



Government  
Security



Industry Security  
Assurance Centre  
A Government Security Centre

# Industry Personnel Security Assurance

## Personnel Reliability Framework





# Contents

---

Introduction	5
Personnel Reliability Framework	6
Implementation and Eligibility	8
Networks	9
Personnel Security Standards	11
Governance and Leadership	12
Insider Threat Risk Assessment	18
Pre-vetting Screening	22
Ongoing Personnel Security	26
Monitoring and Assessment of Workers	30
Investigation & Disciplinary Practice	34
Security Culture & Behavioural Change	38
Glossary	43

# Industry Security Assurance



# Introduction

---

Industry Personnel Security Assurance (IPSA), known as List V during development, is an assurance framework for personnel security in industry. It will help ensure that individuals who have undertaken National Security Vetting (NSV) are effectively managed and provided with the same degree of aftercare as vetted staff in HMG. It is based on CPNI's Personnel Security Maturity Model (PSMM), though looked at through an aftercare lens.

IPSA differs from the PSMM in that it assures whether the activity to support effective aftercare is taking place in order to determine whether an organisation can be given the ability to conduct vetting sponsorship. It does not assess the overall personnel security maturity of an organisation, which is a much more in-depth process and undertaken by CPNI as the National Technical Authority.

IPSA is a part of the integrated Industry Security Assurance (ISA) framework for the assessment of physical and personnel security of industry operating in the classified space at SECRET (or International CONFIDENTIAL) or above. Physical security assurance is undertaken through the Facility Security Clearance (FSC) process. Both assurance processes will be run by the Industry Security Assurance Centre (ISAC), hosted by the Ministry of Defence.

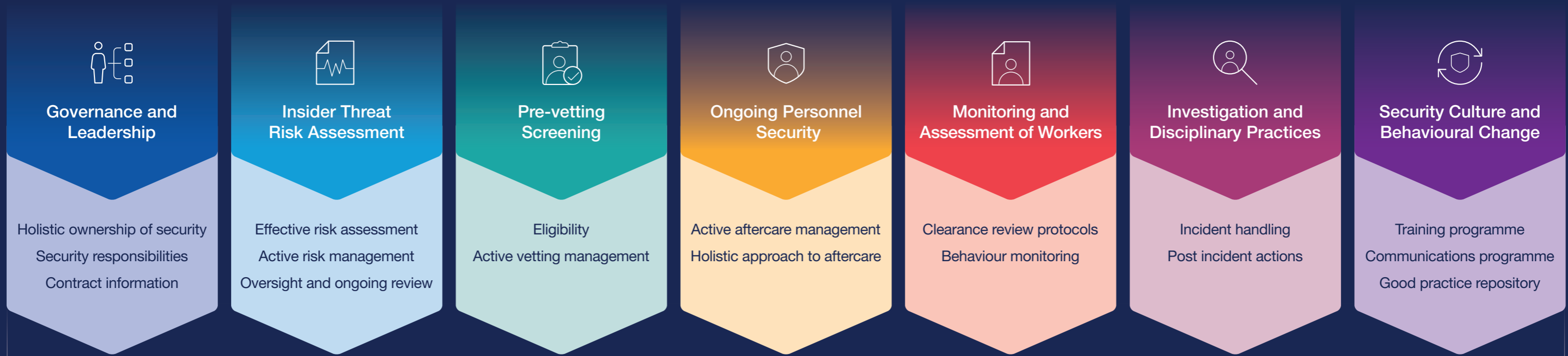
FSC, traditionally known as List X, provides assurance that an organisation has the correct physical measures in place to protect classified material on its own sites. This could include fences, control of access, CCTV or secure cabinets etc. The physical security requirements are always proportionate to the classification, type and amount of information held.

An organisation does not need to have a contractual requirement for an FSC to apply for IPSA. They must however have a requirement to provide vetted staff in support of HMG (or foreign government / international institution) contracts.

All organisations that are required to have an FSC will also be required to undertake IPSA. Further information on this can be found under Implementation and Eligibility.

Both FSC and IPSA share some core checks that include (but are not limited to) due diligence and company checks with a number of government agencies. These checks are completed prior to FSC or IPSA accreditation activity taking place and as part of the ongoing assurance cycle.

# Personnel Reliability Framework



Policy • Process • People • Output

# Implementation and Eligibility

---

The standards within the framework are designed for organisations that manage and/or sponsor staff at SC and above, however the principles can equally be applied across the vetting landscape for CTC/BPSS holders.

IPSA will initially be rolled out to organisations contracted to the Ministry of Defence that hold existing FSCs for one or more facilities. This is to provide assurance for organisations that already hold NSV sponsorship accounts and are managing a significant vetted population. Organisations will be onboarded in tranches over three years starting from late 2021, which will establish an ongoing triennial assurance cycle.

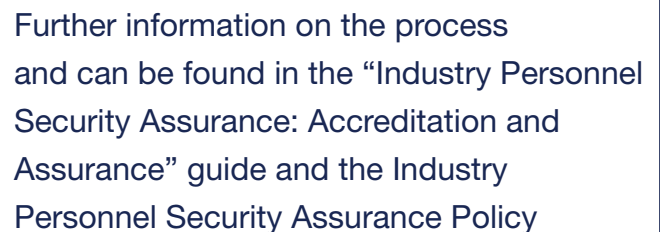
The ISAC will be in touch with organisations holding an FSC directly to inform them when they will be required to undertake the IPSA process for the first time. Organisations should however be as proactive as possible to introduce the policies and process that support IPSA as soon as they can in preparation for assurance.

Organisations without a requirement for an FSC will be able to apply for IPSA from late 2021 if they meet each of the following criteria:

- The organisation is registered with Companies House.
- They have a requirement to provide vetted staff in support of contracts they hold with the MOD, its supply chain, or international Defence organisations (e.g. NATO).  
*Note: Work is underway to determine viability of expanding eligibility requirement for contracts in support of all Government departments.*
- They currently have, or can prove that within three years they will have, a minimum vetted population of 20 individuals. This limit will be reviewed once assurance activity has begun.  
*Note: This limit only applies to organisations without an FSC as all organisations with an FSC will be required to undertake IPSA regardless of vetted population size.*

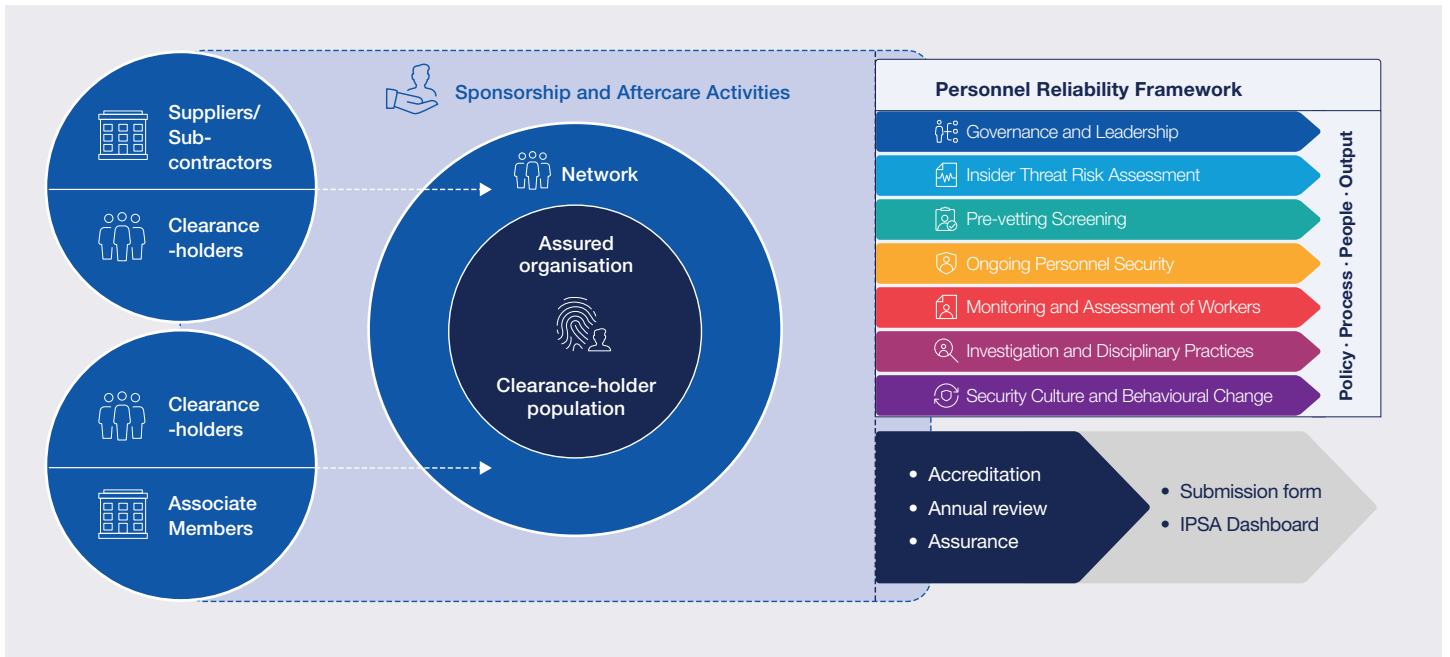
The personnel security and aftercare standards contained within the IPSA framework should apply to all organisations that manage vetted staff regardless of whether they are subject to assurance activity or the department they are contracted to.

By meeting the standards within the framework, organisations will more effectively manage both their own personnel security risks and those they hold on behalf of HMG.



Further information on the process and can be found in the “Industry Personnel Security Assurance: Accreditation and Assurance” guide and the Industry Personnel Security Assurance Policy

# Networks



Within the Personal Reliability Framework (PRF) you will see reference to your clearance holder network and how each element of the framework should be applied across it. Your clearance holder network (or “network”) comprises every individual that you have provided National Security Vetting (NSV) sponsorship for until such time that

- Their NSV expires *or*
- Their NSV is lapsed *or* withdrawn
- Their NSV is transferred to a different NSV sponsor

Your network may include individuals who do not work directly for your organisation. This may be because they are part of your sub-contracting chain and are not able to sponsor NSV themselves, or part of a membership network that you provide sponsorship for in support of other contracts.

In any scenario where you provide NSV sponsorship, you must ensure that the PRF applies equally to all NSV individuals, regardless of whether they are employed directly by your organisation or by a third party.

**For example,** under the Insider Threat and Risk Assessment strand you must include those personnel security risks posed by the network within your Risk Management Framework considerations, including the risk assessment. You may also be required to provide security education and awareness material to support a positive security culture across your network which could include allowing access to your established training materials.

There is no ‘one size fits all’ for how to manage your network - it will always depend on the size, configuration and maturity of the organisations involved. However, you should consider what policies and processes should be in place in order to ensure that the robust personnel security and aftercare behaviours evaluated through the PRF are reflected both within your organisation and across your network.





# Personnel Security Standards

## Personnel Reliability Framework



Governance and Leadership



Insider Threat Risk Assessment



Pre-vetting Screening



Ongoing Personnel Security



Monitoring and Assessment of Workers



Investigation and Disciplinary Practices



Security Culture and Behavioural Change

Policy · Process · People · Output

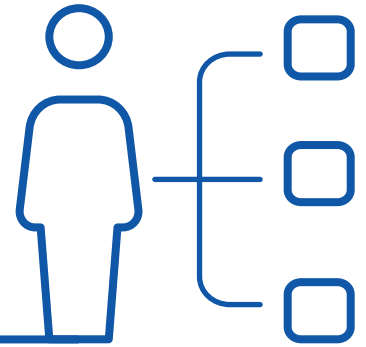
# Governance and Leadership





# Governance and Leadership

## Introduction



### CPNI Definition:

Positive and visible board level support for protective security is vital to demonstrate to staff the value placed on personnel and people security policies and procedures.

Strong security leadership, at all levels across your organisation will:

- Ensure consistency and clear lines of responsibility for the management of security risk
- Foster a multi-disciplinary approach to countering the insider threat
- Ensure proportionate and cost-effective use of resources
- Provide essential management information for the purposes of security planning and people management
- Provide a strong example that both develops and underpins an effective security culture

Governance and Leadership is a key component to aftercare through supporting good practice from the top down.

It shows senior leadership visibility in demonstrating the behaviours expected of individuals who hold NSV and have access to classified material. It also ensures that the appropriate and required mechanisms are in place to support robust personnel security and provides rigorous oversight.

## Governance and Leadership

# What are my responsibilities?

---

It is essential to implement a framework of Governance within your organisation with clear links between HR / Welfare and Security, as well as appropriate senior level oversight and lines of delegation. Security roles and working groups must be clearly defined and understood, with all relevant personnel cleared to the appropriate levels. It is also important to understand, and have a record of, your contractual and clearance-holder network. To this end, it is your responsibility to ensure that the following elements are incorporated into your framework of Governance:

**Decision-making hierarchy:** This should include who is part of the decision-making process, where there is delegated responsibility, where the delegation comes from and what are the limits of those delegations. This will ensure those in the appropriate roles are able to make security-informed decisions.

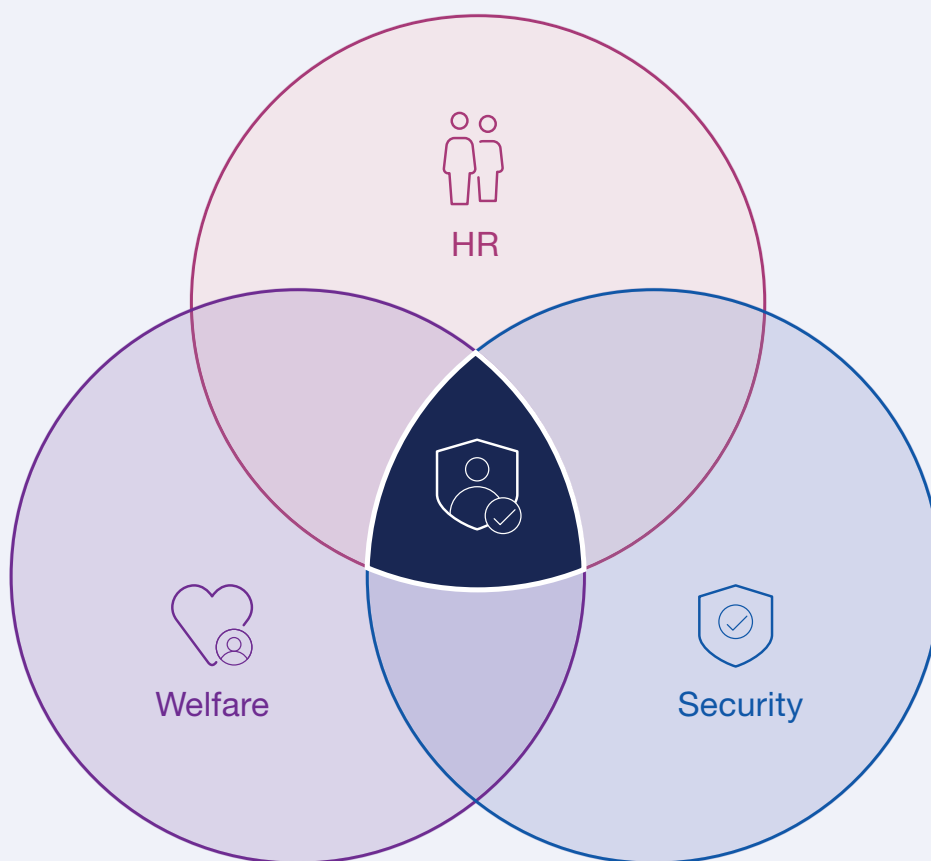
**HR / Welfare links to Security:** it is essential that these areas collaborate, at a minimum, in the reporting & handling of incidents, personnel security risk identification (including categorisation and mitigation), as well as the development of policy related to personnel security. This will guarantee that relevant parts of the organisation that are key to a holistic approach to personnel security are engaged and actively involved. These links should be clearly represented in the Governance processes and should demonstrate how Security and HR engages with each other to ensure that policies that are relevant to personnel security and aftercare are aligned.



# Governance and Leadership

## What are my responsibilities?

HR / Welfare links to Security



## Governance and Leadership

# What are my responsibilities?

---

**Interaction of personnel security functions:** many different functions across an organisation will be involved in the delivery of personnel security and aftercare. Mechanisms for this will include working groups, teams and individuals. It is important to ensure that all personnel security functions within your organisation are appropriately engaged and actively involved in its delivery.

**Board level oversight of personnel security:** Personnel security matters must have the appropriate level of oversight within the organisation. Clearly demonstrate that there is board level oversight of personnel security matters, including personnel security risks.

**Reporting lines and oversight of aftercare:** In order to understand how aftercare is managed and who is involved, your governance processes should clearly demonstrate how aftercare actions are being actively managed throughout the reporting chains, both within the main organisation and the wider network.

**Delegated responsibilities (network):** Where personnel security responsibilities are delegated to network organisations, your organisation's policies and processes should clearly stipulate and demonstrate that they are being followed across the network.



## Governance and Leadership

# What are my responsibilities?

**Personnel security policy review process:** It is important that all appropriate functions are involved in the policy review process where it impacts personnel security. You should have a clearly defined process for creating and updating personnel security policy, including any triggers such as incident review or a regular policy review.

**Ownership of risk management, incident handling and disciplinary protocols:** To ensure that these activities have clear ownership and are being actively managed, your governance processes should clearly demonstrate which roles, teams or working groups own and actively manage risk, incidents and disciplinary protocols.

**Understanding of your NSV population:** You should have a clear record of your NSV population, both within your organisation and across its network. This includes number of NSV individuals that are actively engaged in supporting a contract that requires cleared staff, as well as the number of cleared individuals that are between contracts or working on contracts that don't require cleared staff.

**Understanding of your contract landscape:** It is important that your organisation and network have a clear record of the contracts held where there is a requirement to provide vetted staff.

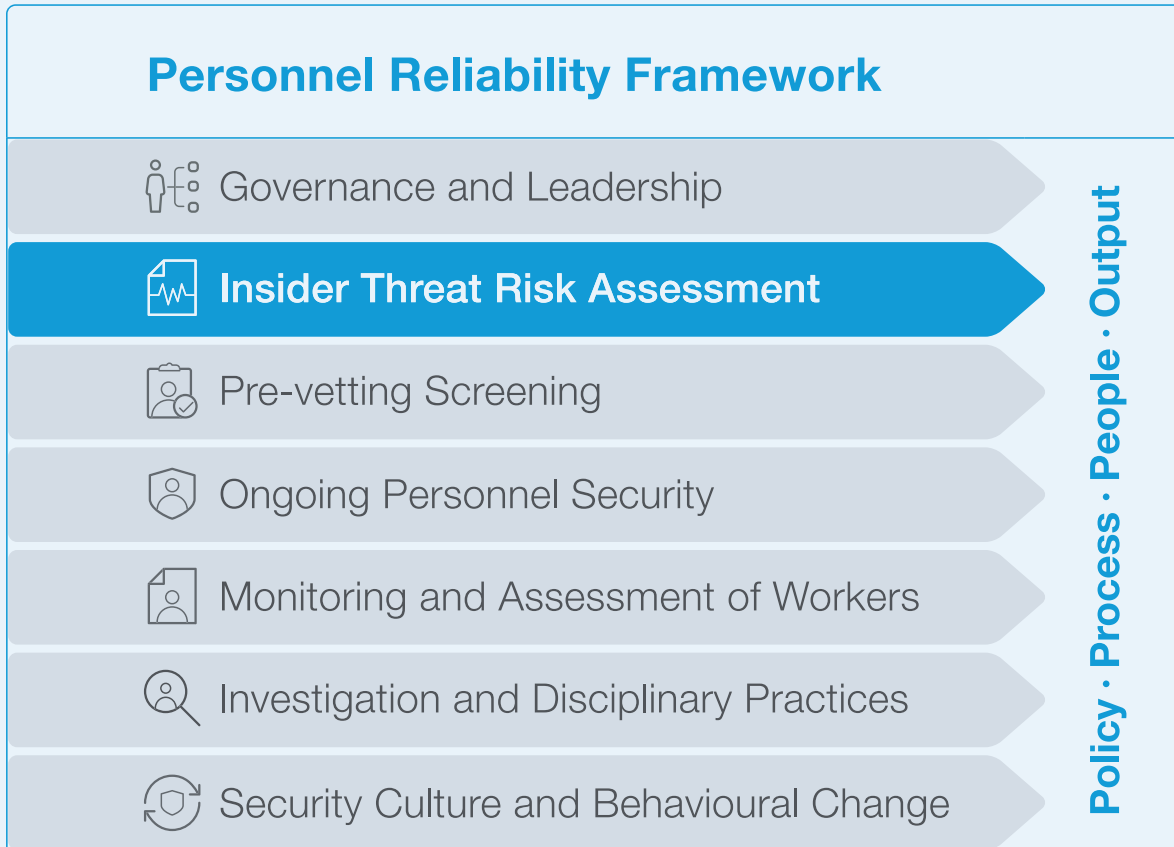


### Key points

- You must ensure that there is appropriate board level oversight and that there is cohesive engagement between the HR / Welfare and Security functions
- Personnel security roles and working groups should be defined and documented, as well as their responsibilities and required vetting levels
- Lines of delegation and decision-making across the network should be clear
- All NSV individuals must be recorded and managed appropriately
- Your landscape of contracts must be recorded and managed appropriately
- All individuals / functions involved in personnel security must be suitably empowered, be appropriately engaged and involved in personnel security-related matters - operating cohesively
- Your framework of governance should be reflected across your organisation's network

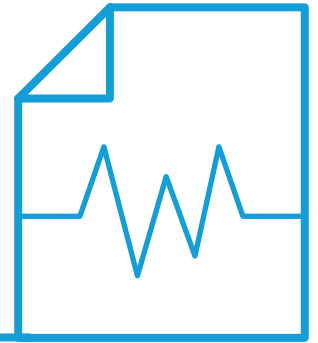


# Insider Threat Risk Assessment





# Insider Threat Risk Assessment Introduction



## CPNI Definition:

Personnel security risk assessment focuses on employees, their access to their organisation's assets, the risks they could pose and the adequacy of existing countermeasures. This risk assessment is crucial in helping security and human resources (HR) managers, and other people involved in strategic risk decisions, communicate to senior managers the risks to which the organisation is exposed.

It is essential for organisations to have a risk management framework in place in order to properly identify, assess and mitigate against personnel security risks.

While the primary risk consideration is for personnel that are able to access HMG information or assets, insider threats can occur from any individual within the organisation that could damage the organisation or its network. Examples include industrial espionage, hostile state activities, criminal activities and activism related to personal ideology.

Risk assessment should be conducted by using a risk methodology that suits your business. At a minimum it should identify and assess the risks that individuals within the organisation and its network pose to HMG assets. You should consider the risks posed by various roles within the organisations, not just the individuals who fill them.

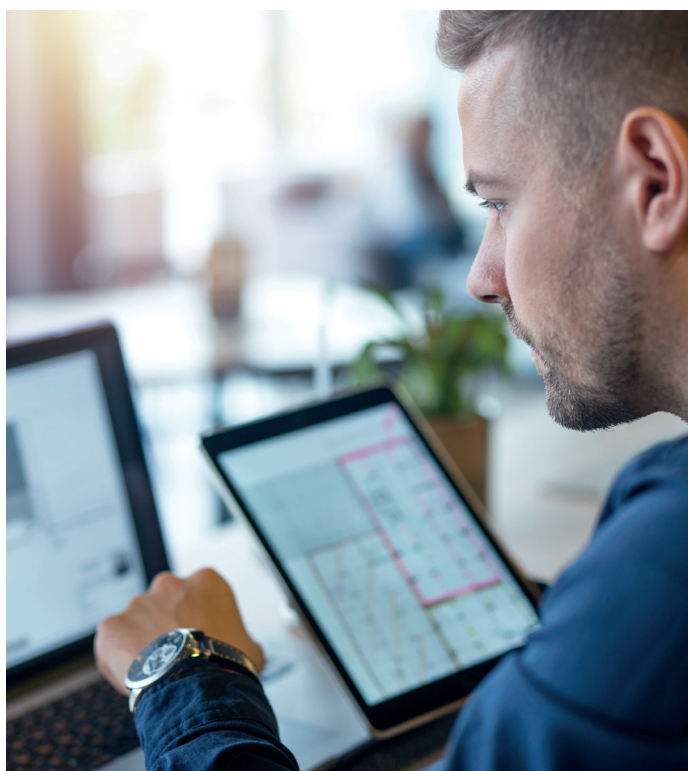
## Insider Threat Risk Assessment

# What are my responsibilities?

---

To implement a clear policy and suite of processes for the identification and mitigation of personnel security risks and insider threats that is appropriate for the size, configuration and maturity of your organisation and network. There should also be mechanisms in place for regularly identifying and assessing new risks as they arise. Your policy and processes should clearly demonstrate the method used to assess, document, categorise, mitigate and regularly track & monitor personnel security risks.

It is recommended that all personnel security risks are captured and managed in a risk register. The risk register should capture all information about each identified risk, such as the nature, impact, likelihood, ownership and mitigation measures proposed or in place to respond to it. A full review of personnel security risks should take place regularly, we recommend at least twice a year.





## Insider Threat Risk Assessment

# What are my responsibilities?

Your organisation should be able to demonstrate clear endorsement and oversight of the personnel security risk register at a senior level, ideally at board level, with ownership of the risk register delegated to a suitably empowered individual.

Overall risk ownership is generally held at board level; however, risks must be actively managed by appropriate individuals who have clear ownership of mitigation activity.

*Note: There is no universal standard for risk categorisation, therefore it is expected that this will differ from organisation to organisation. No standard will be provided by the ISAC, however guidance can be provided if required. CPNI also provides guidance on insider risk management.*



### Key points

- Personnel security risks must be captured and managed in a risk register
- The method used for identifying and managing personnel security risk should be appropriate for the size, configuration and maturity of your organisation and network
- There must be a regular review of personnel security risks by a suitably empowered body. We recommend at least twice a year

# Pre-vetting Screening





# Pre-vetting Screening

## Introduction



### CPNI Definition for Pre-employment Screening:

Pre-employment screening seeks to verify the credentials of job applicants and to check that they meet preconditions of employment (e.g. that they are legally permitted to take up an offer of employment). When conducting checks, it should be established whether the applicant has concealed important information or otherwise misrepresented themselves. To this extent, preemployment screening may be considered a test of character.

The ways in which pre-employment screening is performed vary greatly between organisations. In every case, the aim of pre-employment screening is to obtain information about prospective or existing staff (if promoted and/or changing jobs in the organisation) and use that information to identify individuals who may present security concerns.

Applying the CPNI definition to IPISA, pre-vetting screening comprises the procedures involved in deciding an individual's suitability to hold National Security Vetting (NSV).

This applies to all individual's sponsored for NSV, including new joiners and individuals already employed by an organisation.

All individuals must have been subject to BPSS checks and have a clear requirement to access classified material (SECRET and above) prior to vetting sponsorship. This should include permanent, temporary and contract workers in the organisation and its network.

The mechanisms required to support robust pre-vetting screening includes a check as to whether a clear requirement exists for each individual to hold NSV, a register with key fields to store and manage vetting information, and a secure IT system accredited to OFFICIAL SENSITIVE where that register must be held.

# Pre-vetting Screening

## What are my responsibilities?

### Eligibility policy

Your pre-vetting policy should clearly set out the responsibilities and protocols for verifying that individuals have a clear NSV requirement in line with current NSV policy and GS007 / SPF. The policy must include the eligibility checks that are to be conducted prior to NSV sponsorship, as well as the means to ensure that BPSS checks are satisfactorily completed in line with HMG guidance. This includes where BPSS checks are outsourced. As a sponsor of NSV it is your responsibility to ensure that all BPSS checks have been completed correctly in line with HMG guidance.

### Vetting Register

In order to manage your vetted population, it is important that you have and maintain a robust vetting register where, at a glance, you are able to verify an individual's clearance details and any aftercare activity undertaken. The format that this will take will vary from organisation to organisation dependent on their size, configuration and maturity, however it is essential that the register is held on a Defence Assurance Risk Tool (DART) accredited system (or equivalent) as UKSV have defined the aggregation of vetting information as OFFICIAL SENSITIVE. Details of individuals that hold SC clearance and above must be included on the register, however it could also be utilised for individuals holding BPSS and CTC.

### Forecast

You should be able to provide an annual projection of new clearance applications and / or renewals that you anticipate undertaking in the forecast period indicated for clearances that your organisation will sponsor. This will enable UKSV to accurately manage demand across the entire vetting landscape.



### Key points

- You must be conducting BPSS for every individual prior to submitting an NSV application
- You must utilise a register to actively monitor vetting status and aftercare activity of your vetted population
- Vetting information must be held on a DART (or equivalent) accredited system
- You should be able to accurately forecast future vetting requirements



## Pre-vetting Screening

# What are my responsibilities?

We suggest that your register template should include the following, at a minimum:

→ Clearance applicant / holder's details

→ Clearance details, including clearance level, restrictions, share information (for UKSV-approved shares), expiry date, review date, date of transfer into the organisation's control

→ Justification for clearance

→ BPSS Verification record

→ Aftercare considerations, including:

- Security Appraisal Forms (SAFs) - requests, submissions, completions
- Change of Personal Circumstances (CPCs)
- Aftercare Incident Report (AIR) submissions to UKSV
- Date on which UKSV notified that clearance is no longer required by the company (i.e. lapse)
- Termination by UKSV of clearance
- Organisation if part of a network

Ideally, the following information should also be captured, either in the vetting register or in a separate tool / process.

→ Outcomes of incidents

→ Outcomes of disciplinary processes

→ Outcomes of risk assessments

→ Travel considerations, including travel to high risk countries and travel briefings



# Ongoing Personnel Security





# Ongoing Personnel Security Introduction



## CPNI Definition:

While pre-employment screening helps ensure that an organisation recruits trustworthy individuals, people and their circumstances and attitudes change, either gradually or in response to events.

Ongoing personnel security guidance and tools can be used to help an organisation develop and plan effective practices for countering the insider threat and maintaining a motivated, engaged and productive workforce.

The application of good ongoing personnel security principles adds huge value to physical and technical security measures in a cost-effective manner, promoting good leadership and management and maximising people as part of the security solution.

In GS007 / SPF, aftercare refers to the maintenance of effective ongoing personnel security management.

Effective aftercare by NSV sponsors ensures that vetted individuals continue to meet the obligations of holding a clearance which contributes to the mitigation of risk, particularly in terms of Insider Threat. The aftercare framework ensures that the policy and processes which provide effective aftercare are implemented within each IPSA organisation and for the network it supports.

This requires a holistic approach and includes the full suite of activities for tracking, monitoring and supporting NSV individuals. The outputs may include updates to your vetting register, completion of relevant forms (such as Security Appraisal Forms (SAFs), Aftercare Incident Reports (AIR), and Change of Personal Circumstances (CPC) forms) and notifications to UKSV.

# Ongoing Personnel Security

## What are my responsibilities?

### Policies

Your organisation's aftercare policy must include the management of vetted individuals and the reporting of events that may have a bearing on the holding of a clearance. This may include security and non-security incidents, travel to specified countries, behaviours likely to open an individual to coercion, disciplinary matters and life events such as marriage or divorce etc. It also includes appropriate joining and leaving procedures such as the transfer or lapse of clearances. Your organisation's health and welfare programmes should actively support individuals and their ability to hold a clearance.

Your policy should enable the outcomes of all aftercare-related activities to be captured and reported to UKSV as appropriate as this will contribute to the vetting authority's ability to make decisions on an individual's suitability to hold a clearance. Your policy should also consider the requirement for the role individuals play in providing accurate and up to date information to the vetting authority, for example via self-reporting to UKSV directly or via the security function.

### Examples of events that may have a bearing on the holding of a clearance:



Security and non-security incidents



Travel to specific countries



Behaviours likely to open an individual to coercion



Disciplinary matters



Life events such as marriage or divorce



## Ongoing Personnel Security

# What are my responsibilities?

### Processes

Your aftercare processes should clearly demonstrate how your policies are implemented to effectively manage vetted individuals that you are responsible for. This should include how security, welfare and HR cases are linked to continually provide the vetting authority with the information required to assess the ability of an individual's suitability to hold a clearance. Examples of how this information is provided to the vetting authority include AIRs, CPCs, SAFs and other notifications via UKSV's sponsorship portal.

### Travel to foreign countries

Your processes should also include how vetted individuals travelling to high risk countries are provided with appropriate briefings. You will be provided with access to the list of high risk countries following successful initial assurance.

*Note: Although aftercare activities are required for SC and above, the principles should be applied to all clearance levels, which can include BPSS.*

### Key points

**You must have policies and processes for the handling of all aftercare-related activities across the clearance-holder network including:**

- Security Appraisal Forms (SAFs) for DV Cleared individuals
- Change of Personal Circumstances (CPC) forms
- Aftercare Incident Reports (AIR)
- Transfers (Joiners, Leavers)
- Shares
- Lapses

**You should have a travel policy that:**

- Is aligned with the SPF / GS007
- Includes signposting to CPNI Travel Guidance



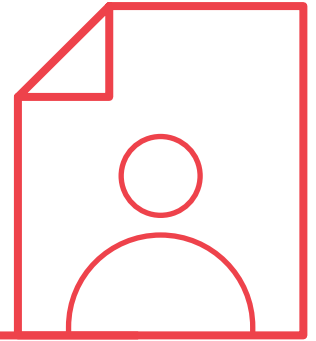
# Monitoring and Assessment of Workers





# Monitoring and Assessment of Workers

## Introduction



### CPNI Definition:

CPNI advocates a holistic approach to protective monitoring where information about employee risks (physical, electronic audit and personnel data) are brought together under a single point of accountability and governance, to ensure a transparent, legal, ethical and proportionate protective monitoring capability.

The purpose of this is to ensure that all workers (and others) are conforming and complying with your policies and systems, identifying individuals who may be posing an insider risk and preventing insider risk to turn into an insider act.

Whilst monitoring and assessment activity of vetted individuals within your organisation and network takes place within each of the strands of the framework, this section highlights specific actions that must be undertaken.

The monitoring of vetted individuals for specific behaviour, as well as the ongoing review of their requirement to hold NSV, is important to reduce the risk of insider threat and to ensure that workers are complying with your organisation's personnel security policies and standards.

This ongoing assurance activity cannot take place in isolation, with aftercare purely owned by the security function. You also need to consider how vetted individuals are monitored when operating elsewhere, such as on client systems and sites.

Line managers and other, potentially non-vetted, staff should be aware of the risks posed to the organisation and the role they play in an organisation's security as a whole.

## Monitoring and Assessment of Workers

# What are my responsibilities?

---

The personnel security section of GS007 / SPF clearly states that the continued holding of a clearance must be subject to the ongoing access of classified material at SECRET or above. In order to ensure that only those individuals with this requirement hold a clearance you should conduct regular reviews of the vetted staff within your organisation and network.

Your policy for reviewing the vetting requirement(s) for individuals to continue to hold a clearance must be tied in with or be part of your eligibility policy. At a minimum it must clearly state the frequency at which reviews will occur and the steps to take if the requirement to hold NSV no longer exists. It is recommended that these reviews occur at least annually, though for some organisations it will be prudent to undertake this more often. The outcome of this review and any steps taken should be captured in your organisation's Vetting Register (see pre-vetting screening).





## Monitoring and Assessment of Workers

# What are my responsibilities?

### Employee Behaviours

Your organisation should have a policy for how the behaviour of workers is monitored to identify suspicious behaviour and / or identify individuals who may be vulnerable or susceptible to coercion. This policy must include what behaviour is being monitored, how it is being monitored (which could include monitoring software, financial checks and line management training to recognise behaviour of concern) and what your organisation does with this information. It must also include the steps that are taken in the event that these behaviours are demonstrated by individuals, such as mechanisms that trigger risk management, incident and HR processes, and notifications to UKSV.

It is worth noting that this activity may include those who do not hold NSV such as colleagues or line managers.

### Key points

- You must hold regular reviews to ensure that only those with an ongoing requirement retain their NSV
- There must be a link between HR / Welfare and security to ensure that potential indicators that an individual is no longer suitable for holding NSV are flagged appropriately
- Mechanisms should be in place for the active monitoring of individuals that hold NSV with clear processes for line managers / colleagues to report potentially suspicious behaviour



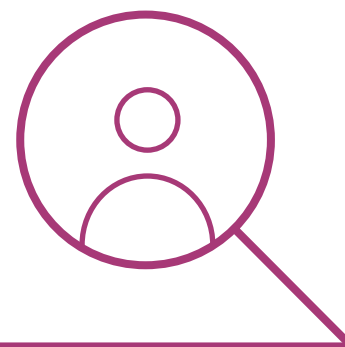
# Investigation and Disciplinary Practices





# Investigation and Disciplinary Practices

## Introduction



### CPNI Definition:

Most organisations will, at some point, need to carry out some kind of internal investigation into a member of staff.

With correct procedures in place, employees who understand policies and regulations, and competent trained investigative staff, your organisation is better equipped to avoid these pitfalls and maintain trust.

In addition to investigating an insider act your organisation needs to have a risk management process in place which manages the consequences of the act and a process in place that helps you:

Identify and analyse the root cause of the incident;

- Identify the appropriate disciplinary actions or interventions that need to be undertaken;
- Assess the effectiveness of current control measures in place;
- Identify gaps in practice and;
- Develop more effective control measures.

This should be in line with the relevant employment law and HR processes.

IPSA requires the implementation of policies and processes that support investigative activities to ensure that the appropriate mitigation takes place.

This includes the identification, root cause analysis and resolution of security incidents, which covers the implementation of mechanisms to future-proof your organisation from the recurrence of these incidents as far as possible.

It also includes the proportionate disciplinary actions for any individual(s) involved, both within the organisation's clearance-holder population and its network. Investigations may trigger aftercare activity such as notifying UKSV through incident reports or further internal risk management.

## Investigation and Disciplinary Practices

# What are my responsibilities?

---

Your policy for the handling of security incidents should reflect the requirements of GS007 / SPF noting that special requirements are in place for the handling of incidents involving international material. There isn't a single standard for incident handling across government, so for further information on incident handling for specific contracts please consult the information owner or relevant contracting authority.

Your policy should include the responsibilities and protocols for identifying, reporting, classifying and resolving security incidents with a view to preventing any recurrence. It must also tie in with your organisation's security, monitoring, risk management and disciplinary policies.

Policies should include proportionate sanctions where appropriate, helping to deter others from repeating this behaviour.

Your disciplinary policies should be integral to your welfare and security policies, clearly setting out the responsibilities and protocols for how behaviour that impacts security is identified and managed. This should support compliance with security regulations and contractual responsibilities.





## Investigation and Disciplinary Practices

# What are my responsibilities?

Your processes should clearly demonstrate how your organisation executes the protocols laid out in your disciplinary policy to effectively and appropriately manage and discipline individuals who have engaged in poor or inappropriate behaviour. Triggers for any subsequent actions such as risk management or aftercare processes must be included.



### Key points

- You must have appropriate policies and processes in place to investigate and (where appropriate) put in place sanctions following security incidents
- Your policies must be aligned to the relevant government security standards (e.g. GS007 or the SPF)
- You should seek guidance from your contracting authority on the procedures you need to follow for your specific contract

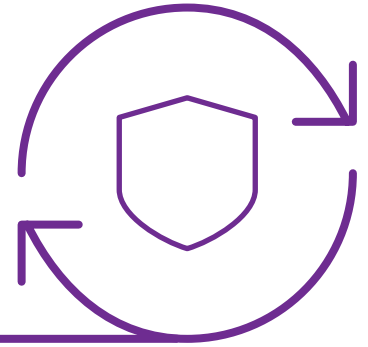
# Security Culture and Behavioural Change





# Security Culture and Behavioural Change

## Introduction



### CPNI Definition:

A good security culture in your organisation is an essential component of a protective security regime and helps to mitigate against insider threats and external people threats (such as hostile reconnaissance).

Security culture is the set of values, shared by everyone in an organisation, which determine how people are expected to think about and approach security, and is essential to the protective security regime as a whole.

### Encouraging a positive security culture within your organisation and network is key to the effective management of aftercare.

Through impactful training and communications you can enable staff to be fully aware of the risks posed to them and how they, as individuals, contribute towards risk mitigation.

Vetted staff should be fully aware of the responsibilities of being a clearance holder. Ways of achieving this include an induction programme, regular training and an annual communications campaign that is tied to current risks and issues faced by an organisation. It is also recommended that vetted staff have access to a central repository where they can find information on security policy and processes.

Activity to support a positive security culture should be proportionate to the size, shape and maturity of the organisation. Key within this strand is the ability to reach individuals in the wider clearance network to ensure they have the same support and knowledge as those within the main organisation.

# Security Culture and Behavioural Change

## What are my responsibilities?

### Training

Your induction and ongoing training programme should train staff on all elements of security culture, ensuring they are aware of the policies and processes they need to follow in order to mitigate security risks. Training should be targeted to the different levels of responsibilities for aftercare and personnel security across your organisation and network, this may include those who do not hold NSV.

How this training is developed and delivered should be pragmatic and proportionate to the size, shape and maturity of the organisations involved. For example, for a small organisation it may be appropriate to provide access to existing packages developed by CPNI, the MOD or another organisation. A larger organisation may need to develop bespoke packages that highlight the specific requirements of their business. In either scenario, an organisation should identify where elements of the training programme are mandatory and how that will be monitored.

Specifically, your training programme must provide vetted staff with the knowledge and understanding of the responsibilities of being a clearance holder, security principles and an appreciation of the threats to individuals, organisations and HMG.

You should consider how your training programme is evaluated to ensure it is fit for purpose and reviewed regularly to ensure it contains the latest information provided by HMG.

**Your training programme must provide vetted staff with the knowledge and understanding of:**



The responsibilities of being a clearance holder



Security principles



An appreciation of the threats to:

- Individuals
- Organisations
- HMG

## Security Culture and Behavioural Change

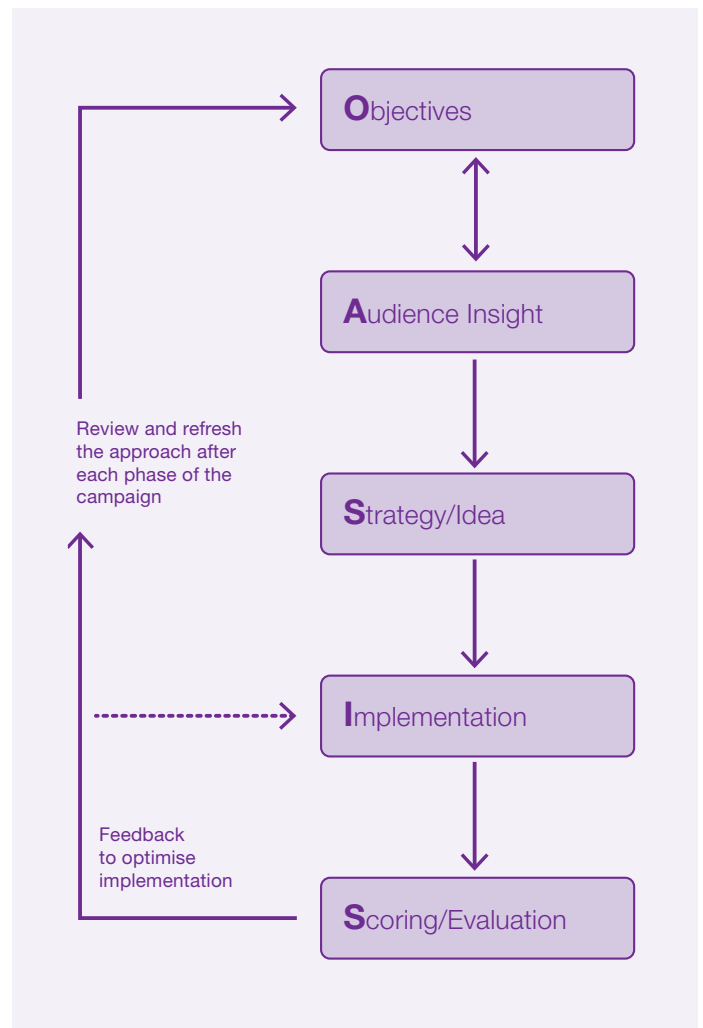
# What are my responsibilities?

### Communications

Your communications programme should engage staff on all elements of security culture, ensuring they are aware of the policies and processes they need to follow to mitigate security risks.

It should demonstrate clear objectives, an understanding of the audiences / stakeholders that need to be reached as well as a clear timeline of activity and evidence of evaluation of risks / previous campaigns to determine output. You should consider how the effectiveness of your campaigns will be measured and assessed. Communication should be targeted to the different levels of responsibilities for aftercare and personnel security across your organisation and network. You should pay attention to how your communications activity will reach vetted staff across your wider network, in particular those outside of the main organisation (e.g. subcontractors).

There is no set method for developing or presenting this, but the OASIS guidance produced by the Government Communications Service can be used as a basis.





# Security Culture and Behavioural Change

## What are my responsibilities?

### Knowledge Repository

It is vital that those who hold NSV are aware of the government / organisation personnel security policies and processes they need to adhere to. This information will partially be provided by robust training and communications programmes; however, it is also recommended that a repository is in place that enables staff to access information on demand whenever a question arises.

By ensuring individuals have access to the right information and expertise you will be able to reduce the risk of security incidents caused by ignorance as well as empowering individuals to play an active role in combating insider threats within your organisations.

The way individuals are able to access this information can take many forms and should be proportionate to the size, shape and maturity of your organisation and network. Options include a nominated point of contact, intranet pages or a fully integrated security web portal / help desk.



### Key points

- Vetted staff are required to be aware of their responsibilities as a clearance holder.
- Information should be regularly refreshed to ensure staff are kept up to date with the latest requirements and risks they need to be aware of.
- A positive security culture stems from all parts of the organisation, and therefore is tied to Governance and Leadership where there is appropriate senior leadership visibility of required security practices.
- By providing easy access to security policies and process you can empower staff to take an active role in personnel security risk management.



# Glossary



## Glossary

### A

#### **Active contracts**

Current, open contracts that IPSA organisations are currently supporting that requires security vetted staff.

#### **Aftercare**

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.

#### **Aftercare Incident Report (AIR)**

Report sent to UKSV following any incident / assessment of behaviour that would impact an individuals ability to hold a clearance. Incidents also should be reported to the relevant contracting authority.

#### **Annual review**

An annual IPSA Dashboard submission, due by the beginning of November each year.

#### **Assessment period**

The full assessment will be undertaken every three years in line with required due diligence refresh. A smaller review will need to be completed annually.

### B

#### **Baseline Personnel Security Standard (BPSS)**

The Baseline Personnel Security Standard (BPSS) is a basic pre-employment check. It is not a National Security clearance, but its rigorous application underpins National Security Vetting.

#### **Board Level Contact**

A Board Level Contact is the senior responsible individual for security in an organisation. They must be a British national and a member of the Board of Directors and is specifically responsible for:

- a) exercising policy control;
- b) giving appropriate authority and effective support to the (Personnel) Security Controller;
- c) approving Company Security Instructions;
- d) informing the DSO or security officials of the relevant Contracting Authority of changes to the company's status (e.g. ownership, control, closure etc).

### C

#### **Change of Personal Circumstances (CPC)**

Adhoc form to report to UKSV any changes that may have an impact on an individuals ability to hold a clearance.

#### **Contracting Authority**

The MOD Project Team or IPSA / FSC organisation that contracts with another IPSA / FSC organisation for the provision of National Security Vetted individuals.

#### **Centre for Protection of National Infrastructure (CPNI)**

CPNI is the government authority for protective security advice to the UK national infrastructure. Their role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. They are the National Technical Authority for personnel and physical security.

#### **Counter-Terrorist Check (CTC)**

CTC is the first level of National Security Vetting. Its purpose is to prevent those who may have connections with terrorist organisations, or who may be vulnerable to pressure from such organisations, from gaining access to certain roles and, in some circumstances, from gaining access to premises, where there is a risk that they could exploit that position to further the aims of a terrorist organisation. A CTC, alone, does NOT allow individuals regular access to, or knowledge or custody of, classified assets.



## Glossary

---

### D

#### **Developed Vetting (DV)**

DV is the third and highest level of National Security Vetting. Its purpose is to counter the threat to the most sensitive material classified TOP SECRET from espionage, terrorism and other threats to national security. It is required for those individuals who need long-term, frequent and uncontrolled access to TOP SECRET assets.

---

#### **Disciplinary Framework**

The framework of policies and processes put in place to appropriately manage individuals who have engaged in any activity that exposes the organisation, its supply chain and / or HMG to increased security risk or threat.

---

### F

#### **Facility Security Clearance (FSC)**

FSC is the physical security assurance process for partners in industry that are required to hold classified material at SECRET (or international CONFIDENTIAL) or above on their own premises.

---

#### **Foreign connections**

Includes links to other countries in terms of company ownership (parent company) and Board level governance as well as overall influence that other countries may have on the operations and strategy of the organisation.

---

### G

#### **GISA**

Government Industry Security Assurance form - The application form to undertake the IPSA and FSC processes. This form is used for application, notification of change of details and at three year assurance checks.

---

#### **Good Practice Repository**

A central resource of information (physical, virtual or on-demand) that individuals can access, which contains security processes, policies and responsibilities. This is to ensure that all staff with National Security Vetting are aware of their role and responsibility in personnel security and aftercare.

---

#### **Governance Framework**

The roles and responsibilities of an organisation in implementing and maintaining the policies and processes that oversee and manage the sponsorship of National Security Vetting, aftercare activities and Personnel Security Risk.

---

### H

#### **Her Majesty's Government (HMG)**

The official term for the Government of the United Kingdom of Great Britain and Northern Ireland.

---

#### **HMG Contracting Authority**

Contracting Authorities means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities (as per Public Contracts Regulations 2015) that you (or the prime supplier in your chain) is contracted to.

---



## Glossary

### I

#### **Incident Handling Framework**

The framework of policies, programmes, processes and governance implemented by an organisation to actively manage security incidents from discovery to resolution within the organisation and its network, in order to future proof the organisation from the recurrence of such incidents.

#### **Incidents**

Any security incident involving HMG owned, processed or generated information (e.g. incursion, security breach, loss or compromise). This includes information owned by a third party e.g. NATO or another country which HMG is responsible for, or any other information which could impact on security.

#### **Insider Threat**

In line with CPNI definition, an insider is someone who exploits, has the intention to exploit or can be exploited by others to use their legitimate access to an organisation's assets for unauthorised purposes.

#### **Insider Threat / Personnel Security Risk**

In line with CPNI definition, these are identified threats or vulnerabilities aligned to personnel that have been assessed for their likelihood (of the threat event occurring) and impact (to the organisation and/or third parties), should the threat transpire.

#### **IPSA**

IPSA is a Personnel Security assurance framework for industry that will ensure that individuals who have undertaken National Security Vetting are effectively managed and provided with the same degree of aftercare as vetted staff in HMG. It gives partners in industry who meet the required standard of management and aftercare the ability to sponsor NSV in support of HMG contracts.

#### **IPSA Dashboard**

The IPSA dashboard is how you will capture statistics that evidence the outputs of your personnel security policies and processes, showing that they support effective aftercare for NSV individuals in your organisation and network. It is submitted during initial accreditation and annually thereafter.

#### **IPSA Evidence Cover Sheet**

The cover sheet supports the submission of the evidence required for IPSA at initial accreditation and during the triennial assurance. Once completed, it serves as a summary of all evidence artefacts that are submitted to the ISAC.

#### **IPSA Organisation**

The organisation that has undertaken IPSA Accreditation and therefore has sponsorship ability and aftercare responsibility.

#### **ISAC**

Industry Security Assurance Centre - One of the Government Security Centres established the Government Security Group.

#### **ISAC Reference Number**

The unique identification number assigned by the ISAC once the organisation has attained IPSA status. For organisations who already hold an FSC this will be your existing DE&S reference number.

### K

#### **Knowledge Repository**

A central resource of information (physical, virtual or on-demand) that individuals can access, which contains security processes, policies and responsibilities. This is to ensure that all staff with National Security Vetting are aware of their role and responsibility in personnel security and aftercare.



## Glossary

---

### L

#### **Lapsed Clearance**

Where a clearance is no longer required and UKSV are informed. Where a clearance is in date it can be re-instated within a 12 month period. After this time a new clearance will need to be sponsored.

---

#### **List V**

The project name used during the development of the Industry Personnel Security Assurance (IPSA) process.

---

#### **List X**

List X is the former name of the Facility Security Clearance (FSC) process. You may still see List X in documentation and policies as they are slowly updated over time.

---

### N

#### **National Security Vetting (NSV)**

National Security Vetting is a key component of Personnel Security and comprises a range of additional checks that are undertaken by the United Kingdom Security Vetting (UKSV) organisation when there is a requirement for an individual to have regular access to classified information or assets or access to a particular HMG site or establishment.

---

#### **Network**

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

---

#### **Network point of contact**

This is the individual within each network organisation that the IPSA organisation will liaise with on Personnel Security matters.

---

#### **NSV Equivalent Clearances (International)**

NSV cannot be transferred between nations. However, under international agreements a recognised clearance issued by a foreign government, subject to determination by UKSV, may be considered to be the equivalent of a UK issued NSV such as SC or DV. This is recorded on the UK vetting system under its UK NSV equivalent.

---

### O

#### **Organisation**

The company / contractor undertaking the IPSA process and therefore has sponsorship ability and aftercare responsibility.

---

### P

#### **PerSec Risk Management Framework**

The set of artefacts related to identifying, assessing and mitigating personnel security risk within the IPSA organisation. This includes policies and processes implemented within the organisation, the output of which is the personnel security risk register that records all PerSec risks, including insider threats. Board level oversight as well as senior management mandate of these artefacts is essential to a robust and effective PerSec risk management framework.

---

#### **PerSec Risk Management Policy**

This is the organisation's approach for how personnel security risk (including insider threats) are actively monitored, assessed, managed and tracked. This must be applicable to the organisation as well as to its network.

---

#### **PerSec Risk Management Processes**

This is the suite of processes embedded within the organisation that facilitate the identification, assessment, mitigation and tracking of personnel security risks both within the organisation and its network.

---



## Glossary

CPNI recommends that the first step in PerSec Risk Management is conducting a risk assessment across your organisation. For IPSA this must include both your organisation and network and involves identifying insider threats as well as personnel security risks.

### **Personnel Reliability Framework**

The framework of policies, programmes, processes and governance that must be implemented by an organisation in order to qualify for IPSA Accreditation. The implementation of this framework enables and facilitates the required sponsorship and aftercare activities required for IPSA.

### **Personnel Security (PerSec)**

Personnel security is the system of policies and procedures which seek to mitigate the risk of workers (insiders) exploiting their legitimate access to an organisation's assets for unauthorised purposes.

### **Personnel Security Controller**

The nominated representative 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. Ultimately 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 (and any Deputies) must be sufficiently empowered by the Board to carry out their responsibilities. The FSC Security Controller can also be the IPSA Personnel Security Controller.

### **Personnel Security Maturity Model (PSMM)**

The Personnel Security Maturity Model is issued by the UK's Centre for the Protection of National Infrastructure (CPNI) with the aim of providing a framework for organisations to assess their maturity in dealing with personnel security risks.

### **Personnel Security Risk Register**

The personnel security risk register is the tool that your organisation uses to document personnel security risks in your organisation and network.

### **Pre-vetting checks**

The activities required to determine suitability for sponsoring clearances.

### **Prime Contractor**

This is the organisation with whom the IPSA organisation / IPSA applicant has a direct contractual relationship, where the contract is not an HMG Contracting Authority. This could include an organisation with a contractual relationship with an HMG Contracting Authority, foreign organisations, foreign governments and Transnational bodies.

### **Process flows**

A visual representation of the steps in a business process. This includes start points / initiators, inputs, activities, decision-points, owners and outputs.

## R

### **RACI**

A responsibility assignment matrix that describes the participation by various roles in completing tasks or deliverables for a project or business process. RACI covers the four key responsibilities: Responsible, Accountable, Consulted, and Informed.

## S

### **Security Appraisal Form (SAF)**

The annual form submitted to UKSV to enable cleared individual and their manager to identify any changes in circumstances or security behaviours that may impact an individual's ability to hold a clearance. This is mandatory for DV holders.



## Glossary

### Security Check (SC)

SC is the second level of National Security Vetting. Its purpose is to counter the threat to material classified SECRET from espionage, terrorism and other threats to national security. It is required for those individuals who need long-term, frequent and uncontrolled access to SECRET assets.

### Security Culture

CPNI defines security culture as the set of values, shared by everyone in an organisation, which determine how people are expected to think about and approach security, and is essential to an effective personnel and people security regime.

### Security Risk Management (SRM) Principle

The principles by which the IPSA organisation assesses risk and determines mitigating actions. The aim of implementing these principles is to ensure consistency across the way an organisation identifies and actively manages risk.

### Shared Clearance

Where responsibility for the management of a clearance is shared between two organisations, usually as a result of providing services to multiple organisations.

### Sponsor / NSV sponsor

The term sponsor can refer to both the organisation that has sponsorship rights, and the individual (usually a vetting officer) who actually undertakes the sponsorship activity.

Throughout the IPSA guidance we use sponsor to refer the wider organisation or company that has undertaken the assurance process and been given the ability to sponsor individuals for National Security Vetting.

## T

### Transfer of Clearance

The activity required where an individual moves from one sponsoring organisation to another and responsibility of aftercare transfers to the new organisation. This includes the acceptance of responsibility from another organisation.

## U

### UKSV

United Kingdom Security Vetting (UKSV) is the single government provider of National Security Vetting (NSV). They are the centre of excellence for security vetting and enable government to protect citizens and provide vital public services, by understanding and managing security risks.

## V

### Vetting Register

The central detailed record of all National Security Vetted staff that includes, at a minimum, the details of the clearance, expiry date and aftercare activity. It must be held in a DART accredited system. It is the tool on which all of your NSV-related information must be stored to aid the management of clearances.

## W

### Withdrawals

Where a clearance is cancelled, usually as the result of an individual no longer being suitable to have access to classified material.









# Government Security

We are government security.

Government Security is a cross-departmental function of HM Government.

ISAC is led by the Ministry of Defence.

For more information, please contact  
[isac-group@mod.gov.uk](mailto:isac-group@mod.gov.uk)