/disciplinary body and/or the employer of conviction and other information when it comes to notice that an individual is working in one of the Category 1 professions or occupations listed in Category 1. Category 1 applies to professions or occupations bearing special trust and responsibility where substantial public interest considerations arise specifically in relation to:

- Protection of the vulnerable, including children;
- National security; and
- Probity in the administration of justice

20. Therefore all civil servants are subject to these arrangements and thus there is a presumption to notify in relation to all recordable convictions, cautions, reprimands and final warnings; unless there are exceptional reasons which make it inappropriate to do so.

[6] This scheme is scheduled to be reviewed by the Home Office

Compliance

21. A sound system of assurance of compliance and the spot checking of related documentation, particularly in respect of contractors, will help maintain confidence in the BPSS and the associated checks. In some departments and agencies, this may include/comprise a checking regime by e.g. the Departmental Security Officer (DSO) or Security Adviser (SA). For List X contractors, the spot checks should form part of routine visits by the Security Adviser or the Contracting Authority's Departmental Security Officer, or representative, who will need to be assured that:

- BPSS Verification Records (**Annex B**) are being completed correctly.
- That the employer has established an excuse from a civil penalty liability for employing an illegal migrant worker (or would have established an excuse in the absence of crown immunity).
- Employees retain an ongoing entitlement to undertake the employment in question.
- The associated checks are being carried out rigorously and consistently.
- Cases are being referred to the Contracting Authority where appropriate.
- Supplementary checks are being carried out only where strictly necessary and are being recorded correctly.

22. In terms of central assurance, departments and agencies should provide the Cabinet Office Government Security Group with annual confirmation of ongoing compliance with the BPSS - this will form part of the Security Policy Framework annual security return which will be completed by the DSO or SA and signed off by the Accounting Officer / Head of Department. It is recognised that, in some cases, it may not be practicable for departments, agencies and List X contractors to fully meet the requirements of the BPSS.

ANNEX A

EXAMPLE OF A PRE-APPOINTMENT TIMETABLE

1. Identify requirement. →

2. Advertise requirement with job criteria, including the need as part of the process to: (i) satisfy basic eligibility criteria/certain conditions of employment (e.g. nationality rules/right to work); (ii) provide appropriate documentation to verify ID, nationality, employment and/or academic history, criminal record (unspent convictions only); and (iii) make available to the applicant a data protection privacy notice. →

3. Receive expressions of interest. ↓

4. Check basic eligibility criteria (some people may be rejected at this stage) and issue application pack, including verification forms with a caveat that this information will be checked prior to any subsequent offer of employment but will not be used as part of the sift. ←

5. Receive applications and completed verification forms. ←

6. Sift applicants (based on suitability for the job) and issue invitations for test and/or interview, including the need to bring with them photo and/or other permissible ID verification documents. ↓

7. Test and/or interview, where ID and other previously provided details can be verified/checked face-to-face. →

8. Selection on merit and offer of employment, subject to completion of any outstanding checks. Complete verification record form and advise Security Units for any NSV requirement and, in respect of migrants, inform appropriate department of the need to recheck documents that retain the excuse against a liability for a civil penalty for employing an illegal migrant worker

Cabinet Office

[intentionally blank page]

ANNEX B

Approved Access No:

BASELINE PERSONNEL SECURITY STANDARD VERIFICATION RECORD

1. Employee/Applicant details

Surname:…….……. Forenames:……...

Address:…….....

Tel No: ……..……..

Date of birth:……
Place of birth:……..……..

Nationality:……
Former or dual nationality:……
(with dates if applicable)

2. Certification of identity

Document: Date of issue:

a…… ……

b……... ……

c…… ……

d…… ……..…..

3. References (if taken)

a.Referee:…….

Relationship:……..

Address:…….

Length of association:……

b.Referee:…….

Relationship:……..

Address:…….

Length of association:……

c.Referee:…….

Relationship:……..

Address:…….

Length of association:……

4. Other information (i.e. verification of employment history (past 3 years); verification of nationality and immigration status, whether and when such immigration status needs to be rechecked and by whom; disclosure of unspent criminal record; academic certificates seen; additional checks carried out etc.):

I certify that in accordance with the requirements of the Baseline Personnel Security Standard:

I have personally examined the documents listed at 2 above and have satisfactorily established the identity of the above named employee/applicant.

I have obtained the references (if taken) and information listed at 3 and 4 above and can confirm that these satisfy the requirements.

I have made available to the employee/applicant an appropriate privacy notice, which informs them as to their statutory rights under the Data Protection Act 2018 and General Data Protection Regulation.

Name:……..

Appointment/Post:……...

Signature:……..

Date:……

[intentionally blank page]

ANNEX C

Note: If you are appointed, documentary evidence will be sought to confirm your answers. Your answers will be checked against UK immigration and nationality records.

BASELINE PERSONNEL SECURITY STANDARD
NATIONALITY AND IMMIGRATION STATUS FORM

Full name: ……

Alias(es)/Other name(s) used: ……
……

Date of birth: ……Male or Female: ……

Current/last known address:……
……
Nationality at birth: ……

Present nationality (if different): ……

Have you ever possessed any other nationality or citizenship? YES/NO

If YES, please specify: ……
……

Are you subject to immigration control?
YES/NO

If YES, please specify: ……
……
Are you lawfully resident in the UK? YES/NO

Are there any restrictions on your continued residence in the UK? YES/NO

If YES, please specify: ……...

……..

Are there any restrictions on your continued freedom to take employment in the UK?

YES/NO

If YES, please specify: ……...

……..

If applicable, please state you Home Office / Port reference number here: …….

Declaration: I undertake to notify any material changes in the information I have given above to the HR or Security branch concerned.

Signature: ……Date: ……

Important – Data Protection. You have robust rights concerning your personal data, as per the Data Protection Act 2018 and General Data Protection Regulation. Details as to your rights and the manner in which your data will be handled and processed are explained in the relevant departmental privacy notice. If you have not had access to this privacy notice, please speak to your Baseline Personnel Security Standard sponsor.

For official use only:

Reference:

(Organisation stamp)

[intentionally blank page]

ANNEX D

BASELINE PERSONNEL SECURITY STANDARD
EMPLOYMENT HISTORY REPORT FORM

(The draft covering letter shown below may be used together with the Baseline Personnel Security Standard Employment History Report Form overleaf. Alternatively, organisations may wish to include the Report Form with their normal letter requesting employment history).

Dear [ ],

SUBJECT: _____

You may be aware that we are required to verify employment history to help confirm the reliability of persons who may have access to Government assets. The person named above who (is an employee of) / (has applied for employment with) this organisation comes within the terms of this procedure.

S/he has given us your name as a (previous employer). It would be appreciated, therefore, if you would be good enough to let us have (confirmation (with dates) of his/her employment with you) by completing the attached Report Form and returning it to us by no later than [insert date]. Your reply will be treated in the strictest confidence.

Your cooperation and understanding in this matter will be greatly appreciated.

Yours sincerely,

[Signed]

SUBJECT: _____

1. How long did the subject work for you and in what capacity?

From:……..... To:……...

Capacity(i.e. appointment/post)……..……

2. Are you related to the subject? If so, please state your relationship.

……

3. Over what period have you known the subject?

From:…….. To:……...

Name:……
Signature:…… Date:……...

Contact address:…….. Tel No:……

Email:……..

Company Name and Address (Stamp if applicable):

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk
You can download this publication from www.gov.uk.