Government
Security

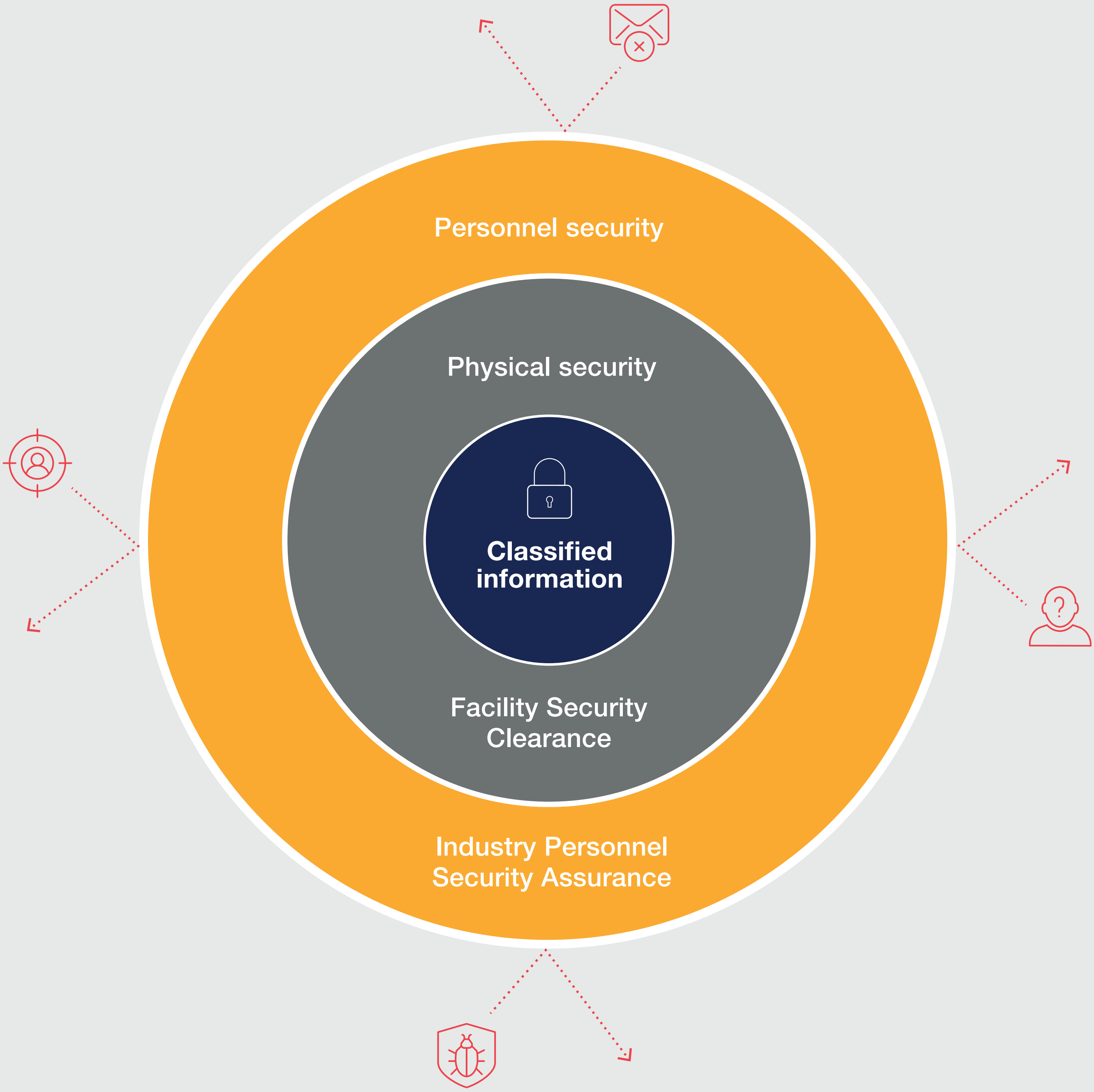
Industry Security
Assurance Centre
A Government Security Centre

Industry Personnel Security Assurance

Accreditation and Ongoing Assurance Guide

Contents

Industry Security Assurance


Personnel security
Physical security
Classified information
Facility Security Clearance
Industry Personnel Security Assurance

Introduction

Industry Personnel Security Assurance (IPSA) is an assurance framework for personnel security in industry. It will help us 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. The process is managed by the Industry Security Assurance Centre (ISAC).

The assurance process assesses your ability to effectively manage personnel security, in particular how you provide aftercare for those staff that require NSV. Aftercare is more than the completion of annual forms, it is the culmination of a number of activities that provide the necessary support for vetted individuals. It covers the screening required pre-vetting, ongoing monitoring and assessment, disciplinary and welfare procedures, risk assessment and cultivating a positive security culture at all levels throughout the organisation and its network.

We do this through assessing that your policies and processes meet required standards (as per GS007 / SPF and the Personnel Reliability Framework contained in the IPSA Policy, as well as NATO, STRAP / SAP and compartmentalisation considerations as appropriate).

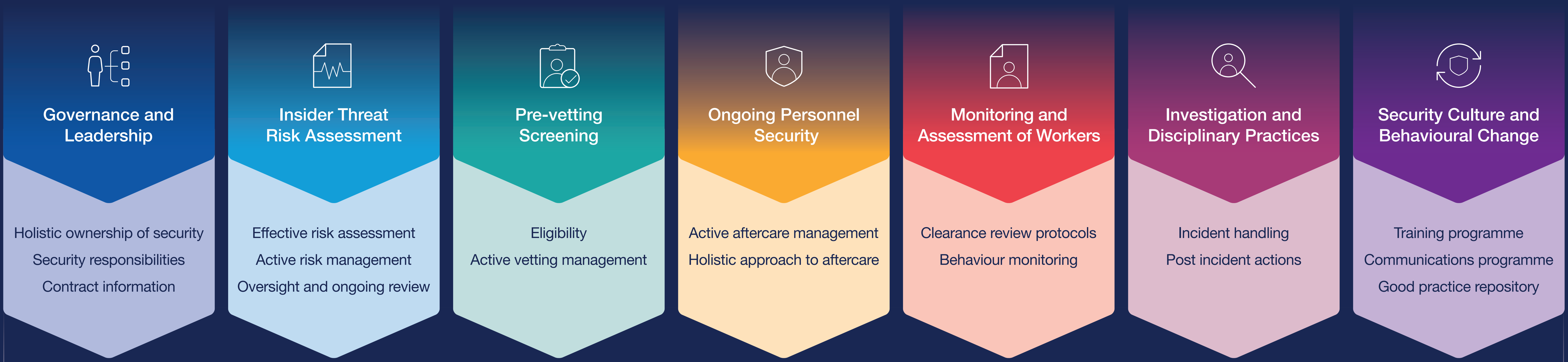
Your policies should lay out the overarching principles and activities required by your organisation to support robust personnel security, in line with the Personnel Reliability Framework (PRF). The processes should demonstrate how these policies are implemented and responsibilities fulfilled across your entire network.

This guide will provide you with the information you need to undergo IPSA accreditation and participate in ongoing annual and triennial assurance. It should be read in conjunction with the IPSA policy and the IPSA PRF guidance, which will provide you with the information on the standards of personnel security and vetting aftercare that your organisation should be reaching.

The standards within the PRF are a series of outputs that we would expect an organisation to be delivering. However, how those outputs are delivered should be tailored based on the size, configuration and maturity of the organisation being assessed.

This guide will provide you with direction on the information that is, and is not, required for each strand of the framework, and how it should be submitted to ensure a smooth assurance process.

Personnel Reliability Framework



Governance and Leadership

- Holistic ownership of security
- Security responsibilities
- Contract information

Insider Threat Risk Assessment

- Effective risk assessment
- Active risk management
- Oversight and ongoing review

Pre-vetting Screening

- Eligibility
- Active vetting management

Ongoing Personnel Security

- Active aftercare management
- Holistic approach to aftercare

Monitoring and Assessment of Workers

- Clearance review protocols
- Behaviour monitoring

Investigation and Disciplinary Practices

- Incident handling
- Post incident actions

Security Culture and Behavioural Change

- Training programme
- Communications programme
- Good practice repository

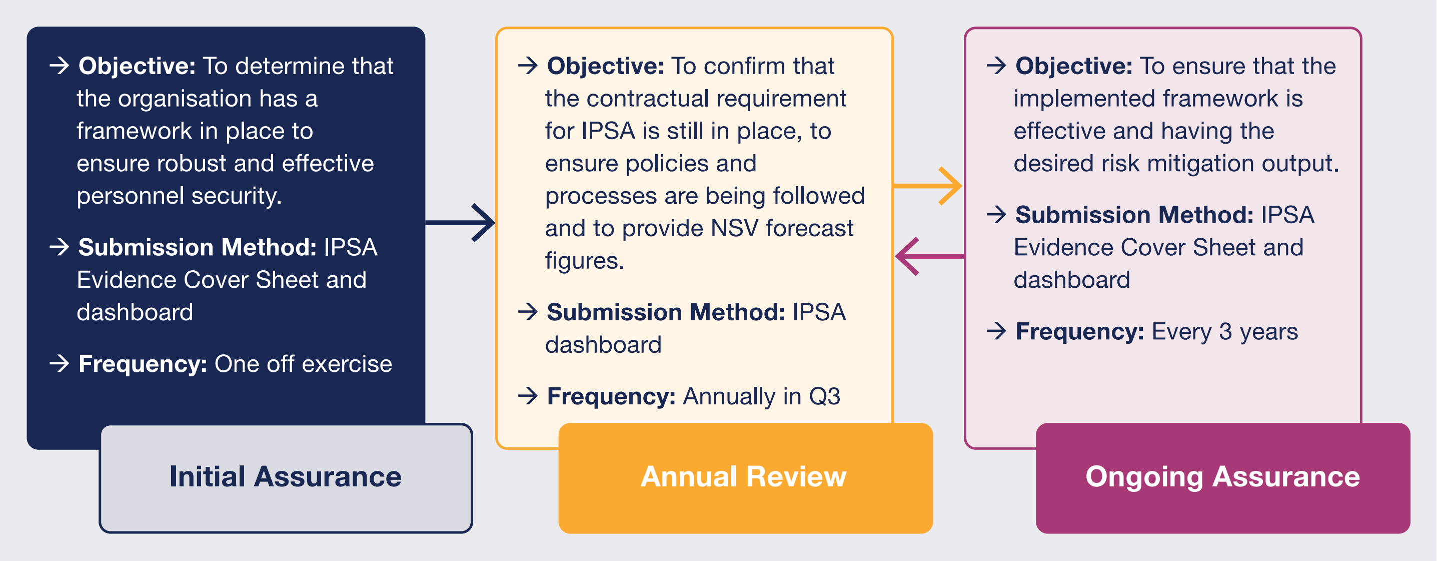
Policy • Process • People • Output

Accreditation and Assurance Process

In order to make an application to undertake IPSA, an organisation must first ensure they meet the eligibility criteria as set out in the IPSA policy, **Part I – Section 2**.

Eligibility Criteria

- The Contractor has a legitimate requirement to provide NSV workers for HMG contracts, or is applying for Facilities Security Clearance.
- The Contractor must be registered with Companies House.
- 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.
- 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:
  - the Ministry of Defence (MOD) or international equivalent; or
  - a sub-contractor within the supply chain of the MOD or international equivalent; or
  - an International Defence Organisation
- At least one individual on the Board of Directors reside in the UK and be a British National.



Initial Assurance

→ **Objective:** To determine that the organisation has a framework in place to ensure robust and effective personnel security.

→ **Submission Method:** IPSA Evidence Cover Sheet and dashboard

→ **Frequency:** One off exercise

Annual Review

→ **Objective:** To confirm that the contractual requirement for IPSA is still in place, to ensure policies and processes are being followed and to provide NSV forecast figures.

→ **Submission Method:** IPSA dashboard

→ **Frequency:** Annually in Q3

Ongoing Assurance

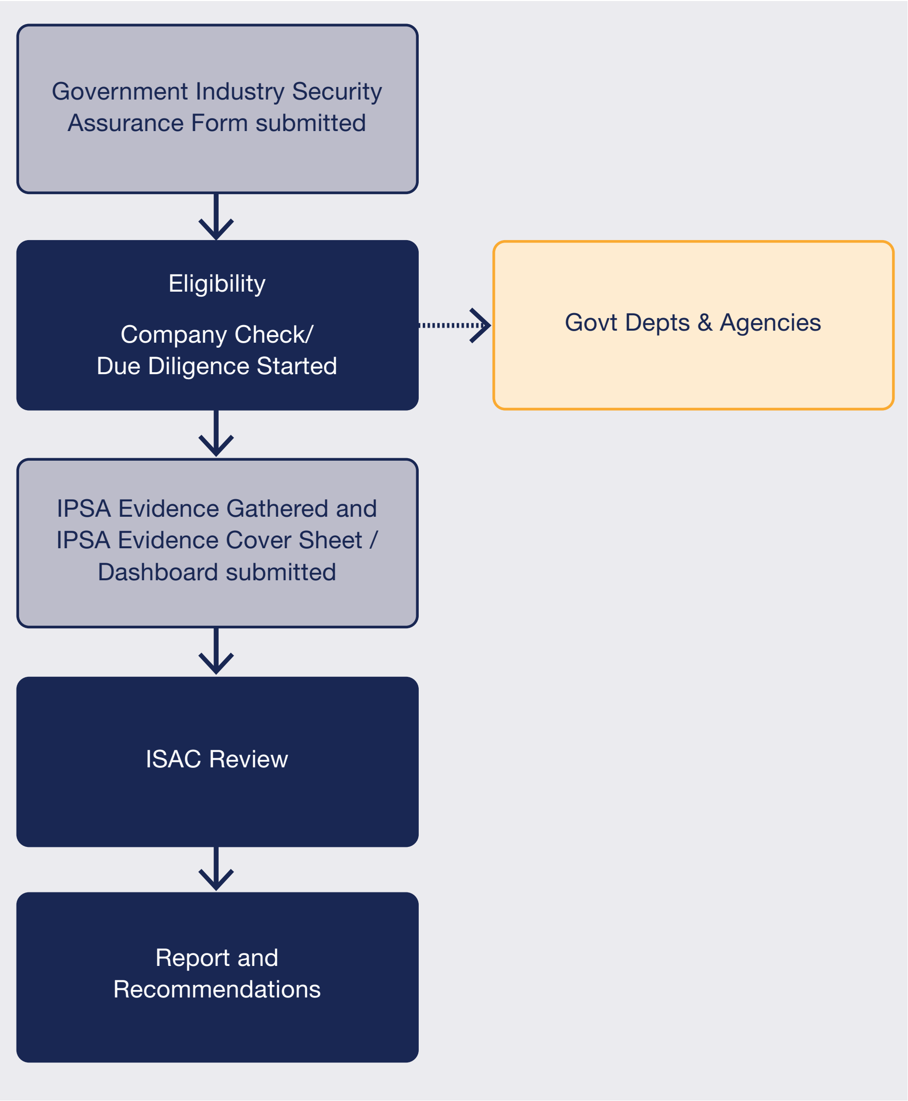
→ **Objective:** To ensure that the implemented framework is effective and having the desired risk mitigation output.

→ **Submission Method:** IPSA Evidence Cover Sheet and dashboard

→ **Frequency:** Every 3 years

This process enables the ISAC to firstly understand whether an organisation has the appropriate framework in place to provide effective aftercare for vetted individuals across their entire network. On an ongoing basis we will review the organisations policies, processes and their outputs to ensure they are having the desired personnel security risk mitigation.

Guidance for Organisations not already subject to IPSA / FSC assurance


Government Industry Security Assurance Form submitted
Eligibility
Company Check/ Due Diligence Started
Govt Depts & Agencies
IPSA Evidence Gathered and IPSA Evidence Cover Sheet / Dashboard submitted
ISAC Review
Report and Recommendations

The first step for organisations not already subject to FSC assurance will be to complete the Government Industry Security Assurance (GISA) form. This will confirm your IPSA eligibility and provide the information required to kick start the company checks with partners across government.

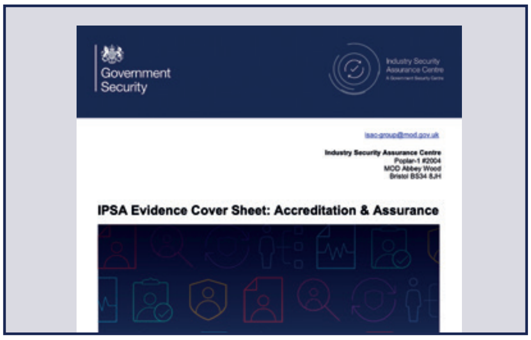
At the same time, organisations should begin to gather the evidence required for the ISAC to assess their ability to conduct effective aftercare.

You will be provided with access to an upload portal when required to submit your evidence, IPSA Evidence Cover Sheet and Dashboard.

When ready, the evidence will be submitted as follows;

- **Your Evidence** – The policies, processes and output evidence that support your IPSA application

- **The IPSA Evidence Cover Sheet –** where the policies and processes relevant to each strand of the framework are highlighted



Government Security

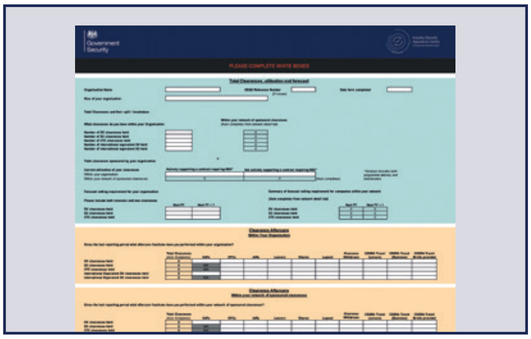
Industry Security Assurance Centre
A Government Security Centre

isac-group@mod.gov.uk

Industry Security Assurance Centre
Poplar-1 #2004
MOD Abbey Wood
Bristol BS34 8JH

IPSA Evidence Cover Sheet: Accreditation & Assurance

- **The IPSA Dashboard –** where metrics are captured to show the outputs of relevant personnel security policies and processes.



Government Security

PLEASE COMPLETE WHITE BOXES

Total Clearances, utilisation and forecast

Clearance Aftercare
Within Your Organisation

Submissions will be assessed to understand whether an organisation is meeting the baseline personnel security requirements or not.

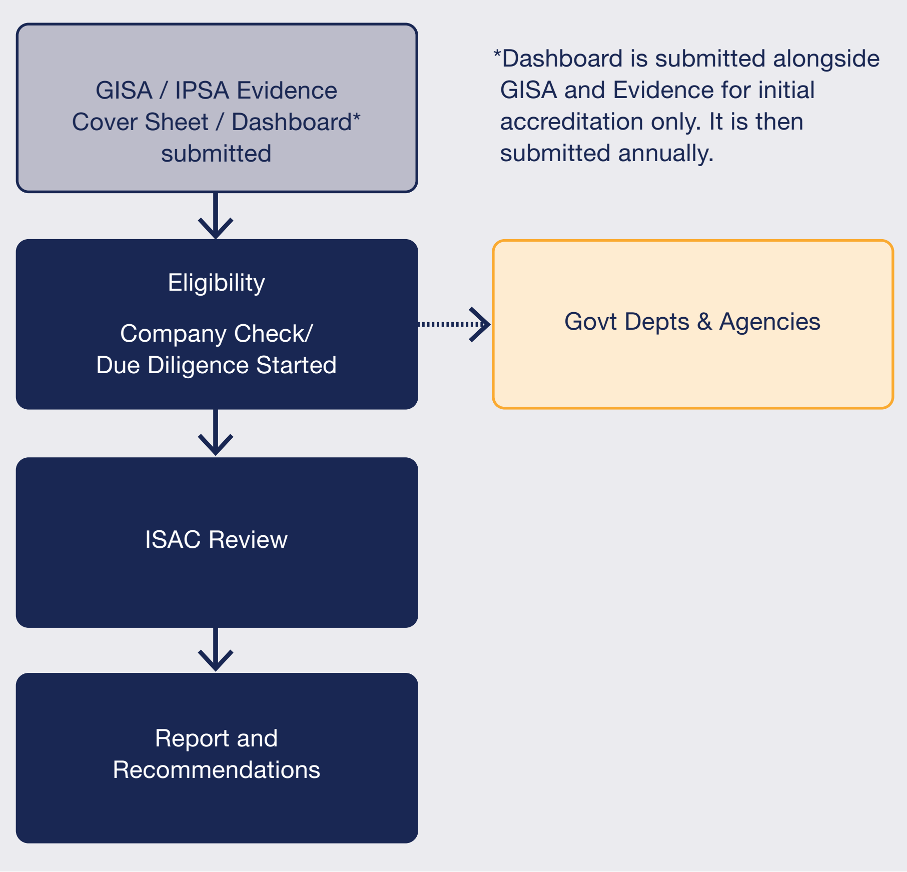
Following the assessment, where required, a series of recommendations will be provided to guide organisations on how to improve their personnel security policies and processes.

!

IMPORTANT

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 contacting the ISAC.

Guidance for Organisations already subject to IPSA / FSC assurance


GISA / IPSA Evidence Cover Sheet / Dashboard* submitted
Eligibility
Company Check/ Due Diligence Started
Govt Depts & Agencies
ISAC Review
Report and Recommendations

*Dashboard is submitted alongside GISA and Evidence for initial accreditation only. It is then submitted annually.

Organisations that already hold an FSC and are undertaking IPSA for the first time, or at the three yearly assurance point, will follow a very similar process. The main difference is that the GISA Form, IPSA Evidence Cover Sheet and Dashboard can be submitted at the same time.

Whilst initial assurance focuses on the policies and processes an organisation has in place, the ongoing assurance checks will place greater emphasis on the outputs of those processes and any changes since the last assessment. In particular, the ISAC will be looking for evidence that policies and processes are being followed, and that they are having a positive impact on the personnel security culture within the organisation and its network.

Completing the Forms

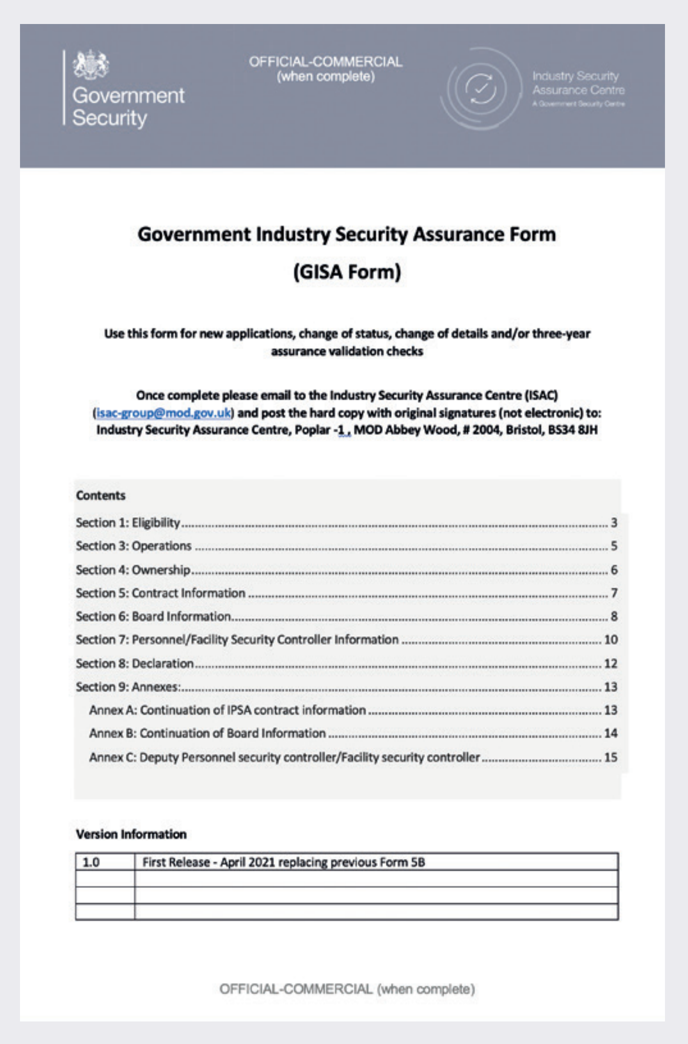
Government Industry Security Assurance (GISA) Form

Completing the Government Industry Security Assurance (GISA) application form is the first step in undertaking either the FSC or IPSA process. It is how you submit your application and provide the background information on your organisation and its leadership required to undertake due diligence checks.

In order to streamline the process, and avoid duplication of effort, this form will also be used to inform the ISAC of a change to any company details – for example a change in Directors, Board Level Contact (BLC) or (Personnel) Security Controller ((P)SC). When being used to inform the ISAC of a change of details, only the relevant sections need to be completed.

Every three years, as part of the ongoing assurance process, you will also need to use the GISA to confirm specific company details and ongoing adherence to the BLC and (P)SC Terms of Reference. If no details have changed since the form was last submitted, you only need to complete the orange highlighted sections and sign the BLC / (P) SC declarations.

Although the form may be completed electronically and emailed to the ISAC, a hard copy with original signatures (not electronic) will also need to be posted to: Industry Security Assurance Centre, Poplar-1, MOD Abbey Wood, # 2004, Bristol, BS34 8JH.



Government Security

OFFICIAL-COMMERCIAL
(when complete)

Industry Security Assurance Centre
A Government Security Centre

Government Industry Security Assurance Form

(GISA Form)

Use this form for new applications, change of status, change of details and/or three-year assurance validation checks

Once complete please email to the Industry Security Assurance Centre (ISAC) (isac-group@mod.gov.uk) and post the hard copy with original signatures (not electronic) to: Industry Security Assurance Centre, Poplar -1 , MOD Abbey Wood, # 2004, Bristol, BS34 8JH

Contents

Version Information

1.0	First Release - April 2021 replacing previous Form 5B

OFFICIAL-COMMERCIAL (when complete)

Completing the GISA form

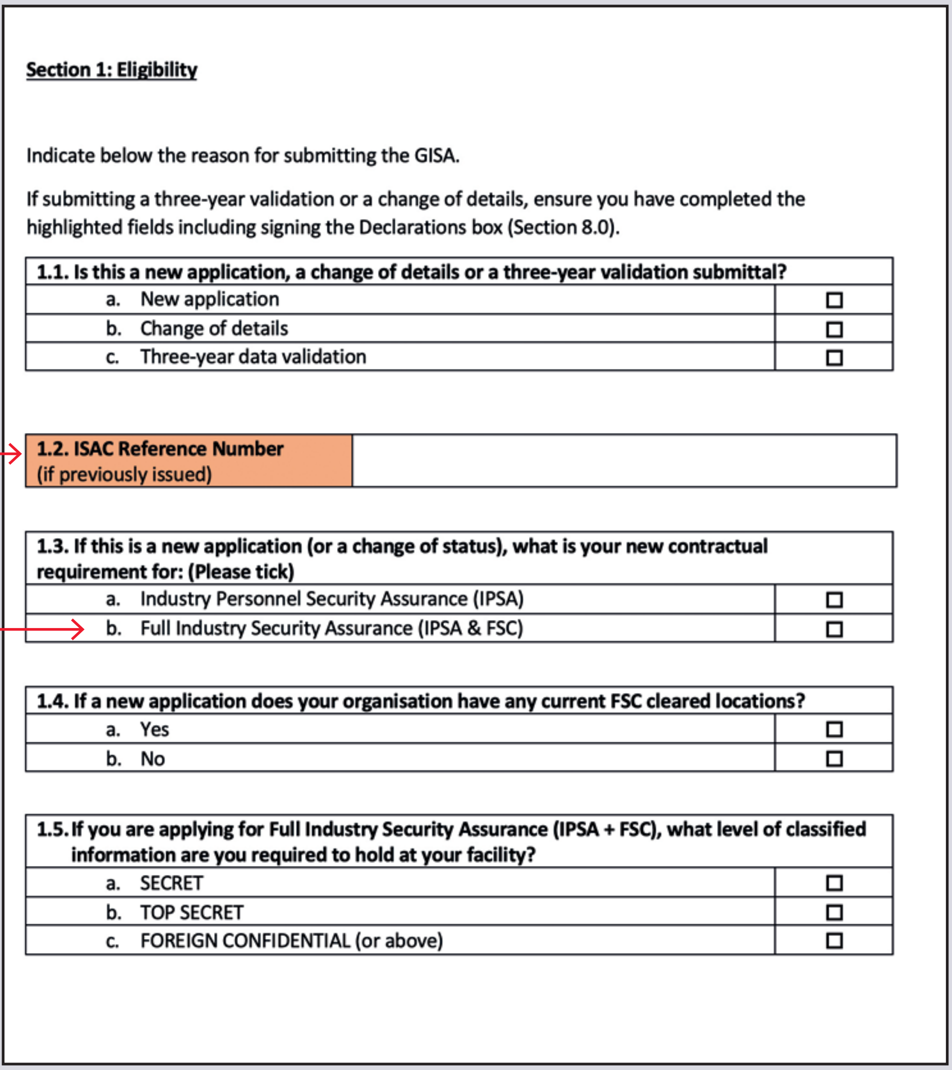
Each section of the form provides specific information that will enable the ISAC to understand your eligibility to undertake Industry Security Assurance and the background of your organisation. Once complete the form will be treated as OFFICIAL-COMMERCIAL and be protected accordingly. The information within this form will only be used for the processing of assurance activity and will not be shared with any agency not involved in that process.

Guidance on the information required for each section of the GISA is included within the form, however, these are some specific elements to be aware of.

Completing the GISA form – Section 1: Eligibility

The ISAC will provide you with a reference number during your assurance, please quote this on future correspondence. For current FSC holders, this will be your DE&S number

Full Industry Security Assurance (IPSA & FSC) will only be granted to organisations which have a contractual obligation to store classified material at their facility. If your contractual obligations only require you to sponsor NSV workers you should select Industry Personnel Security Assurance (IPSA).



Section 1: Eligibility

Indicate below the reason for submitting the GISA.

If submitting a three-year validation or a change of details, ensure you have completed the highlighted fields including signing the Declarations box (Section 8.0).

1.1. Is this a new application, a change of details or a three-year validation submittal?	
a. New application	□
b. Change of details	□
c. Three-year data validation	□

1.2. ISAC Reference Number (if previously issued)	

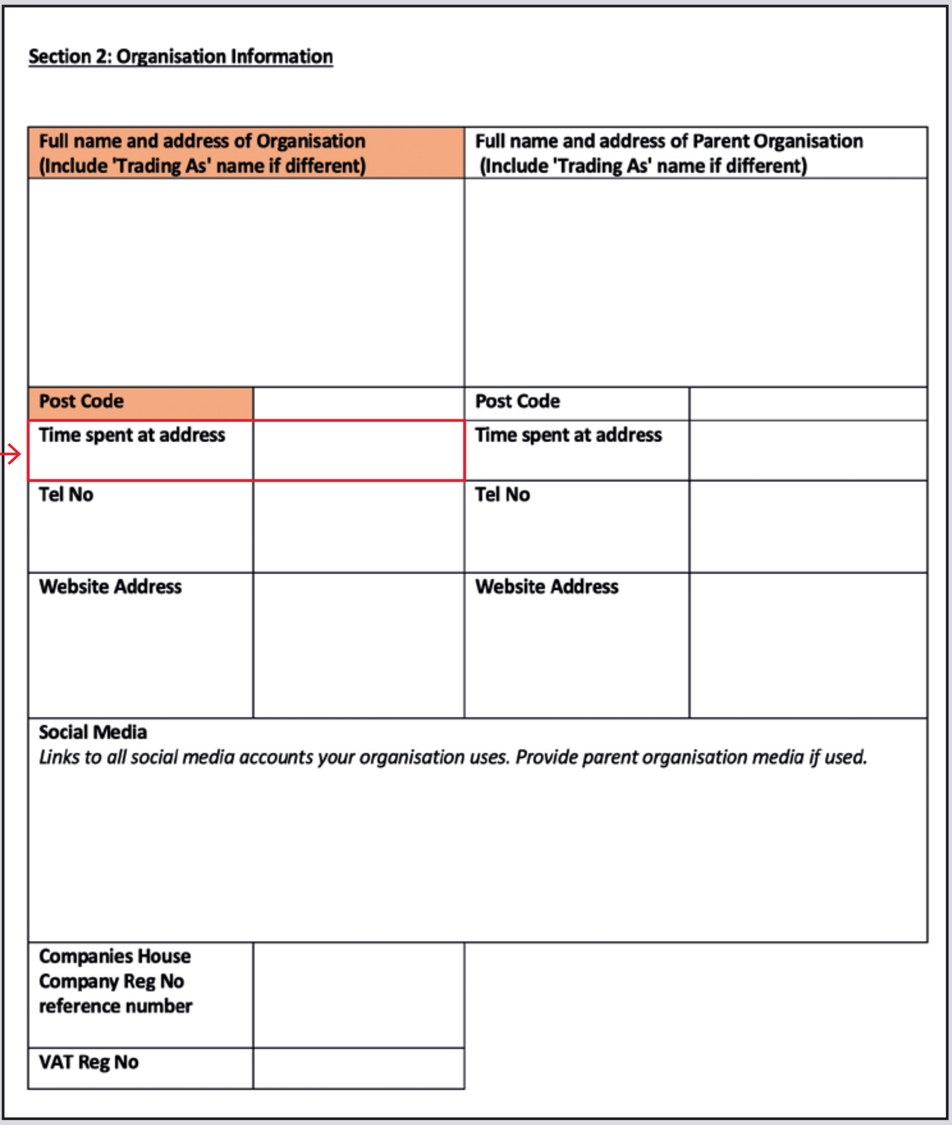
1.3. If this is a new application (or a change of status), what is your new contractual requirement for: (Please tick)	
a. Industry Personnel Security Assurance (IPSA)	□
b. Full Industry Security Assurance (IPSA & FSC)	□

1.4. If a new application does your organisation have any current FSC cleared locations?	
a. Yes	□
b. No	□

1.5. If you are applying for Full Industry Security Assurance (IPSA + FSC), what level of classified information are you required to hold at your facility?	
a. SECRET	□
b. TOP SECRET	□
c. FOREIGN CONFIDENTIAL (or above)	□

Completing the GISA form – Section 2: Organisation Information

Ensure you enter time spent at address, this will ensure company checks are processed quickly, especially where you have vacated old offices or recently taken up new ones from previous owners.



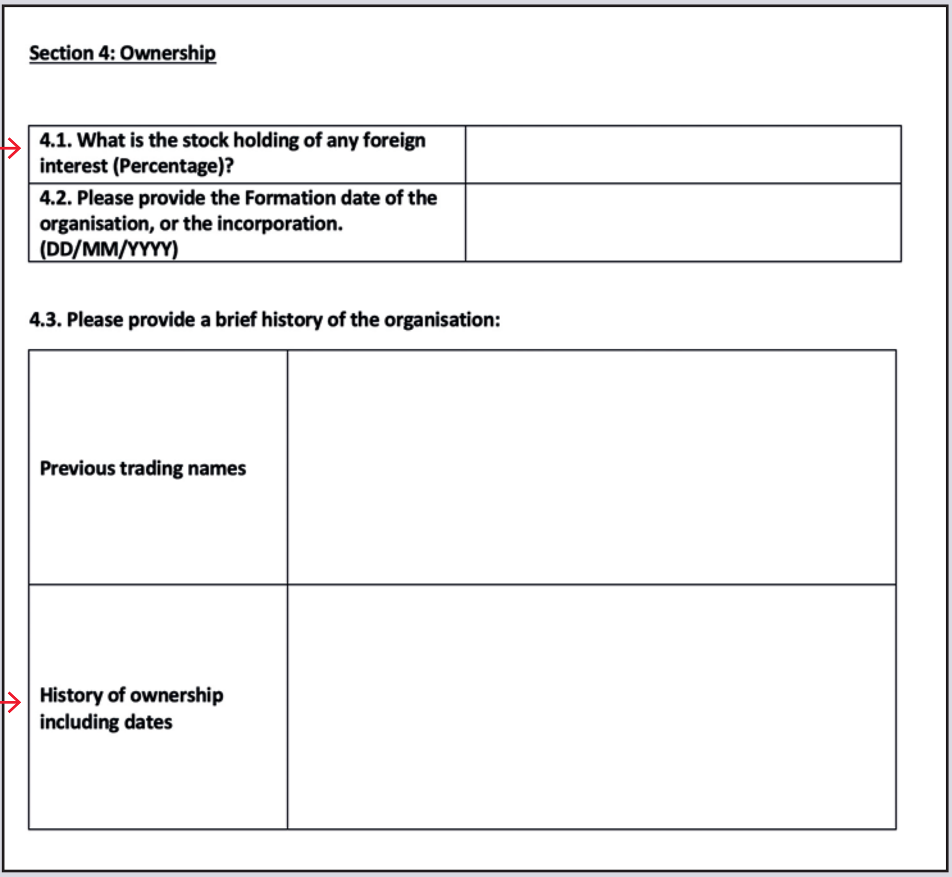
Section 2: Organisation Information

Full name and address of Organisation (Include 'Trading As' name if different)		**Full name and address of Parent Organisation (Include 'Trading As' name if different)**	
Post Code		**Post Code**	
Time spent at address		**Time spent at address**	
Tel No		**Tel No**	
Website Address		**Website Address**	
Social Media *Links to all social media accounts your organisation uses. Provide parent organisation media if used.*			
Companies House Company Reg No reference number			
VAT Reg No			

Completing the GISA form – Section 4: Ownership

Understanding who owns your organisation is important in enabling us to assess what level of control is held over those who have access to classified information.

Links to your organisation's history if hosted online may be provided.



Section 4: Ownership

4.1. What is the stock holding of any foreign interest (Percentage)?	
4.2. Please provide the Formation date of the organisation, or the incorporation. (DD/MM/YYYY)	

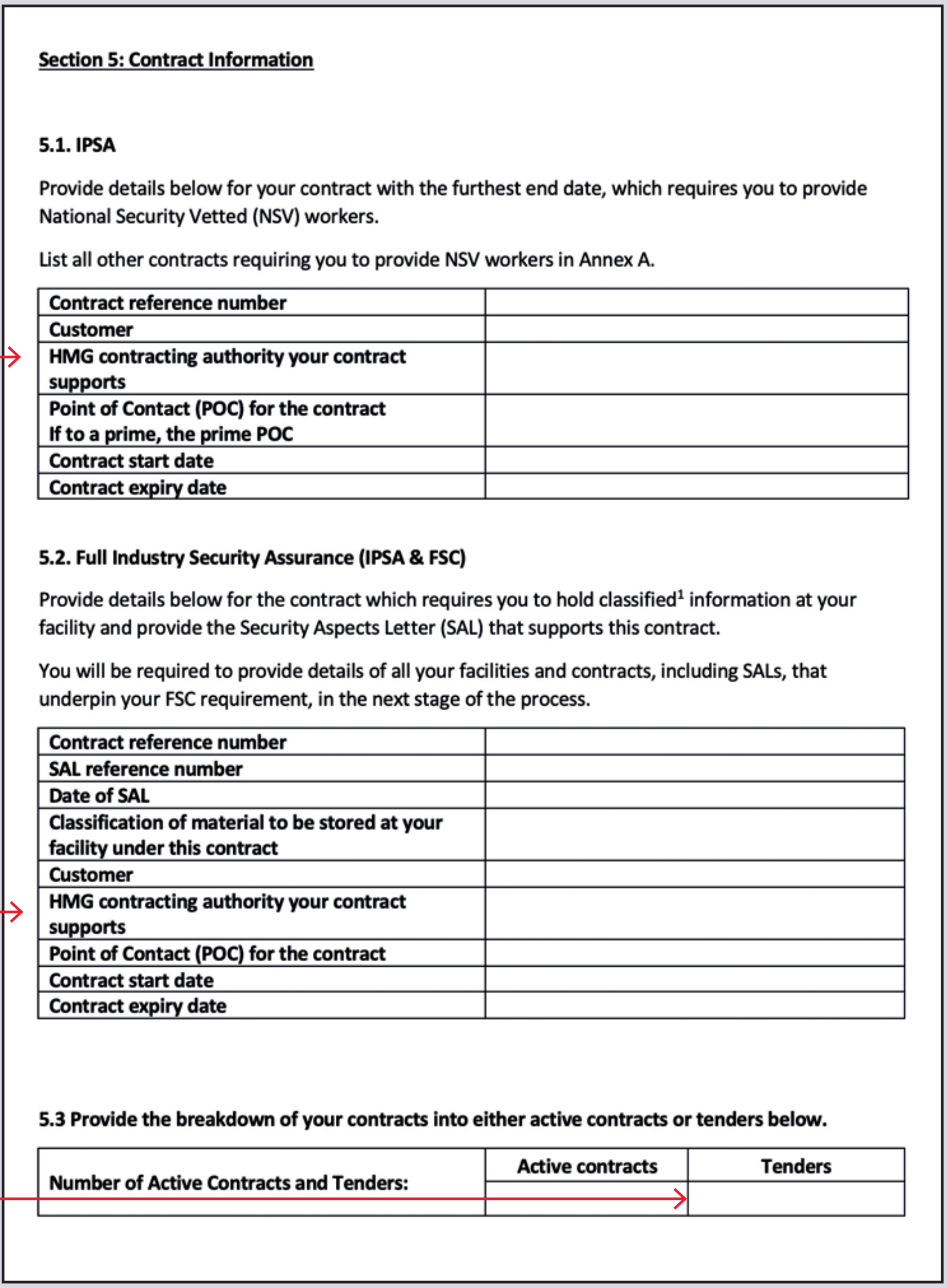
4.3. Please provide a brief history of the organisation:

Previous trading names	
History of ownership including dates	

Completing the GISA form – Section 5: Contract Information

You will need to provide the contract information which underpins your application to either IPSA or Full Industry Security Assurance, depending on which option you selected in question 1.3.

If you are applying for IPSA alone you will need to provide all contracts requiring you to provide NSV workers in Annex A of the GISA, to allow us to scope your requirement.



Section 5: Contract Information

5.1. IPSA

Provide details below for your contract with the furthest end date, which requires you to provide National Security Vetted (NSV) workers.

List all other contracts requiring you to provide NSV workers in Annex A.

Contract reference number	
Customer	
HMG contracting authority your contract supports	
Point of Contact (POC) for the contract **If to a prime, the prime POC**	
Contract start date	
Contract expiry date	

5.2. Full Industry Security Assurance (IPSA & FSC)

Provide details below for the contract which requires you to hold classified[1] information at your facility and provide the Security Aspects Letter (SAL) that supports this contract.

You will be required to provide details of all your facilities and contracts, including SALs, that underpin your FSC requirement, in the next stage of the process.

Contract reference number	
SAL reference number	
Date of SAL	
Classification of material to be stored at your facility under this contract	
Customer	
HMG contracting authority your contract supports	
Point of Contact (POC) for the contract	
Contract start date	
Contract expiry date	

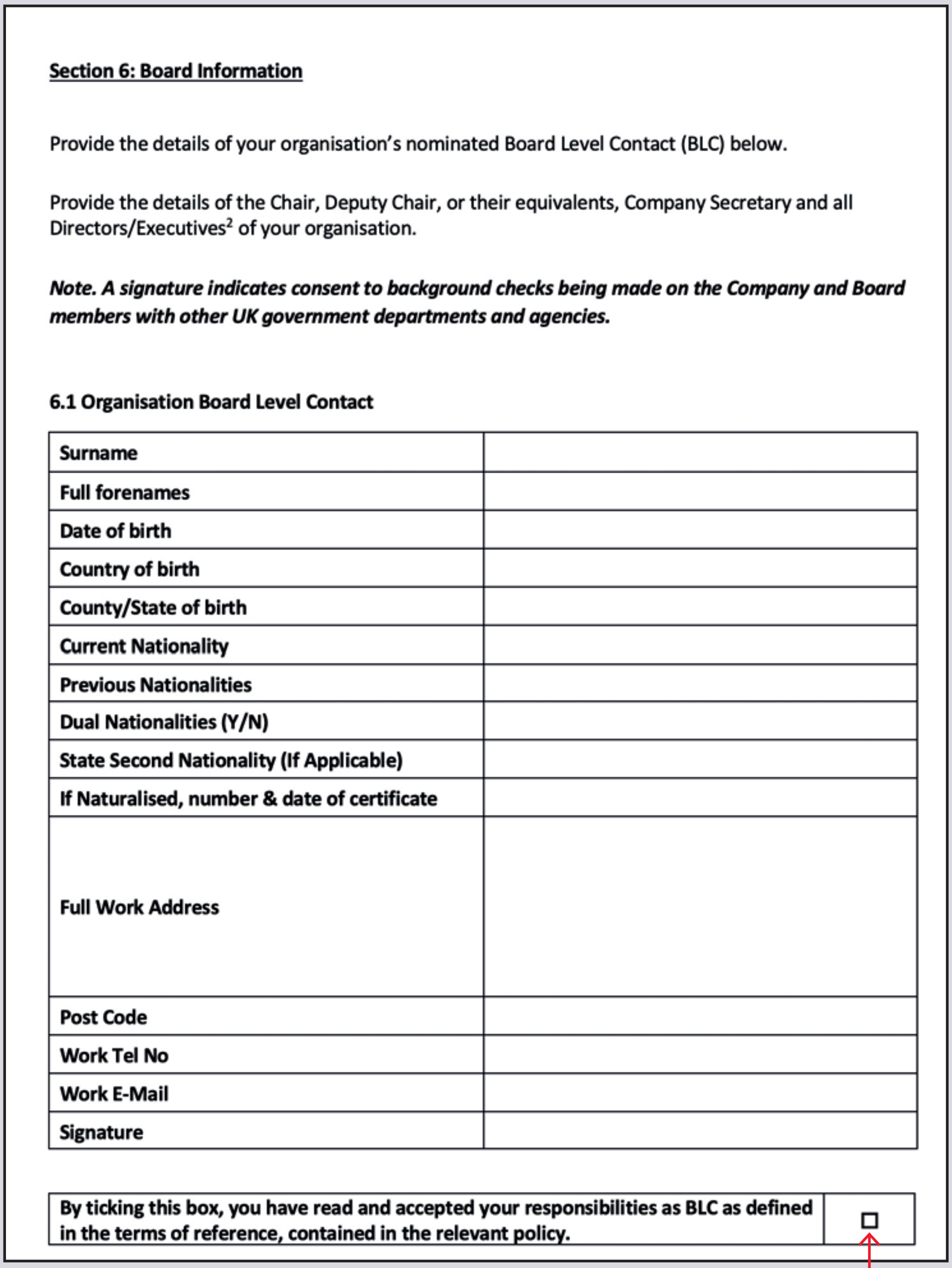
5.3 Provide the breakdown of your contracts into either active contracts or tenders below.

	Active contracts	**Tenders**
Number of Active Contracts and Tenders:		

For Prime Contractors, your customer and HMG Contracting Authority may be the same. For companies in the supply chain you may have a contract to supply a Prime, but we also need to know which Contracting Authority your Prime is supporting.

We do not need to know the details of your tenders, just the number you are engaged in versus the number of contracts you currently hold which require you to provide NSV workers. This is especially important as a tender may result in an increase to your requirement for NSV workers.

Completing the GISA form – Section 6: Board Information



Section 6: Board Information

Provide the details of your organisation's nominated Board Level Contact (BLC) below.

Provide the details of the Chair, Deputy Chair, or their equivalents, Company Secretary and all Directors/Executives[2] of your organisation.

Note. A signature indicates consent to background checks being made on the Company and Board members with other UK government departments and agencies.

6.1 Organisation Board Level Contact

Surname	
Full forenames	
Date of birth	
Country of birth	
County/State of birth	
Current Nationality	
Previous Nationalities	
Dual Nationalities (Y/N)	
State Second Nationality (If Applicable)	
If Naturalised, number & date of certificate	
Full Work Address	
Post Code	
Work Tel No	
Work E-Mail	
Signature	

By ticking this box, you have read and accepted your responsibilities as BLC as defined in the terms of reference, contained in the relevant policy.	□

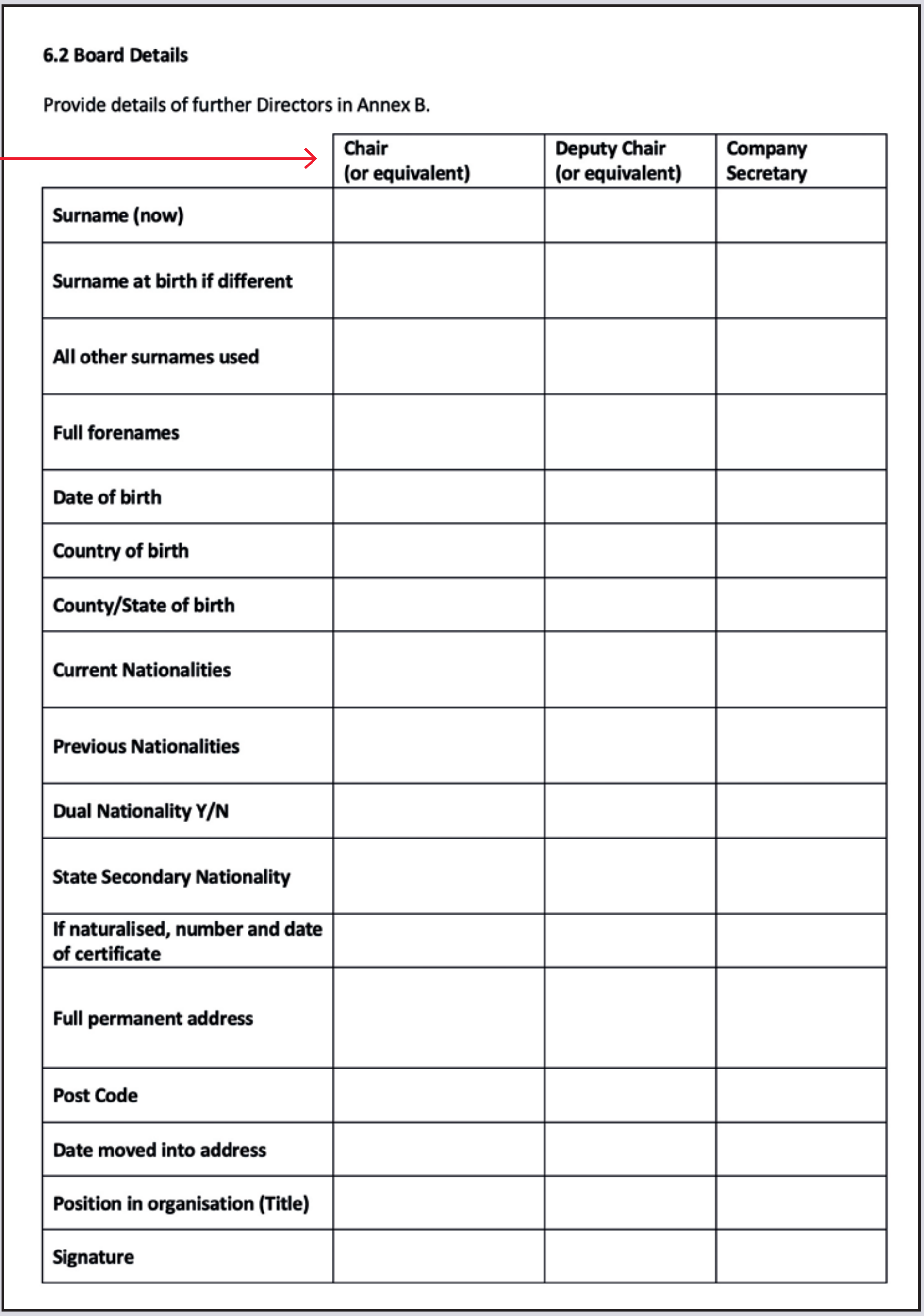
The BLC responsibilities are set out in the Terms of Reference, contained within the relevant policy. These will need to be accepted by ticking this box.

Completing the GISA form – Section 6.2: Board Details

The term “Director” applies to any Director of the Board of the Company that has voting or decision-making rights irrespective of whether the individual is in an executive position or not.

Information should be provided for all individuals holding more than one fifth of paid up shares, preference shares or loan using Annex B of the GISA.

Whilst Chair and Deputy Chair are recognised positions within government security policy, your organisation may not use these titles, in which case please include your equivalent.



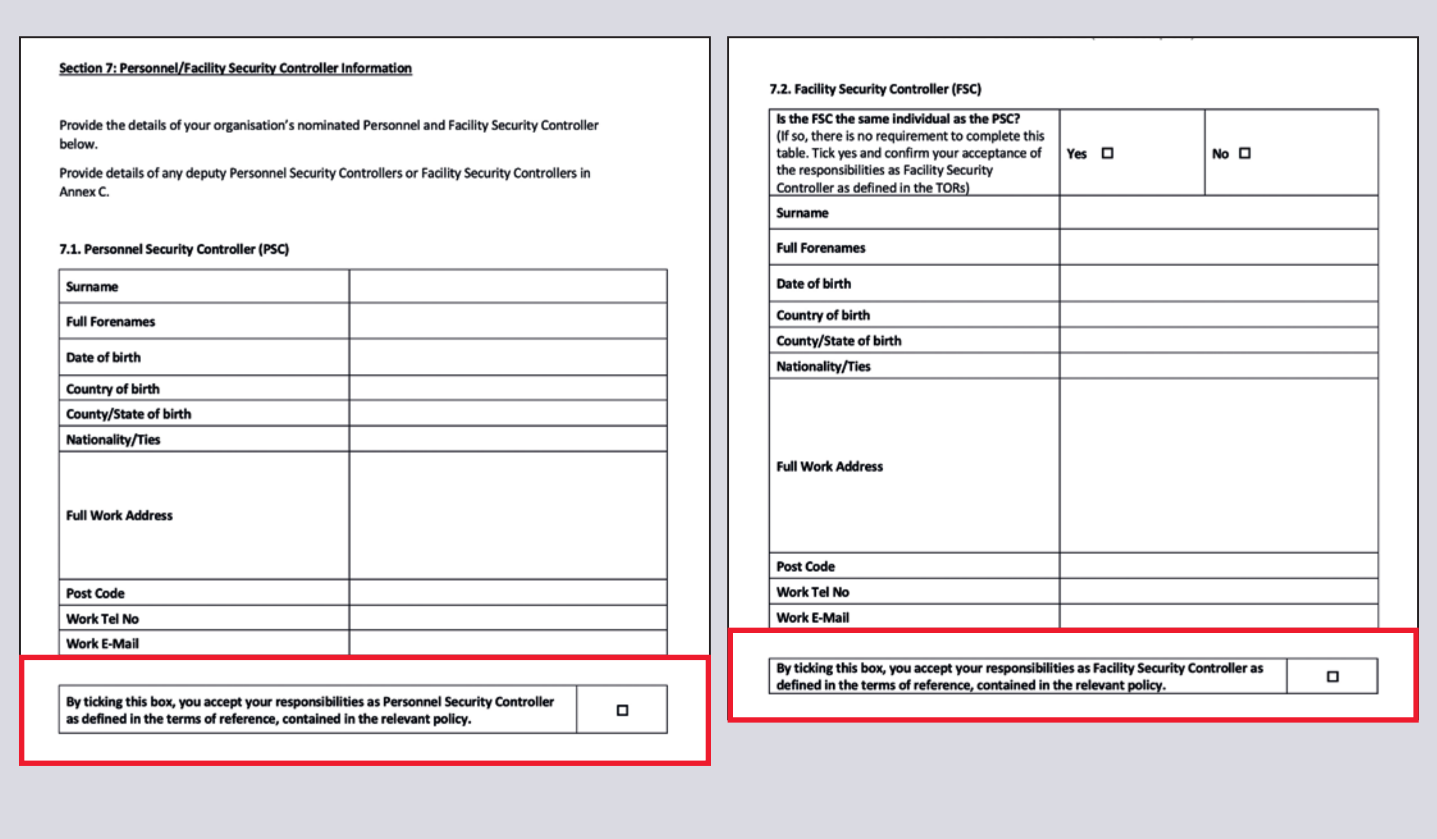
6.2 Board Details

Provide details of further Directors in Annex B.

	Chair (or equivalent)	Deputy Chair (or equivalent)	Company Secretary
Surname (now)			
Surname at birth if different			
All other surnames used			
Full forenames			
Date of birth			
Country of birth			
County/State of birth			
Current Nationalities			
Previous Nationalities			
Dual Nationality Y/N			
State Secondary Nationality			
If naturalised, number and date of certificate			
Full permanent address			
Post Code			
Date moved into address			
Position in organisation (Title)			
Signature			

Completing the GISA form – Section 7: Personnel/Facility Controller Information

There is no requirement for your personnel and facility security controller positions to be filled by separate individuals. As long as the Terms of Reference for both roles are accepted, they can be fulfilled by the same person. The Terms of Reference for each role can be found in the relevant policy.



Section 7: Personnel/Facility Security Controller Information

Provide the details of your organisation's nominated Personnel and Facility Security Controller below.

Provide details of any deputy Personnel Security Controllers or Facility Security Controllers in Annex C.

7.1. Personnel Security Controller (PSC)

Surname	
Full Forenames	
Date of birth	
Country of birth	
County/State of birth	
Nationality/Ties	
Full Work Address	
Post Code	
Work Tel No	
Work E-Mail	

By ticking this box, you accept your responsibilities as Personnel Security Controller as defined in the terms of reference, contained in the relevant policy.	□

7.2. Facility Security Controller (FSC)

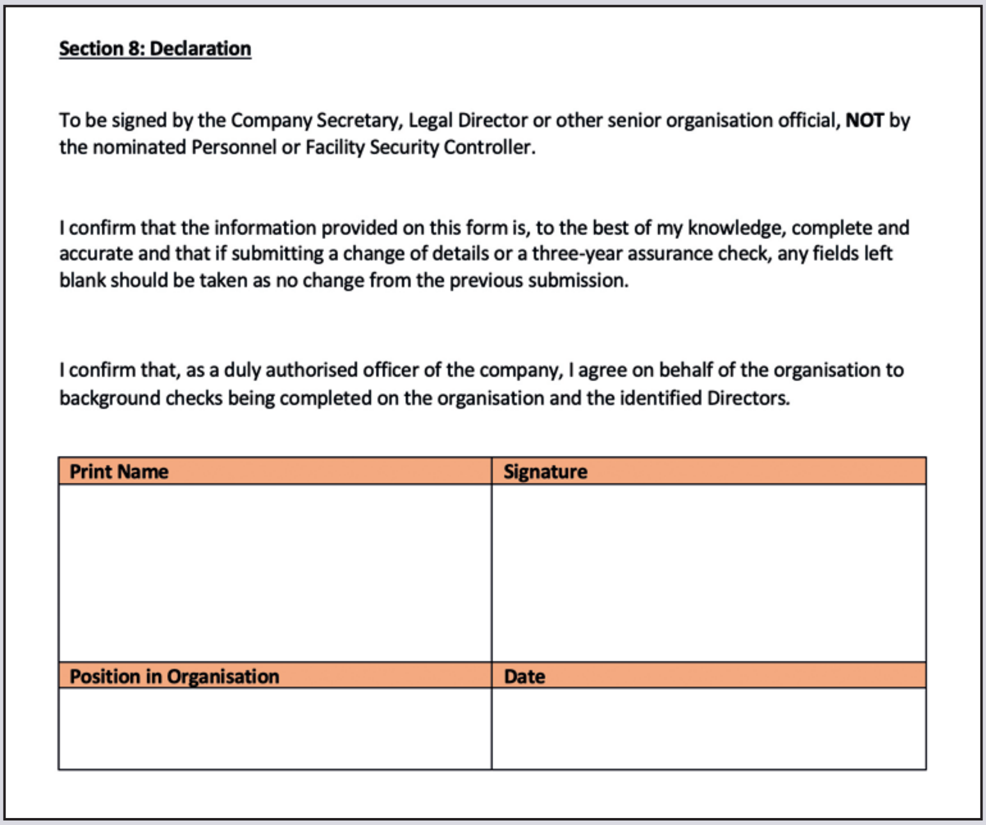
Is the FSC the same individual as the PSC? (If so, there is no requirement to complete this table. Tick yes and confirm your acceptance of the responsibilities as Facility Security Controller as defined in the TORs)	**Yes** □	**No** □
Surname		
Full Forenames		
Date of birth		
Country of birth		
County/State of birth		
Nationality/Ties		
Full Work Address		
Post Code		
Work Tel No		
Work E-Mail		

By ticking this box, you accept your responsibilities as Facility Security Controller as defined in the terms of reference, contained in the relevant policy.	□

Completing the GISA form – Section 8: Declaration

The declaration will need to be made each time the form is submitted.

It is important that this is signed by an office holder and not by the Personnel or Facility Security Controller.



Section 8: Declaration

To be signed by the Company Secretary, Legal Director or other senior organisation official, **NOT** by the nominated Personnel or Facility Security Controller.

I confirm that the information provided on this form is, to the best of my knowledge, complete and accurate and that if submitting a change of details or a three-year assurance check, any fields left blank should be taken as no change from the previous submission.

I confirm that, as a duly authorised officer of the company, I agree on behalf of the organisation to background checks being completed on the organisation and the identified Directors.

Print Name	**Signature**
Position in Organisation	**Date**

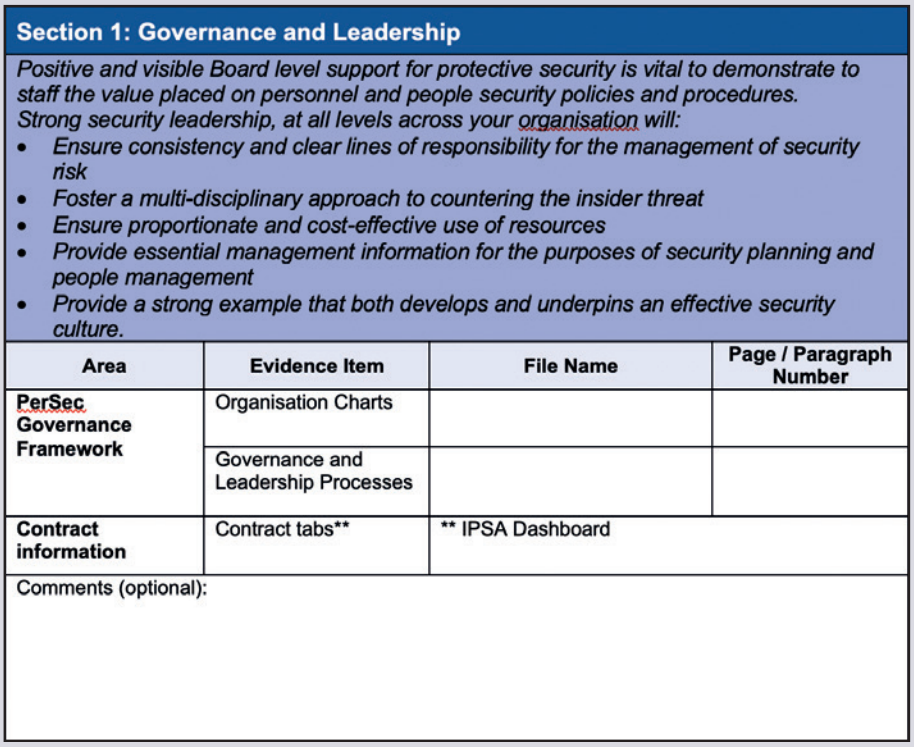
IPSA Evidence Cover Sheet

The objective of this sheet is to support the submission of the evidence required for Industry Personnel Security Assurance. Once completed, it serves as a summary of all evidence artefacts that are submitted to the ISAC for assurance.

The sheet has been split into sections that are aligned with CPNI's 7 core pillars of security and the standards detailed in the IPSA Personnel Reliability Framework. Within each section is a list of the evidence required for that particular area.

Section i.e CPNI pillar

List of evidence required



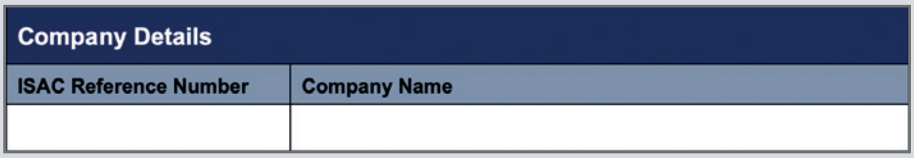
Section 1: Governance and Leadership

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.*

Area	Evidence Item	File Name	Page / Paragraph Number
PerSec Governance Framework	Organisation Charts		
	Governance and Leadership Processes		
Contract information	Contract tabs**	** IPSA Dashboard	
Comments (optional):			

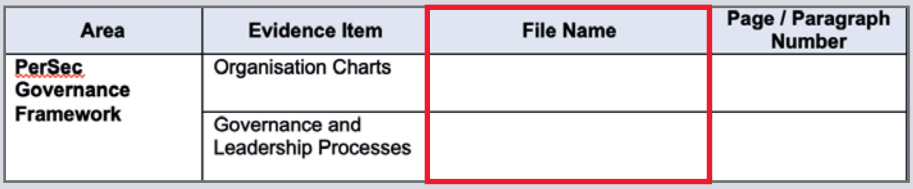
Before completing the cover sheet, be sure to capture your company name and unique ISAC reference number (if you have been assigned one). For organisations with an existing FSC this will be your DE&S reference number.



Company Details

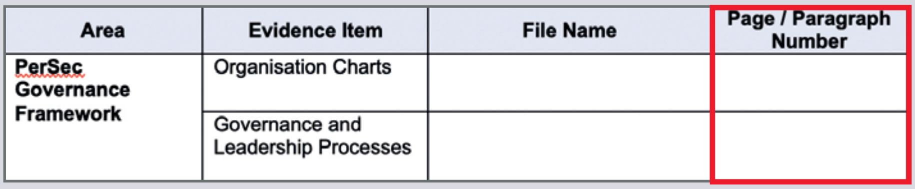
ISAC Reference Number	Company Name

For each of the evidence items listed in this guide and on the cover sheet, provide your evidence and capture the file name of each document clearly alongside the appropriate evidence item on the form, inserting additional rows as required



Area	Evidence Item	File Name	Page / Paragraph Number
PerSec Governance Framework	Organisation Charts		
	Governance and Leadership Processes		

Where the evidence requested is embedded within a document please also capture the page number and paragraph where it can be found.



Area	Evidence Item	File Name	Page / Paragraph Number
PerSec Governance Framework	Organisation Charts		
	Governance and Leadership Processes		

There is an area available within each section for you to provide any additional comments related to that section. There is also a space available at the end of the form to provide comments related to your overall submission. Please note that providing this additional commentary is optional.

When submitting your evidence, do NOT provide us with:

- Any information on how business / commercial decisions are made.
- Proprietary Board information and outcomes, including decisions or detailed meeting minutes.
- Detailed, live records held in registers / databases, such as risks, incidents or NSV holders.
- Information relating to individuals (other than those requested in the GISA form)

The Dashboard

The IPSA dashboard is how you will capture data 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.

You will capture the outputs of the Vetting Register (including aftercare data) for you and your network of clearance holders. This includes information on the outputs of the Incident Log, contracts that require NSV, as well as Insider Threat / Personnel Security risk register review.

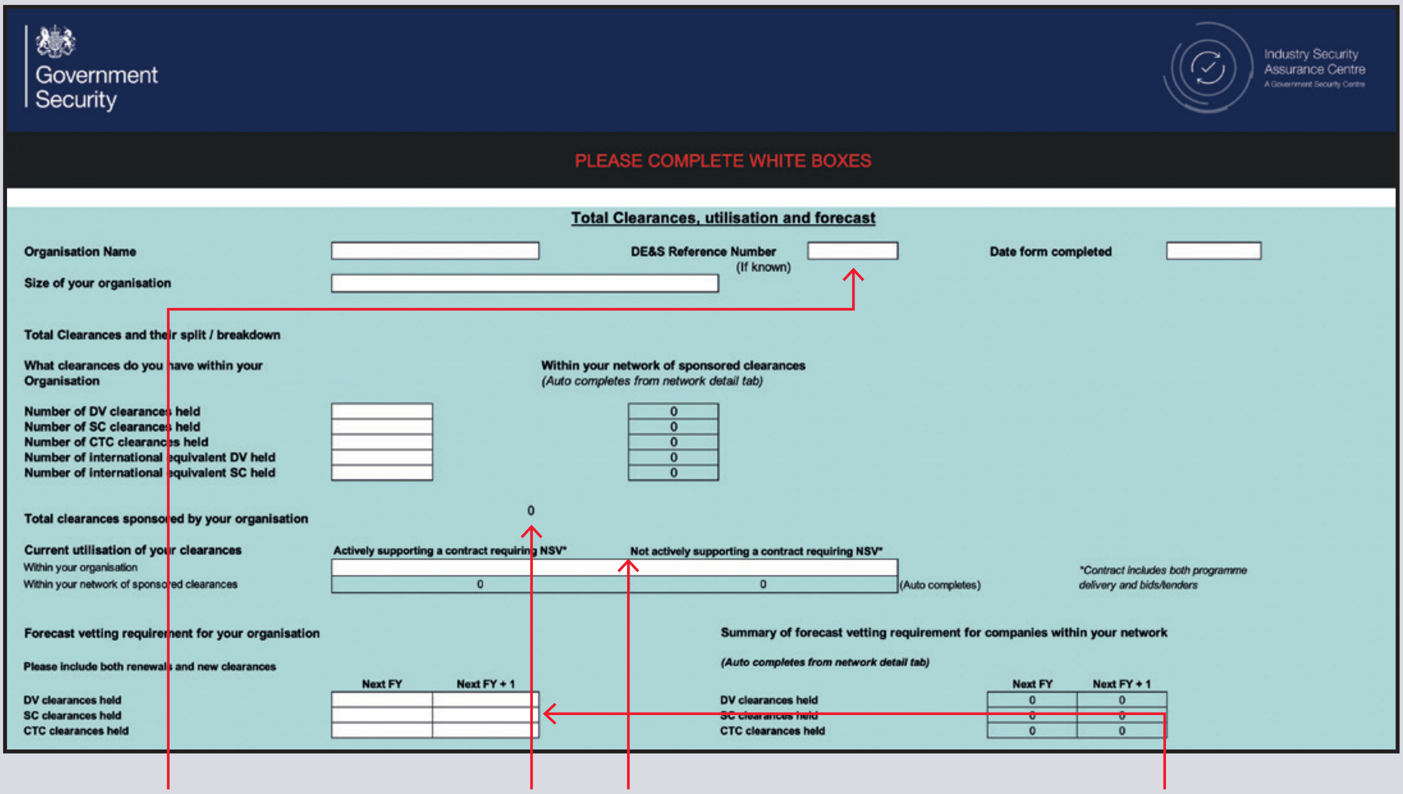
Further information on how each strand is evidenced through the dashboard can be found in the relevant pages in the standards part of this document.

The dashboard is submitted at accreditation and annually thereafter, normally by the end of November. If this is the first time you are completing the IPSA Dashboard your reporting period will be the previous twelve months from the date you completed the form. Note that not all sections of the dashboard need to be completed at accreditation.

Overview

This section captures general information about your organisation, the date you completed the form as well as the number of clearances held within your organisation. You will also record the number of NSV individuals within your organisation that are actively engaged in supporting a contract that requires cleared staff, as well as the number of NSV individuals that are between contracts or working on contracts that don't require cleared staff.

Please only complete the sections in white. The dashboard will automatically populate this information for your network of sponsored clearances once you have completed the network tab.


Government Security
Industry Security Assurance Centre
A Government Security Centre

PLEASE COMPLETE WHITE BOXES

Total Clearances, utilisation and forecast

Organisation Name □ DE&S Reference Number (If known) □ Date form completed □

Size of your organisation □

Total Clearances and their split / breakdown

What clearances do you have within your Organisation		Within your network of sponsored clearances (Auto completes from network detail tab)
Number of DV clearances held		0
Number of SC clearances held		0
Number of CTC clearances held		0
Number of international equivalent DV held		0
Number of international equivalent SC held		0

Total clearances sponsored by your organisation 0

Current utilisation of your clearances	Actively supporting a contract requiring NSV*	Not actively supporting a contract requiring NSV*	
Within your organisation			
Within your network of sponsored clearances	0	0	(Auto completes)

*Contract includes both programme delivery and bids/tenders

Forecast vetting requirement for your organisation

Please include both renewals and new clearances

	Next FY	Next FY + 1
DV clearances held		
SC clearances held		
CTC clearances held		

Summary of forecast vetting requirement for companies within your network

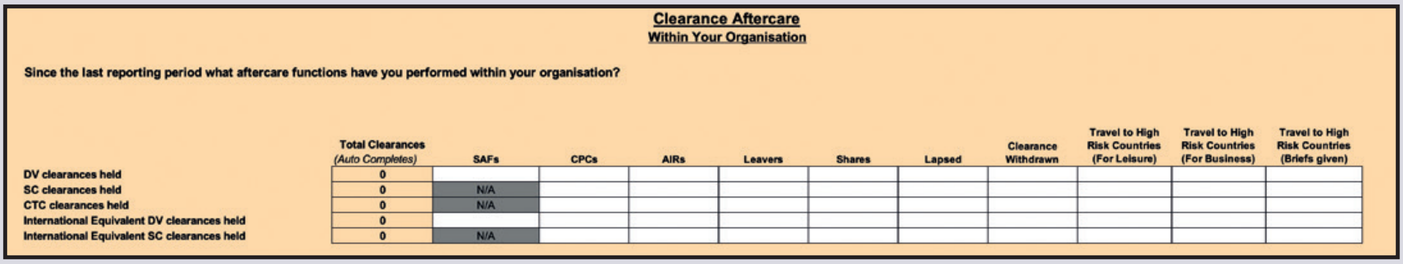
(Auto completes from network detail tab)

	Next FY	Next FY + 1
DV clearances held	0	0
SC clearances held	0	0
CTC clearances held	0	0

The ISAC will provide you with a reference number during your assurance, please quote this on future correspondence. For current FSC holders, this will be your DE&S number.

Ensure your utilisation table tallies with the total clearances you are sponsoring within your organisation.

The projection of new clearance applications and / or renewals that you anticipate undertaking in the forecast period indicated. Your forecast should be reflective of the clearances required to conduct your business in support of HMG contracts over the next two financial years. Large deviations between forecast and actual figures may require further investigation.



Clearance Aftercare
Within Your Organisation

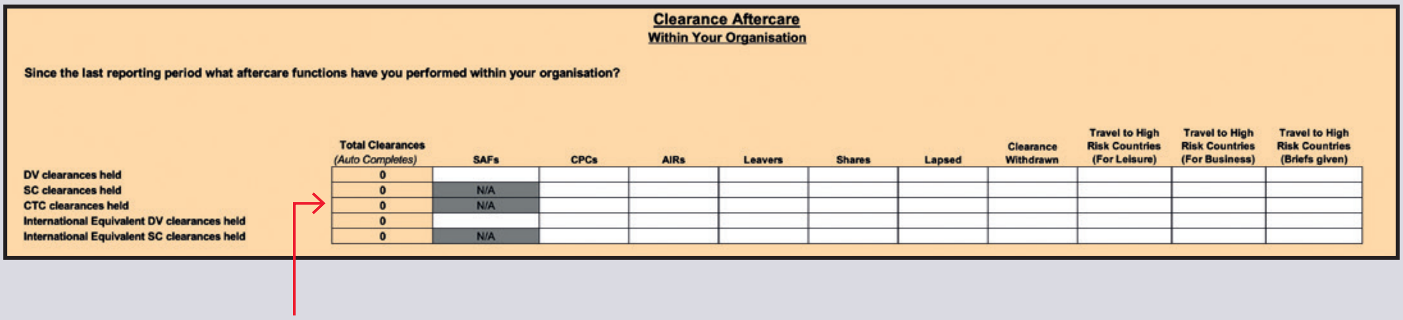
Since the last reporting period what aftercare functions have you performed within your organisation?

	Total Clearances *(Auto Completes)*	SAFs	CPCs	AIRs	Leavers	Shares	Lapsed	Clearance Withdrawn	Travel to High Risk Countries (For Leisure)	Travel to High Risk Countries (For Business)	Travel to High Risk Countries (Briefs given)
DV clearances held	0										
SC clearances held	0	N/A									
CTC clearances held	0	N/A									
International Equivalent DV clearances held	0										
International Equivalent SC clearances held	0	N/A									

You should capture the aftercare information that has been submitted on behalf of your organisation during the reporting period. This includes the amount of travel to “high threat” countries, a list of which will be provided to you following accreditation.

Please capture this information to the best of your ability, though it is understood that some information (such as changes in personal circumstances) may have been reported directly to UKSV by the vetted individual.

You should capture aftercare information that has been submitted on behalf of your network separately.



Clearance Aftercare
Within Your Organisation

Since the last reporting period what aftercare functions have you performed within your organisation?

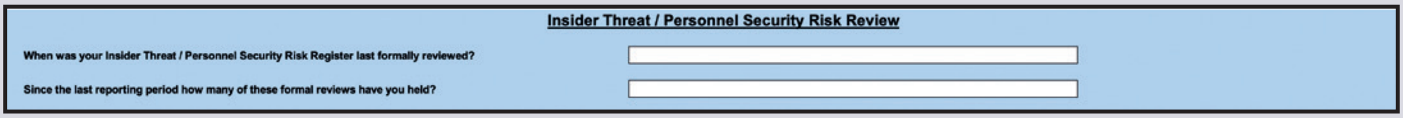
	Total Clearances *(Auto Completes)*	SAFs	CPCs	AIRs	Leavers	Shares	Lapsed	Clearance Withdrawn	Travel to High Risk Countries (For Leisure)	Travel to High Risk Countries (For Business)	Travel to High Risk Countries (Briefs given)
DV clearances held	0										
SC clearances held	0	N/A									
CTC clearances held	0	N/A									
International Equivalent DV clearances held	0										
International Equivalent SC clearances held	0	N/A									

Note: Total Clearances will be auto populated once you have completed the network detail tab.

!

There is no requirement to complete the Aftercare section of the dashboard at initial accreditation.

To ensure that your insider threat / personnel security risks are being regularly reviewed and managed, please capture the date that your register was last formally reviewed as well as the number of formal reviews you've held since you last completed the dashboard.

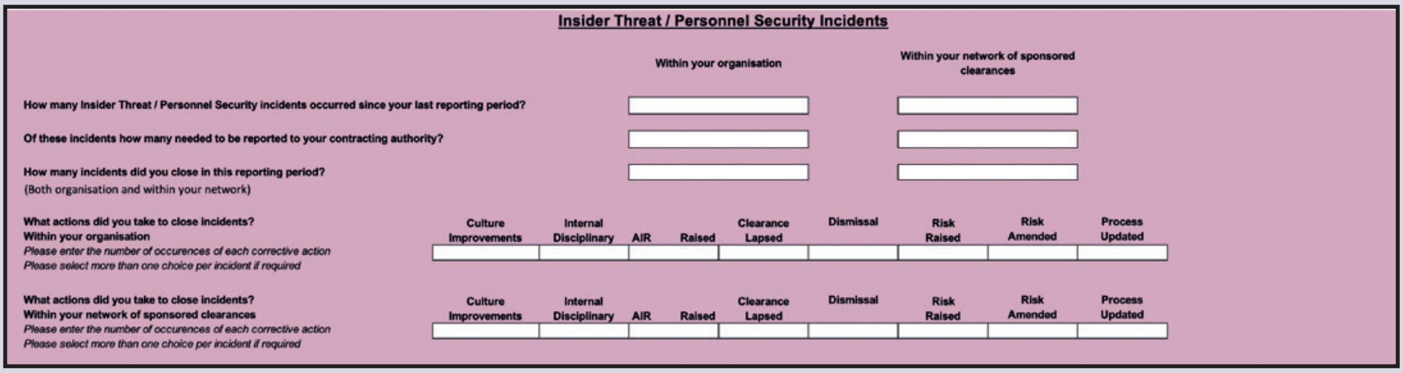


Insider Threat / Personnel Security Risk Review

When was your Insider Threat / Personnel Security Risk Register last formally reviewed?	
Since the last reporting period how many of these formal reviews have you held?	

Please provide the outputs of the insider threat / personnel security incident management processes for you and your network.

This includes information on the number of incidents that occurred during the reporting period, how many of these incidents needed to be reported to the relevant contracting authority, how many incidents were closed and what actions were taken to close them.

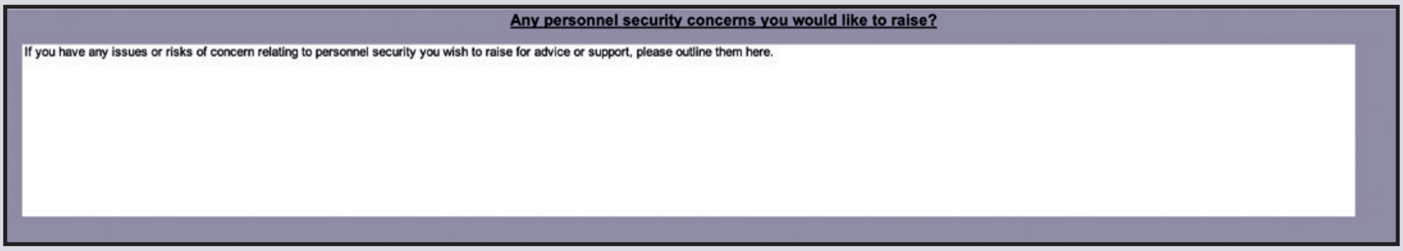


Insider Threat / Personnel Security Incidents

	Within your organisation	Within your network of sponsored clearances
How many Insider Threat / Personnel Security incidents occurred since your last reporting period?		
Of these incidents how many needed to be reported to your contracting authority?		
How many incidents did you close in this reporting period? (Both organisation and within your network)		

	Culture Improvements	Internal Disciplinary	AIR Raised	Clearance Lapsed	Dismissal	Risk Raised	Risk Amended	Process Updated
What actions did you take to close incidents? Within your organisation *Please enter the number of occurences of each corrective action* *Please select more than one choice per incident if required*								
What actions did you take to close incidents? Within your network of sponsored clearances *Please enter the number of occurences of each corrective action* *Please select more than one choice per incident if required*								

You have the opportunity to record any other specific personnel security concerns you would like to raise, ensuring that the security classification of the document is observed. Specifics can be discussed with your assessor. Please list concerns rather than wait for your ISAC assessor to identify them during your assessment as listing them demonstrates known action areas have been identified.



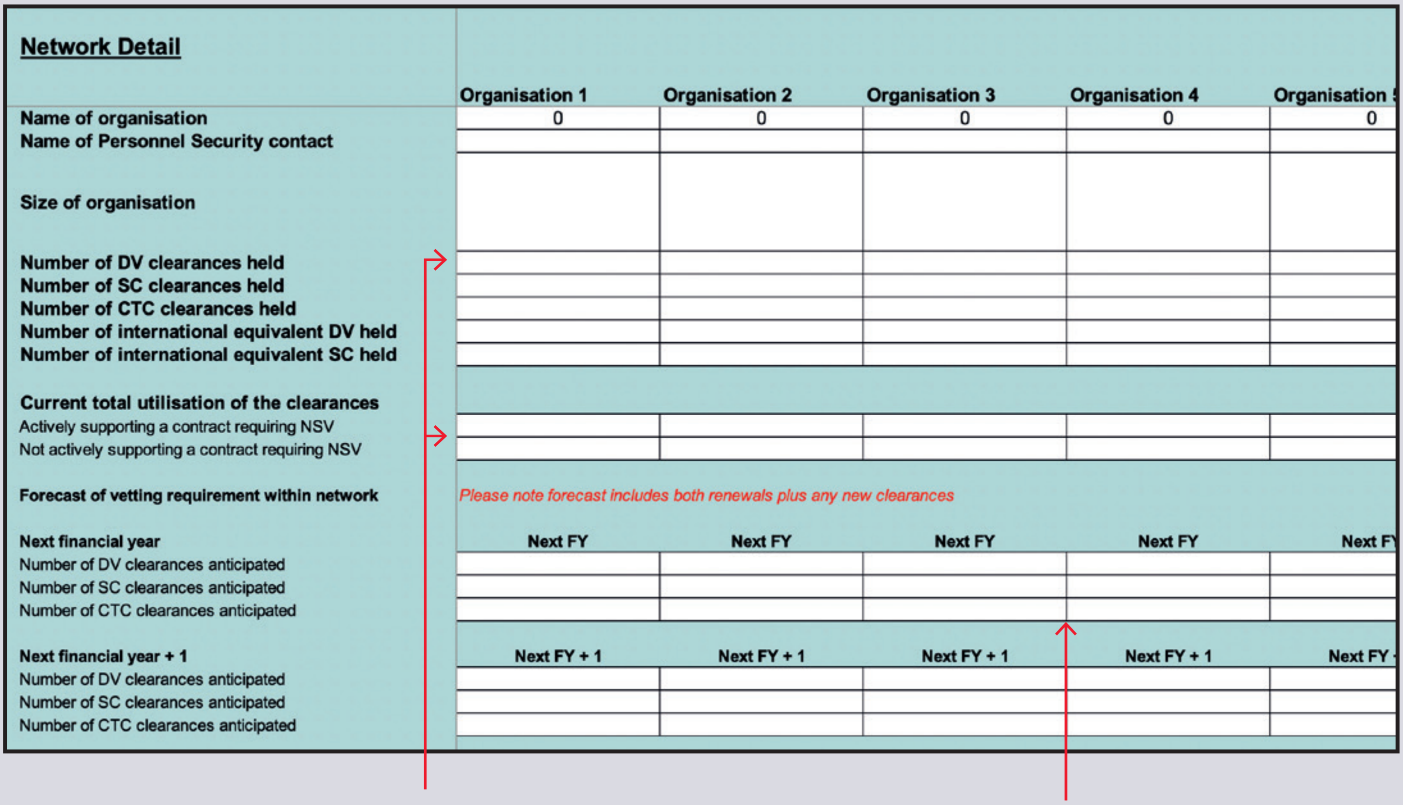
Any personnel security concerns you would like to raise?

If you have any issues or risks of concern relating to personnel security you wish to raise for advice or support, please outline them here.

Network Detail

In this section, please capture the overview, clearance and forecast information for each organisation in your network. Clearance and forecast information is only required for clearances that your organisation has sponsored / will sponsor, please do not include any information on clearances held by a different sponsor.

There is space for 50 organisations, if data for additional organisations needs to be captured then insert more columns by clicking on column.



Network Detail

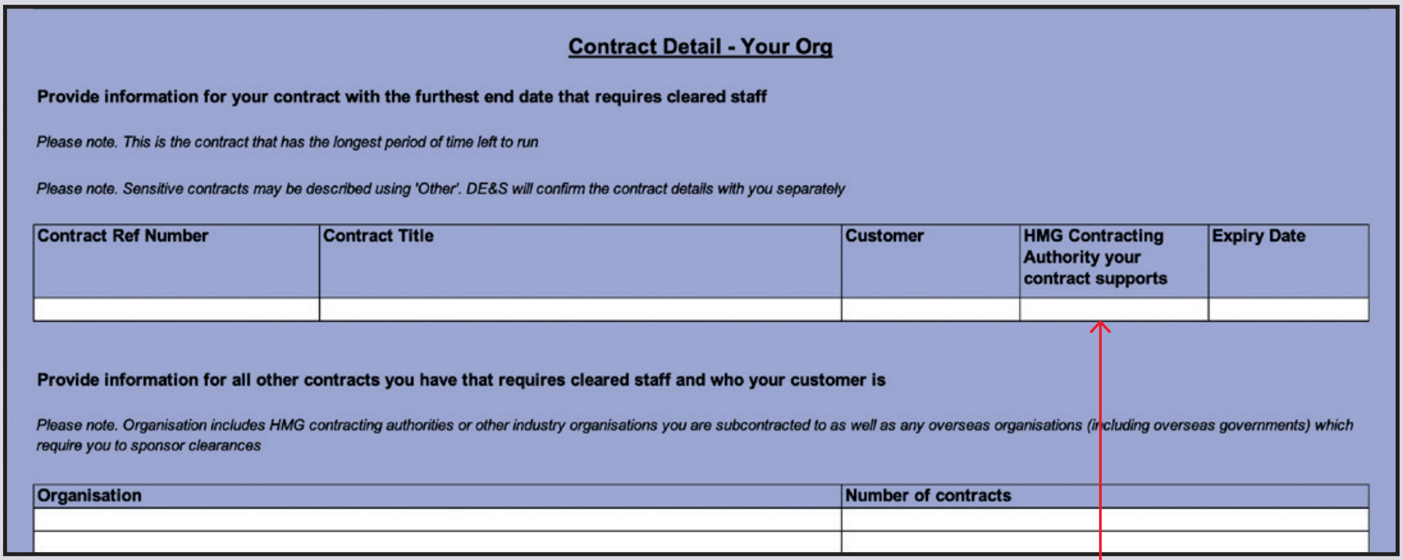
	Organisation 1	Organisation 2	Organisation 3	Organisation 4	Organisation
Name of organisation	0	0	0	0	0
Name of Personnel Security contact					
Size of organisation					
Number of DV clearances held					
Number of SC clearances held					
Number of CTC clearances held					
Number of international equivalent DV held					
Number of international equivalent SC held					
Current total utilisation of the clearances					
Actively supporting a contract requiring NSV					
Not actively supporting a contract requiring NSV					
Forecast of vetting requirement within network	*Please note forecast includes both renewals plus any new clearances*				
Next financial year	**Next FY**	**Next FY**	**Next FY**	**Next FY**	**Next F**
Number of DV clearances anticipated					
Number of SC clearances anticipated					
Number of CTC clearances anticipated					
Next financial year + 1	**Next FY + 1**	**Next FY + 1**	**Next FY + 1**	**Next FY + 1**	**Next FY**
Number of DV clearances anticipated					
Number of SC clearances anticipated					
Number of CTC clearances anticipated					

Ensure that the total utilisation of clearances matches the total number of clearances you are sponsoring for each organisation.

The projection of new clearance applications and / or renewals that you anticipate undertaking for organisations within your network in the forecast period indicated. Your forecast should be reflective of the clearances required to conduct each organisation's business in support of HMG contracts over the next two financial years. Large deviations between forecast and actual figures may require further investigation.

Contract Summary (Your Org)

In order for us to understand how long you anticipate conducting vetting sponsorship, provide the details of the contract with the furthest end date that requires you to provide NSV staff (i.e. the contract that has the longest period of time left to run), as well as the Contracting Authority linked to that contract.



Contract Detail - Your Org

Provide information for your contract with the furthest end date that requires cleared staff

Please note. This is the contract that has the longest period of time left to run

Please note. Sensitive contracts may be described using 'Other'. DE&S will confirm the contract details with you separately

Contract Ref Number	Contract Title	Customer	HMG Contracting Authority your contract supports	Expiry Date

Provide information for all other contracts you have that requires cleared staff and who your customer is

Please note. Organisation includes HMG contracting authorities or other industry organisations you are subcontracted to as well as any overseas organisations (including overseas governments) which require you to sponsor clearances

Organisation	Number of contracts

For Prime Contractors, your customer and HMG Contracting Authority may be the same. For companies in the supply chain you may have a contract to supply a Prime, but we also need to know which Contracting Authority your Prime is supporting.

In addition to your longest running contract, provide a list of the organisations that you have contracts with that require you to provide NSV staff. This includes:

- Government Departments
- Other industry organisations that you are sub-contracted to
- Overseas organisations (including overseas Governments).

You only need to list each organisation once and include how many contracts you have with each.

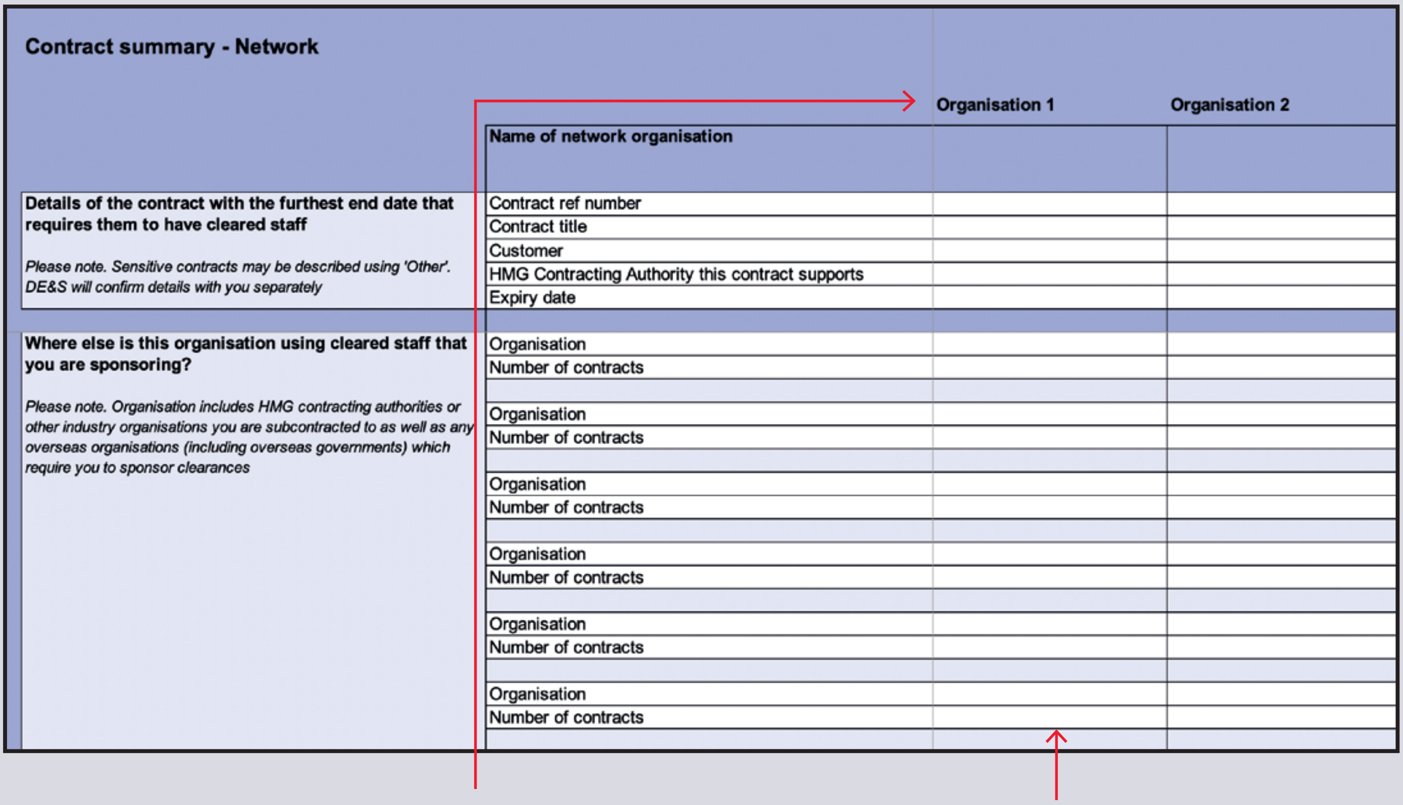
There is space for 50 organisations. If you need more, please enter new rows.

This contract summary in the dashboard is different from the detailed contract information you will provide in the Government Industry Security Assurance Form (GISA) on initial application or when reporting changes to the ISAC.

This detailed information (and Security Aspect Letters where applicable) is required to verify the full justification for undertaking IPSA or full Industry Security Assurance and should only be required once (or when there are changes).

Contract Summary (Your Network)

In order to understand vetting requirements within your network it is also essential that you provide a separate summary of the contracts they hold that requires them to provide NSV staff. You should split this in the same way as the information provided for your organisation, listing the contract with the furthest end date followed by a summary of each organisation each member of your network is contracted to and how many contracts they have.



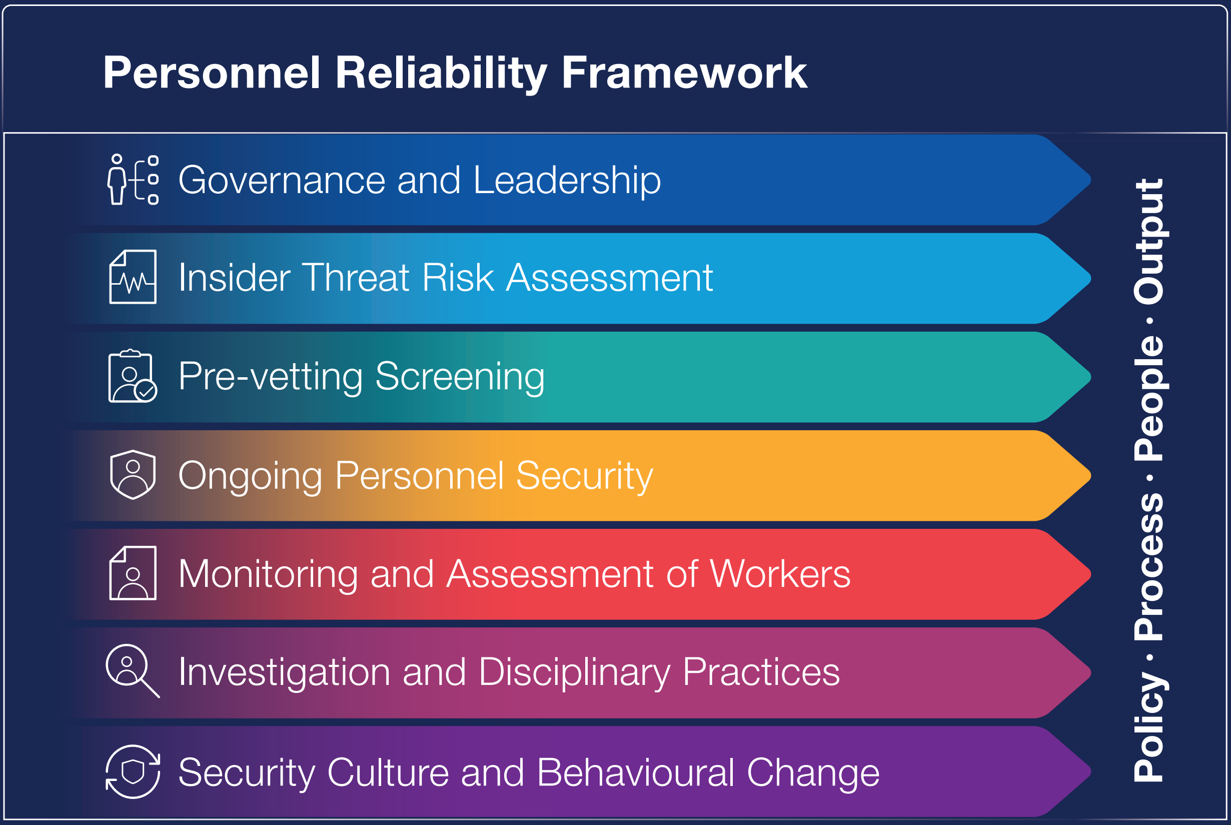
Contract summary - Network

		Organisation 1	Organisation 2
	Name of network organisation		
Details of the contract with the furthest end date that requires them to have cleared staff *Please note. Sensitive contracts may be described using 'Other'. DE&S will confirm details with you separately*	Contract ref number		
	Contract title		
	Customer		
	HMG Contracting Authority this contract supports		
	Expiry date		
Where else is this organisation using cleared staff that you are sponsoring? *Please note. Organisation includes HMG contracting authorities or other industry organisations you are subcontracted to as well as any overseas organisations (including overseas governments) which require you to sponsor clearances*	Organisation		
	Number of contracts		
	Organisation		
	Number of contracts		
	Organisation		
	Number of contracts		
	Organisation		
	Number of contracts		
	Organisation		
	Number of contracts		
	Organisation		
	Number of contracts		

There is space for 50 network organisations. If you need to enter more enter new columns.

There is space for 30 contract organisations, if you need more please enter new rows.

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 is a key component to aftercare through supporting good security practices from the top down.

The evidence items that you submit need to show senior leadership visibility in demonstrating the behaviours expected of individuals who hold National Security Vetting and have access to classified material. They also need to demonstrate that the appropriate and required mechanisms are in place to support robust personnel security and provide rigorous oversight. Key to this is ensuring that the HR, Welfare and Security functions are joined up and working collaboratively.

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

The items that need to be submitted in order to evidence that you have implemented an effective Governance Framework are:

Evidence	Dashboard	Submission Form	Preferred Format
Terms of Reference for Security Positions and Working Groups		✓	Text
Evidence that the Personnel Security Controller has accepted their responsibilities		✓	Text
Company Security Governance Policy		✓	Text and diagram (for example process flow or organisation chart), RACI matrix
Clearance levels of the Personnel Security Controller, the Board Level Contact and anyone else involved in NSV-related activities within your organisation.		✓	Text
Terms of Reference / responsibilities of all individuals in involved in NSV-related activities within your organisation.		✓	Text
Organisation charts clearly demonstrating security functions and lines of delegation.		✓	Text and diagram
Documentation providing Board level oversight of personnel security.		✓	Diagram
Contract information, for your company and organisations in its network	✓		*Contract Summary – Your Org tab & Contract Summary – Network tab*
For your company's network (i.e. where your company has sponsored NSV-holders within other organisations), provide: • Details of the company • PSC representative / representation	✓		Network Detail tab

Insider Threat Risk Assessment

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.

You must ensure that a risk assessment is conducted for your organisation using a risk methodology that suits your business. The evidence items that you submit must clearly demonstrate that robust policy, processes and mechanisms have been implemented to identify, assess, classify, mitigate and monitor personnel security risks and insider threats.

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

The items that need to be submitted in order to evidence that you have implemented appropriate measures that support Insider Threat Risk Assessment are:

Evidence	Dashboard	Submission Form	Preferred Format
Personnel security risk management policy which includes Security Risk Management Principles and Insider Threat considerations		✓	Text
Personnel security risk management processes, which includes clear endorsement and oversight of the personnel security risk register at a senior level, ideally at board level		✓	Text, diagram
Performance of formal risk assessment, including role-based risk assessment, against the Contractor and their network.		✓	Text
Risk register template*		✓	At PSC's discretion**
Regular reviews of Insider Threat / Personnel Security risk	✓		*Dashboard* tab, *Insider Threat / Personnel Security Risk Review* section

!

*There is no requirement to provide your completed risk register or expose privileged organisational risks. We are assessing the process you use to assess and manage risks, not the risks themselves.

** The format will depend on the system used. For a fully integrated IT solution a series of screenshots will suffice, for a simpler spreadsheet-based system then a copy of the blank template would be appropriate.

Pre-vetting Screening

Pre-vetting screening comprises the procedures involved in deciding an individual's suitability to hold NSV.

The evidence that you submit must clearly demonstrate that you have the proper secured tools in place to manage your vetted population and network, as well as the mechanisms in place to ensure effective pre-vetting screening.

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

The items that need to be submitted in order to evidence that you have implemented appropriate measures that support Pre-vetting Screening are:

Evidence	Dashboard	Submission Form	Preferred Format
Formal accreditation of the IT system, for example DART		✓	Text / screenshot of DART accreditation
Vetting Register template*		✓	At PSC's discretion**
NSV data relating to your direct clearance-holder population.	✓		*Dashboard tab, Total Clearances, utilisation and forecast* section
NSV data relating to your network	✓		*Network detail* tab
Eligibility policy which includes checks conducted prior to NSV application such as: • Clear requirement for NSV • BPSS checks		✓	Text

!

*There is no requirement to provide your completed vetting register or provide individual vetting data. We are assessing the process you use to managethe vetting process, not the vetting itself.

** The format will depend on the system used. For a fully integrated IT solution a series of screenshots will suffice, for a simpler spreadsheet-based system then a copy of the blank template would be appropriate.

Ongoing Personnel Security

Your aftercare processes should clearly demonstrate how your policies are implemented to effectively manage vetted individuals that you are responsible for.

The evidence you provide must 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. Your evidence should also include how vetted individuals travelling to high risk countries are provided with appropriate briefing.

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

The items that need to be submitted in order to evidence that you have implemented an effective aftercare framework are:

Evidence	Dashboard	Submission Form	Preferred Format
Aftercare policy that includes international travel		✓	Text
Aftercare processes		✓	Diagram, for example process flow or organisation chart, templates.
Aftercare data relating to your direct clearance-holder population (as raised during your reporting period). **Please note that if you are applying for IPSA accreditation that you do not need to complete this section of the Dashboard.**	✓		*Dashboard tab: Clearance Aftercare: Within Your Organisation* section
Aftercare data relating to your network (as raised during your reporting period). **Please note that if you are applying for IPSA accreditation that you do not need to complete this section of the Dashboard.**	✓		*Dashboard tab: Clearance Aftercare: Within your network of sponsored clearances* section

Monitoring and Assessment of Workers

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

This activity cannot take place in isolation, and a holistic approach to protective monitoring is required. The evidence that you submit must clearly demonstrate:

- How your organisation ensures that the NSV holders it is responsible for continue to be eligible for NSV on an ongoing basis.
- How all levels of the organisation are actively engaged in identifying individuals who may be vulnerable or susceptible to coercion.

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

The items that need to be submitted in order to evidence that you have implemented appropriate measures that support Monitoring and Assessment of Workers are:

Evidence	Dashboard	Submission Form	Preferred Format
NSV eligibility review policy		✓	Text
NSV eligibility review processes		✓	Diagram, for example process flow or organisation chart, templates.
Behaviour monitoring policy		✓	Text

Investigation and Disciplinary Practice

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

The evidence you provide must clearly demonstrate how security incidents are identified, understood and resolved; ensuring that the recurrence of these incidents is mitigated as far as possible. The evidence must also demonstrate proportionate disciplinary handling for any individual(s), both within the organisation's clearance-holder population and its network.

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

The items that need to be submitted in order to evidence that you have implemented appropriate measures that support Investigation and Disciplinary Practices are:

Evidence	Dashboard	Submission Form	Preferred Format
Incident handling policy		✓	Text
Incident handling processes		✓	Diagram, for example process flow or organisation chart, templates.
Incident data	✓		*Dashboard* tab: *Insider Threat / Personnel Security Incidents* section
Disciplinary policy		✓	Text
Disciplinary processes		✓	Diagram, for example process flow or organisation chart, templates.

Security Culture and Behavioural Change

Implementing and enabling a positive security culture within your organisation & network is key to the effective management of aftercare.

The evidence you provide must include the training, communications and information resources that you have implemented to ensure that your staff and the NSV holders within your network are aware of the risks posed to them, and how they can contribute towards mitigating personnel security risk.

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

The items that need to be submitted in order to evidence that you have implemented appropriate measures that support Security Culture and Behavioural Change are:

Evidence	Dashboard	Submission Form	Preferred Format
Personnel Security Training Plan / Programme		✓	Text / diagrams / presentation
Personnel Security Communications Plan / Programme		✓	Text / diagrams / presentation
Good Practice Repository Description		✓	Text description / process diagram / screenshot

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 indviduals ability to hold a clearance. Incidents also should be reported to the relevent 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.

Discplinary 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 individuals 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.

Notes

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