Cabinet Office

Industry Personnel Security Assurance (IPSA)

Version 1.0 – May 2021

Contents

PART I – OVERVIEW

Introduction

1. Purpose

1.1. Some UK companies (hereafter referred to as ‘Contractors’) hold contracts that require employees to access information classified at SECRET or TOP SECRET. In order to protect Government information whilst fulfilling these contracts, employees are required to undergo the appropriate level of National Security Vetting (NSV). Some of these contractors are given an NSV sponsorship account to directly sponsor their employees. It is important that these contractors handle the associated personnel security risk of employing vetted staff, just as we would expect from government departments.

1.2. The Industry Personnel Security Assurance (IPSA) policy stipulates what contractors need to do to be granted an NSV sponsorship account. It clarifies the personnel security measures expected of contractors that are granted IPSA status. IPSA gives accredited companies the ability to sponsor their own employees, however, there are a number of other ways in which contractors can put forward employees for NSV (principally sponsorship through the Contracting Authority).

1.3. This document sets out the policy of Her Majesty’s Government (HMG) with regards to sponsorship rights, roles and responsibilities applied as per the IPSA framework. The document explains IPSA in detail and is aimed at UK contractors for practical application, and to government departments, agencies, and other public bodies for information.

1.4. This document is a supplement to the overarching GovS 007 - Security and Personnel Security Policy and Standard, and should be read in that context.

2. Strategic context

2.1. The UK benefits from having a well-developed, highly diverse and technologically advanced industrial base. Contractors play a key role in the delivery of government services to citizens and the maintenance of the UK’s capabilities, particularly in the context of defence, transport, energy, telecommunications, and a wide range of other sectors. Contractors play a vital role in protecting government whilst fulfilling their public-sector contracts and IPSA sits alongside other measures to help do this.

3. National Security Vetting (NSV)

3.1. NSV is a protective safeguard applied by HMG as a means of assuring the suitability, integrity and reliability of workers within government service and throughout government supply chains. NSV is granted to individuals on a case-by-case basis following a series of assessments. It is required in order to have access to classified materials, information, individuals, facilities and systems (hereafter collectively referred to as 'assets').

3.2. NSV is managed by (United Kingdom Security Vetting (UKSV)). UKSV services and obligations are unchanged by the introduction of IPSA.

4. [1]Industry Personnel Security Assurance (IPSA)

4.1. IPSA is a personnel security assurance framework for Contractors that will ensure that workers that they have sponsored for NSV are effectively managed and provided with the same degree of aftercare[2] as vetted staff are in HMG. This applies whether workers are directly employed by the contractor or are employed within their supply chain (i.e. their NSV network[3]). It is based on CPNI's Personnel Security Maturity Model (PSMM). Unlike Facility Security Clearance (FSC), previously known as List X, an organisation does not need to have a contractual requirement to hold classified material on their own premises to apply for IPSA, however they must have a requirement to provide NSV workers in support of HMG contracts (or international defence classified contracts as set out in 5.5 of this document). While IPSA can be standalone in this respect, all Contractors who undertake FSC must also undertake IPSA.

4.2. The IPSA framework applies to any form of relationship where the assured organisation acts as an NSV sponsor for an individual, whether the individual is directly employed by the Contractor or not (such as NSV workers within the Contractor's supply chain). The NSV sponsor is bound by their responsibilities and obligations to these individuals until this relationship ends i.e. the NSV is lapsed or transferred to another NSV sponsor.

4.3. The IPSA policy consists of two parts, namely the Standards (Part II of this document), and the Assurance and Enforcement of these standards (Part III of this document).

4.4. IPSA is aimed at only those Contractors that have workers with either an ongoing need to access material classified at SECRET or above, or that require access to sites that require NSV.[4]

4.5. **IPSA accreditation is a privilege and not a right. It is provided at the discretion of the accreditors in accordance with this policy and in accordance with public law principles.**

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714017/HMG_Personnel_Security_Controls_-_May_2018.pdf

[2] The ongoing monitoring activities that support individuals holding National Security Vetting over the lifetime of their clearance to assess their ability to have continued access to classified material.

[3] Network refers to any form of relationship where the IPSA organisation is acting as a sponsor for vetted personnel not within their own company.

[4] International CONFIDENTIAL and above for international defence contracts

IPSA Eligibility Criteria

5. In order to apply for IPSA accreditation, Contractors must fulfil the minimum criteria as per the sub-headings below:

5.1. Requirement for IPSA:

a. The Contractor has a legitimate requirement to provide NSV workers for classified contracts, or is applying for Facilities Security Clearance.

5.2. Companies House Registration:

a. The Contractor must be registered with Companies House.

5.3. NSV Population:

a. The Contractor must hold a minimum NSV population of at least 20 individuals or have forecasted to meet this threshold within three years of confirmation of meeting the IPSA standards.

b. Forecasts which consistently overrate the expected NSV population, to the extent that the Contractor does not fulfil the cleared population requirement, will be subject to further examination by the Industry Security Assurance Centre (ISAC).

5.4. Contractual Relationship with UK Government or an international partner:

a. To become an NSV sponsor via IPSA, contractors must have their NSV operations based in the United Kingdom and have an existing contract between themselves and:
   i. the Ministry of Defence (MOD) or international equivalent; or
   ii. a sub-contractor within the supply chain of the MOD or international equivalent; or
   iii. an International Defence Organisation (e.g. NATO)

5.5. Board Composition:

a. At least one individual on the Board of Directors (the nominated Board Level Contact – see 6.1) must reside in the UK and be a British National. However, in certain circumstances Contracting Authorities may require the majority of Directors to be British Nationals.

Key Contacts / Roles

6.1 Board Level Contact:

a. One member of the Board must be designated as the individual responsible for personnel security for the Contractor (hereafter referred to as ‘the Board Level Contact’). The Board Level Contact must be a British National (or a dual National where one of the dual nationalities is British) and must hold a minimum clearance of SC. The Terms of Reference for the position of Board Level Contact can be found in Annex D.

b. The Board Level Contact is responsible to the Chairperson of the Board of Directors for the strategic delivery and senior management oversight of an effective personnel security culture. The Board Level Contact acts as the Senior Personnel Security Risk Owner for the Contractor and is responsible for ensuring that the Board is sufficiently aware of personnel security risk, measures, policy and incidents.

c. The role of the Board Level Contact should be recorded in Terms of Reference administered internally by the Contractor.

6.2 Personnel Security Controller:

a. An employee of the Contractor must be designated as the ‘Personnel Security Controller’, who will be responsible to the Board of Directors for the strategic development of an effective personnel security culture and the day to day management and delivery of personnel security policy, procedures, risk assessment, management and general security processes. The Personnel Security Controller is ultimately responsible for the implementation of effective aftercare for the NSV individuals that the Contractor is responsible for.

b. The Personnel Security Controller also refers to, and explicitly includes, any secondary individual(s) with equivalent roles and responsibilities in the event of the absence of the primary title holder (e.g. a Deputy).

c. The Personnel Security Controller and any secondary individuals with equivalent roles and responsibilities must be suitably empowered to carry out their duties, including ensuring the maintenance of appropriate standards and to drive rectification measures if necessary. The Terms of Reference for the position of Personnel Security Controller can be found in Annex E.

d. The Personnel Security Controller must be a British National (or a dual National where one of the dual nationalities is British) and must hold a minimum clearance of SC. If, at IPSA application, the Personnel Security Controller does not already hold NSV, they must apply for and be granted an SC clearance as minimum. Their role in facilitating further clearance applications will be subject to them successfully being granted and maintaining their clearance.

e. The role of the Personnel Security Controller should be recorded in the individual’s Terms of Reference / Job Description administered internally by the Contractor.

f. The Contractor’s Facilities Security Controller (for FSC) and their Personnel Security Controller may be the same individual.

Application Process

7 Application Procedure - In order to apply for IPSA accreditation, the Contractor should follow the steps below:

7.1. To minimise any delay in the application process, the Contractor should ensure that it already meets the eligibility criteria as specified in Section 5. The Contractor should also identify their key contacts and ensure that they meet the requirements as specified in Section 6.

7.2. The Contractor must complete the Application Form (the Government Industry Security Assurance form, or GISA), which can be found in Annex A. This should be submitted to isac-group@mod.gov.uk.

7.3. The application will be assessed by the ISAC. This will involve conducting checks on the Contractor in terms of its eligibility for IPSA. It will also involve checks on the entire Board and checks regarding the suitability of the nominated Board Level Contact and Personnel Security Controller.

7.4. Once these checks have been completed successfully, the Contractor will be expected to implement the IPSA Standards as documented in Part II – STANDARDS. The Contractor will have to provide evidence to support the implementation of these standards to the ISAC for assessment.

7.5. Where initial NSV clearances may be required, such as for the Personnel Security Controller, this shall be sponsored by the Contracting Authority.[5]

7.6. Advice and guidance will be available from the ISAC to assist the Contractor in meeting and evidencing adherence to the required standards. Once the necessary personnel have been granted NSV and the Contractor has been assessed and determined to meet the standards as laid out in Part II of this document, the ISAC may award the Contractor IPSA status. In addition, NSV individuals designated by the Contractor will be provided with sponsorship accounts for the NSV IT system, which will enable them to sponsor individuals for NSV, where there is a genuine and confirmed necessity for it. Guidance for sponsors is available here.

7.7. IPSA accredited organisations will be subject to annual reviews and a three-yearly assurance cycle. The annual review involves the submission of a completed IPSA dashboard. The three-yearly assurance cycle involves the submission of a completed GISA, IPSA Evidence Cover Sheet and associated evidence and a completed IPSA dashboard.

8 Factors to note

8.1 In some cases, IPSA accreditation may be awarded subject to recommendations from the ISAC that the Contractor will be expected to implement within a period specified by ISAC. These will be reviewed as part of the ongoing assurance process.

[5] For international classified contracts the ISAC should be consulted

8.2 All companies that currently have Facilities Security Clearance (FSC), previously known as ‘List X’, will be required to undertake IPSA. However, FSC is not required to be eligible for IPSA.

9 Notification of changes in ownership and control

9.1. The Contractor must notify NSV authorities of any change in the circumstances of the Contractor which may have a bearing on its security status. These changes may impact whether a contractor is eligible for IPSA accreditation. The following must be immediately reported:

a. proposed change of ownership and control, including any foreign acquisition, or purchase of equity, by any foreign interest of 5% or more of the total company stock;

b. any changes to the executive Board;

c. appointment of a person, who is not a British national (or a dual national where one of the dual nationalities is British) to a position which could influence the Contractor’s NSV population.

9.2. In cases where the Contractor is subject to a change of ownership, it should not be assumed that any existing HMG contracts will be automatically novated to the new owners. Before any novation can take place, the Contracting Authority will need to be satisfied that HMG can be protected from any increase in security risk

10. HMG reserves the right to rescind accreditation at any time.

11. **It is to be noted that if accreditation is not granted or rescinded there is no right of appeal. In this event any future NSV requirements would have to be fulfilled via your Contracting Authority or equivalent.**

PART II – STANDARDS

Methodology

12. Approach

12.1. The suitability of a Contractor for applying for IPSA is determined by the checks conducted on the information provided in the GISA, or application form, as per section 7. Once this has been assessed and the Contractor has implemented the standards detailed in sections 14 to 21, they will be evaluated by the ISAC as to their suitability for being awarded IPSA status. These standards are also referred to as the Personnel Reliability Framework (PRF). Further advice and guidance as to the implementation of these standards can be found on gov.uk.

12.2. It will be determined whether a Contractor is suitable to hold IPSA status based on an evaluation of their implementation and adherence to the requirements of the PRF.

12.3. The scoring criteria which grades the Contractor against the constituent elements within the PRF and determines a final rating will not be made public. However, the same criteria will be applied consistently to each applicant.

12.4. Contractors will be expected to implement the PRF in a way that is appropriate to the size, configuration and maturity of their operations.

13. Applicability

13.1. The PRF applies across the entire NSV population over which the Contractor has oversight (i.e. their NSV network).[6] This may include NSV individuals who are employed by separate legal entities, such as subsidiary or partner companies, contingent labour, contractors, and other such personnel. **All of these individuals are considered as being under the scope of the PRF, and the implementation and adherence to the PRF will be judged against the Contractor's protocols for managing this population.**

14. Further information

14.1. This document is a supporting document to the overarching GovS 007

14.2. Further information on complementary Industrial Security Policies and the HMG Personnel Security Standards can be found on GOV.UK

14.3. The PRF is closely modelled on the Centre for the Protection of National Infrastructure's (CPNI's) seven core elements of effective personnel security. Further information from CPNI regarding personnel security can be found throughout their website.

Personnel Reliability Framework (PRF)

15. Introduction

15.1. The PRF is a framework of policies, programmes, processes and governance that must be implemented by a Contractor in order to qualify for IPSA status. The implementation of this framework enables and facilitates the required sponsorship and aftercare activities required for IPSA.

15.2. In order to attain and hold IPSA status, the requirements of the PRF as detailed below must be implemented and adhered to. Evidence to support this must be provided at accreditation and for ongoing tri-annual assurance.

[6] Network refers to any form of relationship where the IPSA organisation is acting as a sponsor for vetted personnel not within their own company.

16. Governance and Leadership:

16.1. Governance Framework:

a. Documented Terms of Reference for Security Positions and Working Groups.

b. Formal records that the Personnel Security Controller and any deputies have accepted their responsibilities, as detailed in Annex E of this document.

c. Implementation of a Company Security Governance policy demonstrating:

i. Lines of delegation and responsibility;

ii. Governance;

iii. HR and Welfare policies linked into Security policies;

iv. Formal involvement of PSC in the approval of new personnel security policy as well as changes to policy related to personnel security.

d. Ensure that the PSC, the Board Level Contact and all individuals involved in the Contractor's NSV-related activities have NSV.

e. Documented responsibilities of all individuals involved in the Contractor's NSV-related activities.

f. Organisation charts that clearly demonstrate the security functions.

g. Board level oversight of personnel security.

16.2. Contract information:

a. Formally recorded contract information, for the Contractor and their network;

b. Where a Contractor has sponsorship responsibilities to a network:

i. Details of each organisation where NSV individuals are employed;

ii. The PSC contact for each of these organisations.

17. Insider Threat Risk Assessment:

17.1. Personnel Security Risk Management Framework:

a. Implementation of a Personnel Security Risk Management Policy (including Security Risk Management Principles and Insider Threat considerations);

b. Implementation of Personnel Security Risk processes;

c. Performance of formal risk assessment, including role-based risk assessment, against the Contractor and their network;

d. Implementation of regular Insider Threat / Personnel Security risk review;

e. Formally record outcomes of Personnel Security risk review;

f. Implementation of a formal Risk Register. Only the template for the Risk Register must be provided for IPSA accreditation and ongoing assurance.

18. Pre-vetting Screening:

18.1. Vetting Register and Dashboard

a. Implementation of a formal Vetting Register, which must include the following fields, at a minimum:

i. NSV holder's details;

ii. NSV details;

iii. Justification for NSV;

iv. Baseline Personnel Security Standard (BPSS) Verification record.

Only the template for the Vetting Register must be provided for IPSA accreditation and ongoing assurance.

b. Formal accreditation of the IT system where the Vetting Register is stored (i.e. DART). The classification of this IT system is Official-Sensitive. During accreditation this must be complete or in progress.

18.2. Eligibility:

a. Implementation of an eligibility policy detailing the checks that must conducted prior to NSV application, including:

i. Clear requirement for NSV;

ii. BPSS checks.

19. Ongoing Personnel Security:

19.1. Aftercare Framework:

a. Implementation of policies and processes for the appropriate handling of all Aftercare-related activities, applicable to the Contractor and their network. These policies and processes must include provision for:

i. Security Appraisal Forms;

ii. Change of Personal Circumstances;

iii. Aftercare Incident Reports;

iv. Transfers (Joiners, Leavers);

v. Shares;

vi. Lapses.

b. Formally recorded outcomes of these processes in the Contractor’s Vetting Register.

c. Implementation of an overseas travel policy that:

i. Is aligned with the SPF / GovS 007;

ii. Includes signposting to CPNI travel guidance.

20. Monitoring and Assessment of Workers:

20.1. NSV review protocols:

a. Implementation of a policy and processes for the regular review of NSV holders, to assure ongoing NSV eligibility.

20.2. Behaviour monitoring protocols:

b. Implementation of policy and protocols for monitoring the security conduct of staff in order to identify suspicious behaviour and / or to identify NSV individuals who may be vulnerable or susceptible to coercion. This must include:

i. The behaviour to be monitored;

ii. How this information will be used;

iii. The steps that will be taken in the event these behaviours are demonstrated by individuals.

21. Investigation and Disciplinary Practices:

21.1. Incident handling framework:

a. The implementation of processes for handling incidents related to Personnel Security, including those raised with Joint Security Coordination Centre (JSyCC);

b. Formally recorded outcomes of these processes in the Contractor’s Vetting Register.

21.2. Disciplinary framework:

a. Implementation of a disciplinary policy that includes:

i. Links to Welfare and Security policies;

ii. Approach for how poor and inappropriate behaviour is tackled;

iii. Approach for enforcement of good security behaviour.

b. Implementation of disciplinary processes.

c. Formally recorded outcomes of these processes in the Contractor's Vetting Register.

22. Security Culture and Behavioural Change:

22.1. Training Programme:

a. Implementation of a programme for delivery of security training.

b. Implementation of training plans. Minimum training requirements includes:

i. Induction Training;

ii. Refresher Training;

iii. Training on BPSS document checks;

iv. Line management training to recognise behaviour of concern.

c. Implementation of mechanisms to measure the effectiveness of security training as well as any ongoing improvements to training.

d. Could include training for Senior Leadership.

22.2. Security Communications Programme/Plan:

a. Implementation of an annual Security Communications Programme / Plan which includes:

i. Awareness campaigns;

ii. Reminder notices;

iii. Signposting.

b. Implementation of mechanisms to evaluate the effectiveness of communications as well as any ongoing improvements to the communications programme/plan.

22.3. Knowledge repository:

a. Implementation of a centralised repository / library of good security practice that is easy to access and includes information on:

i. Responsibilities and duties of NSV holders;

ii. Related policies and processes;

iii. Guidance documentation;

iv. Signposting.

PART III – ASSURANCE & ENFORCEMENT

Oversight and Decision-Making

23. The ISAC, a part of the MOD, will have sole discretion and decision-making power as to whether to award IPSA status to applicant Contractors. This includes ongoing inspection of those Contractors, as well as recommending rectification measures or imposing suspension of accreditation, if these are deemed necessary.

24. IPSA policy and NSV policy are set, issued and owned by the Government Security Group in the Cabinet Office. UKSV, also within the Government Security Group, will have the lead responsibility for the conduct of vetting casework. HMG remains the ultimate decision-maker as to whether to grant or refuse NSV for individuals.

25. The Contractor will be responsible for developing and maintaining its own internal protocols, including in terms of policies and processes, in order to maintain compliance with IPSA standards. The Contractor will determine with the Contracting Authority or customer which individuals are required to apply for NSV, while being mindful of the vetting process, costs and risk tolerances. This includes candidates for specific roles related to IPSA, such as the Board Level Contact and the Personnel Security Controller.

Responsibilities

26. On the part of the Contractor:

26.1. The Contractor shall submit a completed IPSA Dashboard annually to the ISAC who will determine whether the Contractor continues to meet the standards outlined in the PRF. The ISAC may provide recommendations or requests for rectification which they will expect to see implemented in a reasonable timeframe.

26.2. The Contractor will maintain and update all appropriate records, including, but not limited to, policies and registers.

26.3. IPSA assurance will be undertaken every three years. This process will be initiated at the discretion of the ISAC and may be sooner. The accredited Contractor will be asked to highlight any changes since their initial application or most recent review. In the event that the ISAC requires additional information the Contractor will be expected to cooperate with ISAC in order to facilitate this.

26.4. The Contractor is required to maintain ultimate oversight over all NSV holders for whom they are the sponsor, until such time as those individuals have been formally transferred to an alternative NSV sponsor's remit (e.g. due to becoming an employee of a Government Department or another organisation who has undertaken IPSA) or they leave employment. The Contractor is responsible for the oversight of NSV holders that are transferred into their employment, even if they have originally received their NSV from a different sponsor.

26.5. The Contractor may have contractual arrangements for other legal entities to maintain day-to-day oversight over their NSV holders (e.g. contingent labour providers, lone contractors, subsidiary organisations, etc.). However, the Contractor will still be considered by HMG as ultimately responsible for the ongoing personnel security of those workers, within the context of IPSA.

26.6. The Contractor must uphold their NSV Sponsor reporting obligations, ensuring that any changes in personal circumstances or serious personnel security incidents are reported to UKSV as soon as they are made aware of them.

26.7. The Contractor shall not use IPSA accreditation for promotional and marketing purposes, nor shall they declare their IPSA status in any public-facing material. There are limited circumstances where IPSA status can be disclosed and this can be confirmed by using the contact details in this policy.

26.8. The Contractor must ensure that their policies conform with HMG policy and that any subsequent changes to HMG policy is reflected in their internal Personnel Security policies.

27. On the part of HMG:

27.1. The ISAC will ensure that the Contractor is given clear guidance and up to date information regarding the expectations that will be placed upon them in the course of their duties and responsibilities as an IPSA accredited organisation.

27.2. The ISAC will own and administer a central database of those organisations with IPSA accredited status. The ISAC will be responsible for the promulgation of IPSA security notices and other such communications as and when necessary.

Specific Roles

28. Further information as to the responsibilities and duties of the Board Level Contact are included at **Annex D**.

29. Further information as to the responsibilities and duties of the Personnel Security Controller are included at **Annex E**.

Contact

30. For further information or queries about IPSA please contact the ISAC via:

Isac-group@mod.gov.uk
Industry Security Assurance Centre
Poplar -1
MOD Abbey Wood
# 2004
Bristol
BS34 8JH
Tel No. 030 67934378

ANNEXES ATTACHED

- A – Application Form (GISA)
- B – IPSA Evidence Cover Sheet
- C – IPSA Dashboard

ANNEX D – The Board Level Contact Terms of Reference

Title	Board Level Contact (BLC)
Role	Responsible to the Chairperson of the Board of Directors for the strategic delivery and senior management oversight of an effective personnel security culture within the company. Acting as the Senior Personnel Security Risk Owner for the organisation.
Task Description	The Board Level Contact is specifically responsible for: ● Ownership of personnel security risk assessment and mitigation for the company. ● Responsibility for the exposure of personnel security risk, measures, policy and incidents to the Board ● Responsible for ensuring that security is a standing agenda item at Board meetings ● The exercise of policy control and ownership for personnel security policy within the company. ● Establishing and delegating the appropriate authority and effective support to the nominated Personnel Security Controller. ● Informing the relevant officials of the appropriate Contracting Authority of changes to the company's status, that is, ownership, control, closure etc. ● Assuring at an Executive level that the company's business processes are compliant with relevant legislation, and that the company operates according to the principles embedded in relevant Government standards. ● Responsible for ensuring the Board, and senior managers are compliant with all security obligations and business choices in respect of personnel security risks and controls. ● Leading on personnel security as a standing agenda item at Board meetings. ● Agreeing the setting of personnel security risk levels, appropriate to the company and acceptable to the Contracting Authority. ● Owning all personnel security risks that are identified, documented, tracked, mitigated and monitored within the company and its sponsored subcontractor vetted population.

	● Providing Board oversight and assurance that measures are in place to measure the impact of risk mitigation. ● Leading within the company, and between the company and Security Officials of the relevant Contracting Authority, on personnel security related issues. ● Leading the Board on the interpretation and implementation of contractual and, where appropriate, legislative or regulatory personnel security controls. ● Sets strategic plans, which satisfy the current and ongoing needs of the company's business strategy, and its current and future capabilities. ● Agreeing to the personnel security elements of employee controls in the event of insolvency, mergers or buy-outs. ● Ensuring that security education and training is an integral part of the company's strategic security goals.
Skills Required	● Communicates and influences orally and in writing, to senior colleagues at both internal and senior external stakeholder levels. ● Can present complex technical and non-technical security information, concepts and intelligence to a wide range of audiences and stakeholders. ● Willing to challenge assumptions and 'business as usual'. ● Actively manages strategic collaboration between stakeholders. ● Project/business leading skills to meet time and quality targets. ● Maintains an awareness of security technologies and thinking to drive strategic business development.
Suggested Training	**Relevant CPNI Briefings and Courses** http://www.cpni.gov.uk/

Notes:

1. The individual identified as the Board Level Contact (BLC) must be a Security Cleared British National (or a dual National where one of the dual nationalities is British), who is responsible to the Company Board for the strategic management and oversight of personnel security aspects within the company.

2. The individual fulfilling the role should indicate their acceptance of the role and its responsibilities by signing and dating a suitably worded acceptance document.

3. The ISAC must always be informed, where possible in advance, if the Board Level Contact is to change.

ANNEX E – The Personnel Security Controller Terms of Reference

Title	Personnel Security Controller
Role	Responsible to the Board of Directors for the strategic development of an effective personnel security culture within the company and the day to day management and delivery of personnel security policy, procedures, risk assessment, management and general security processes. Responsible for implementation of National Security Vetting aftercare within the company and any subordinate organisations that the company provides sponsorship for. The Personnel Security Controller will ensure that all aftercare activities are managed and undertaken promptly and effectively, liaising with HR and Welfare organisations within the company as necessary. The role must be suitably empowered by the Company Board to carry out all the required personnel security controller responsibilities. Elements of this role can be carried out by other individuals, such as a suitably empowered Deputy or vetting team. However, responsibility for oversight and delivery of any of the activities associated with the role rests with the Personnel Security Controller.
Task Description	● The establishment and oversight of an organisation's approach to Personnel Security including: ● Assures that the company's personnel security business processes are compliant with relevant legislation, and that the company operates according to the principles embedded in relevant Government standards. ● Facilitate where necessary visits and inspections by individuals representing either the Government or Contracting Authority and to ensure any relevant documentation, process or records are available for inspection. ● Interpreting, implementing and monitoring security controls for the appropriate maintenance of personnel security for National Security Vetted staff either in the employment of the company or subcontractor.

	● Assessment and agreement with companies within the Network to ensure that appropriate controls are present for Vetting Sponsor responsibilities to be discharged effectively. ● Ensure that any aftercare responsibilities for individuals within the company’s network are undertaken to ensure compliance with current regulation and guidance for the holding of a National Security Vetting clearance. ● Responsible for ensuring the Board, and senior managers are aware of and discharge their security obligations and business choices in respect of personnel security risks and controls. ● Active management in the setting of personnel security risk levels, appropriate to the company and acceptable to the Contracting Authority. ● Owning and maintaining a personnel security Risk Register where risks are identified, documented, tracked, mitigated and monitored. ● Ensuring that measures are in place to measure the impact of risk mitigation. ● Promotes policies, practices and decisions which recognise the current and evolving needs of all the stakeholders. ● Ensuring that any personnel security policies are coherent with, and complement any HR or Welfare policies, either planned or in existence. ● Ensure that security considerations are included in any HR or Welfare cases or decisions. ● Ensure that ongoing personnel security is embedded within the company’s ways of working. ● Overall responsibility for pre-vetting checks (BPSS) and the subsequent National Security Vetting process. ● The Personnel Security Controller should ensure that they have the necessary UKSV access to have effective oversight of both the vetting process and the vetting sponsor activities of any subordinate vetting sponsor accounts. ● Taking clear ownership of all personnel security incidents/breaches or ensuring that oversight is kept if handled by other parts of the company. ● Ensuring that incidents, changes of circumstances or any other situation or event that may affect an individual’s ability to hold an NSV clearance are reported via the appropriate means to UKSV in their role as UK Vetting Authority for Government.

	● Liaising within the company, and between the company and security officials of the relevant Contracting Authority, on security related issues. ● Advising management on the interpretation and implementation of contractual and, where appropriate, legislative or regulatory security controls. ● Advise on the appropriate security controls for a new contract. ● Preparing and implementing the Company Personnel Security Instructions, ensuring that any new or revised policy is appropriately ‘staffed’ and considered throughout the organisation, liaising with other disciplines such as HR or Welfare to ensure personnel security is considered and embedded within all appropriate policies. ● Ensuring that all policies are made available to, and understood by all employees, updating them as necessary. ● Ensuring that staff are aware that they are operating under the ambit of the Official Secrets Act. ● Ensuring that processes are in place to brief/de-brief Security Check (SC) and Developed Vetting (DV) cleared staff who may travel to certain foreign countries, either on business or privately. ● Being readily available for consultation and giving security advice to the company’s management and employees. ● Contributes to strategic plans, which satisfy the current and ongoing needs of the company’s business strategy, and its current and future capabilities. ● Co-ordinating the planning of appropriate security controls for a new contract or for the personnel security elements of employee controls in the event of insolvency, mergers or buy-outs. ● Arranging for appropriate security education and awareness training, ensuring that staff understand the scale, nature of the threats and security actions required. ● Ensuring that security education and training is an integral part of the employee’s time with the company, covering induction, ongoing security awareness and education and termination/exit from the comapny. ● Ensuring that any breach of personnel security is immediately reported in accordance with Government requirements and contractual responsibilities. ● Ensure that the outcome of any security incident is recorded in a breaches register, and a full report and impact analysis is passed to

	the Contracting Authority, or other Government organisation, where appropriate.
Skills Required	● Communicates and influences orally and in writing, to Board and senior internal and external stakeholder levels. ● Can present complex technical and non-technical security information, concepts and intelligence to a wide range of audiences and stakeholders. ● Willing to challenge assumptions and 'business as usual'. ● Actively seeks and promotes collaboration between stakeholders. ● Project, planning and monitoring skills to meet time and quality targets. ● Maintains an awareness of security technologies and thinking to drive business and personal development.
Suggested Training	**Relevant CPNI Briefings and Courses** http://www.cpni.gov.uk/ **Suitable Document Verification Course**

Notes:

1. The individual identified as the Personnel Security Controller must be a Security Cleared British National (or a dual National where one of the dual nationalities is British). The Personnel Security Controller is responsible to the Board Level Contact for the day to day personnel security aspects within the company.

2. The individual fulfilling the role should indicate their acceptance of the role and its responsibilities by signing and dating a suitably worded acceptance document.

3. A large company, or a company with substantial contractual obligations, may have a full time Personnel Security Controller, perhaps supported by one or more subsidiary security staff.

4. If a Deputy Personnel Controller or other security staff are appointed, the Personnel Security Controller should ensure that they are suitably empowered by appropriate delegations to carry out their respective functions.

5. A company with a number of different sites, may need to appoint Local Personnel Security Contacts, who report to a Group/Regional/HQ Personnel Security Controller.

6. The size of a company or its contractual obligations will vary between companies. For smaller companies it may be acceptable for the Board Level Contact and Personnel Security Controller to be the same person.

7. The ISAC must always be informed, where possible in advance, if the Security Controller is to change.