Ministry of Defence

Facility Security Clearance (FSC) Policy and Guidance for UK Defence Suppliers and MOD Contracting Authorities

Version History

Document Version	Date Published	Summary Of Changes
1.0	Jan 2023	
1.1	Sept 2023	WARP Contact Details Updated
1.2	Nov 2023	Updated to reference the National Security Act which replaces the Official Secrets Acts 1911-1939
1.3	Jan 2024	Clarification of wording regarding Remote/Home Working
1.4	Mar 2024	Clarification of wording at Para 19.4 and replacement of the term “Contractor” with “Supplier” throughout the guidance.

Related Documents

GovS 007: Security

National Security and Investment Act 2021

Terminology

shall: denotes a requirement: a mandatory element.
should: denotes a recommendation: an advisory element.
may: denotes approval.
might: denotes a possibility.
can: denotes both capability and possibility.
is/are: denotes a description.

Contents

PART 1 – FSC POLICY

1 FSC Requirement

1.1 Some Companies operating in the UK (hereafter referred to as 'Suppliers') hold contracts which require them to safeguard assets classified SECRET or above or International Partners' assets classified CONFIDENTIAL or above (hereafter referred to as 'classified above OFFICIAL[1]'), on their own premises.

1.2 A Facility Security Clearance (FSC) is required to ensure the Supplier meets and maintains the required protective security controls to safeguard these classified assets. It provides the Contracting Authority (CA) with assurance that these assets will be appropriately protected. Clearances are facility specific so a larger Supplier may require multiple clearances for one or more establishments.

1.3 This policy and guidance is a MOD supplement to GovS 007: Security (issued by the Cabinet Office) which sets the baseline standards for protective security. This document is specifically directed at UK Defence Suppliers and MOD Contracting Authorities (MOD Delivery/Project Teams).

2 FSC Sponsorship

2.1 Suppliers cannot request FSC. The requirement for clearance shall be sponsored by the CA. The CA can be:

- a UK Government Department or Agency;
- a Supplier that already holds FSC and intends to subcontract classified work subject to the agreement of the Government CA;
- an Overseas Government with which the UK has a bilateral security agreement/arrangement;
- an International Organisation such as NATO.

[1] Please note OFFICIAL-SENSITIVE is part of the OFFICIAL tier and not a separate classification.

3 FSC Accreditation and Assurance

3.1 Each UK Government Department or Agency is responsible for accrediting and assuring their own Suppliers including any Third-Party Suppliers (Subcontractors). Accreditation and assurance shall include an assessment of the physical, personnel, and cyber security controls.

3.2 The Ministry of Defence, Defence Equipment & Support, Principal Security Advisor hosts the Industry Security Assurance Centre (ISAC). The ISAC is responsible for FSC accreditation and assurance in relation to MOD contracts and contracts with International Defence Organisations. Additional ISAC responsibilities include Industry Personnel Security Assurance (IPSA) together with administration of the FSC and IPSA Databases, the promulgation of Security Notices and other security guidelines, and advice or instructions via the ISAC Vault (restricted access website), or other appropriate methods.

4 Obtaining Confirmation of an Extant FSC

4.1 Confirmation of whether a Supplier holds FSC shall be obtained from the ISAC. Contact details for the ISAC are included below:

MOD Defence Equipment & Support
(MOD DE&S PSyA ISAC)
Poplar -1
MOD Abbey Wood
2004
Bristol
BS34 8JH

Email: ISAC-Group@mod.gov.uk.

4.2 In order to avoid drawing attention to the nature of the assets held on a Supplier's site, and thereby increasing the level of threat to that site, the knowledge of holding FSC is itself classified OFFICIAL-SENSITIVE. For the protection of the Supplier, its employees and the assets it holds, a Supplier shall not publicise, or divulge that it holds FSC to anyone other than HMG Personnel or other FSC accredited Suppliers.

5 FSC Linkage to Industry Personnel Security Assurance (IPSA)

5.1 All UK Defence Suppliers with, or undertaking FSC accreditation shall also be required to undertake Industry Personnel Security Assurance (IPSA) at an organisational level as part of the process unless they have already undertaken IPSA accreditation separately.

6 The Importance of Protecting Classified Assets

6.1 Everyone who has access to classified assets is responsible for their safeguarding. This document should be read as a supplement to Government Functional Standard GovS 007: Security which sets out the expectations for protective security.

6.2 Assets are classified to indicate the sensitivity of the information and the baseline personnel, physical and cyber security controls necessary to defend against a range of threats.

6.3 Suppliers holding FSC are therefore required to put in place enhanced security controls as assets classified above OFFICIAL need to be defended against serious threats such as economic and state-sponsored espionage.

6.4 If classified assets are compromised, it could have serious consequences such as:

- disruption to military or intelligence operations;
- damage to diplomatic relations with friendly governments;
- damage to the resilience and security of Critical National Infrastructure assets;
- widespread loss of life.

6.5 Suppliers that hold FSC constitute ‘critical suppliers to government’ under the National Security and Investment Act 2021. The Act is designed to protect the UK from investment activity that might harm national security.

6.6 If a Supplier does not maintain the required security controls it could result in financial penalties, contract termination, loss of FSC and even prosecution under the Official Secrets Act or National Security Act.

7 Financial Costs and Principles of Free Trade

7.1 There is no financial cost for Suppliers undertaking FSC accreditation, but they might need to make changes to their site, infrastructure, and business administration, at their own cost, to meet the standards required for accreditation.

7.2 FSC operates in accordance with the principles of free trade. A Supplier does not have to hold FSC to bid for a government contract, nor does holding FSC allow a Supplier to receive preferential treatment during the tender process.

8 FSC Eligibility Criteria

8.1 FSC shall only be issued if the Supplier fulfils the minimum criteria as per the subheadings below:

8.2 **Requirement for FSC**

- The Supplier shall have a legitimate reason to safeguard assets classified above OFFICIAL on their own premises.

8.3 **Companies House Registration**

- The Supplier shall be registered with Companies House.

8.4 **Board Composition**

- At least 50% of the Board of Directors or UK Management Board shall legally reside in the UK and be British Nationals, or dual Nationals where one of the dual nationalities is British subject to any restrictions. However, where contracts concern Critical National Infrastructure or particularly large quantities of classified material need to be held on the Supplier premises, UK MOD may require the majority of the Directors to be British Nationals. Where the nationalities of the Directors are on a 50/50 basis and FSC is approved, the Chairperson of the Board shall be a British National, with a casting vote.

9 Key Supplier Contacts/Roles

9.1 Board Level Contact

- One member of the Board shall be designated as the individual responsible for security within the organisation. (hereafter referred to as ‘the Board Level Contact’). The Board Level Contact shall be a British National, or a dual National where one of the dual nationalities is British subject to any restrictions.

Appointment of the Board Level Contact is subject to them successfully being granted and maintaining the appropriate level of NSV clearance.

- The Board Level Contact should be of sufficient seniority to be able to ensure the maintenance of appropriate standards and to drive rectification measures if necessary. The role of the Board Level Contact should be recorded in Terms of Reference administered internally by the Supplier.

9.2 Facility Security Controller

- One employee shall be designated as the individual, responsible to the Board Level Contact, for all aspects of and day to day management of security within the facility. A large Supplier, or a Supplier with substantial contractual obligations, shall have a full time Facility Security Controller, supported by one or more security staff (including the roles set out below). A Supplier with a number of different sites, may need to appoint Local Security Contacts, who report to a [Group] Facility Security Controller. Whilst not mandatory a Supplier may wish to identify an individual to act as the Deputy in the absence of the appointed Facility Security Controller. The Facility Security Controller shall be a British National, or a dual National where one of the dual nationalities is British subject to any restrictions. Appointment of the Facility Security Controller is subject to them successfully being granted and maintaining the appropriate level of NSV clearance.

- The role of the Facility Security Controller, including which individuals can exercise the Controller’s responsibilities in their absence, should be recorded in Terms of Reference administered internally by the Supplier.

9.3 Personnel Security Controller

- An employee of the Supplier shall be designated as the 'Personnel Security Controller' who is responsible for determining which other employees will be put forward for National Security Vetting (NSV).

- The Personnel Security Controller also refers to, and explicitly includes any secondary individual(s) with equivalent roles and responsibilities in the event of the absence of the primary title holder (e.g., a Deputy). The Personnel Security Controller shall be a British National, or a dual National where one of the dual nationalities is British subject to any restrictions. The Supplier's Facility Security Controller and Personnel Security Controller can be the same individual.

- The Personnel Security Controller shall apply for NSV. Their role in facilitating further clearance applications will be subject to them successfully being granted and maintaining their clearance.

- The role of the Personnel Security Controller, including which individuals can exercise the Controller’s responsibilities in their absence, should be recorded in Terms of Reference administered internally by the Supplier.

9.4 Cyber Security Officer

- One employee within the organisation shall be designated the individual responsible for oversight and compliance with cyber aspects of information security including undertaking cyber compliance reviews, managing cyber related security incidents and assisting in remediation of information security incidents.

9.5 Crypto Custodian

- Where the Supplier is required to hold cryptographic material or equipment one employee shall be designated as the individual responsible for the secure handling, that is, receipt, storage, distribution and disposal, of all cryptographic material on the Supplier's site. A Deputy shall also be appointed. Security Officials of the relevant CA shall notify the Supplier of the procedure for appointing and registering a Crypto Custodian.

9.6 Atomic Liaison Officer

- Where the Supplier requires access to ATOMIC information one employee shall be designated as the individual responsible for the security measures adopted for the protection of all ATOMIC information. The Facility Security Controller may also be appointed to this role. The appointment of the ATOMIC Liaison Officer shall be notified for approval, on behalf of all Contracting Authorities to the ATOMIC Coordination Officer, UK MOD.

PART 2 – FSC PROCESS

10 Preliminary Discussions

10.1 Prior to sending out an Invitation to Tender and subsequently placing a contract involving assets classified above OFFICIAL, preliminary discussions are often necessary between the CA and prospective Supplier representatives. During such discussions it may be necessary to divulge a limited amount of classified information above OFFICIAL. As discussions proceed, and the nature of the proposed work is more clearly defined, the CA shall specify the 'security aspects', if only provisionally, as clearly as possible so that prospective Suppliers are able to assess the security controls, and estimate the likely costs involved.

10.2 Preliminary discussions with non-FSC Suppliers may take place prior to contract award provided that no information classified above OFFICIAL is physically sent to the potential Suppliers. Information classified above OFFICIAL may be verbally or physically disclosed to Supplier personnel at the CA's establishment provided that the individuals having access have been granted the appropriate Baseline Personnel Security Standard (BPSS) or NSV Clearance. In respect of the latter, the CA must act as the Sponsor for such clearances.

10.3 Information classified OFFICIAL may be provided to the Supplier but shall be accompanied with a copy of the "OFFICIAL and OFFICIAL-SENSITIVE Contractual Security Conditions" included in the SAL and Contractual Security Conditions Industry Security Notice.

10.4 If classified information is disclosed orally, its classification shall be made clear to the recipient and, the recipient informed that the information falls under the scope of the Official Secrets Act and National Security Act. The CA shall also ensure that it is understood that no commitment is being entered into on the part of the CA and that discussions may be terminated without explanation.

10.5 To avoid legal challenge the CA shall not give preference to an existing FSC holding Supplier over a non-FSC Supplier when preparing their Invitation to Tender (ITT) shortlist.

10.6 At each stage in the negotiation process, the prospective Suppliers should be encouraged to think about the implications of providing appropriate security controls to protect the relevant classified assets against compromise. Where a prospective Supplier envisages difficulties or specific requirements, it shall be made clear what level and type of support, if any, might reasonably be expected from the CA.

11 Provisional FSC and Release of the ITT

11.1 Once the CA has identified the prospective Suppliers to whom it wishes to issue the ITT, it shall obtain confirmation that the chosen Suppliers currently hold an appropriate FSC. If not, and it is intended to issue an ITT for a contract that will involve assets classified above OFFICIAL being held on a Supplier's premises prior to Contract Award, the ISAC shall undertake the due diligence/security clearance checks with third party organisations for a Provisional FSC.

11.2 The ISAC may undertake a physical security assessment of the premises at the ITT phase where required by the CA and this will be assessed in parallel with the aforementioned checks. The standard for physical security will be based on the CA's risk appetite for the tender. A re-assessment against the terms of the contract would be required should the contract be awarded. Use of existing Government approved or FSC locations is preferred for above OFFICIAL assets at the ITT phase.

11.3 Following successful completion of the above checks or, if considered appropriate in tandem with them, the CA shall initiate and progress NSV clearances or instruct the Supplier to initiate BPSS checks as appropriate for those individuals who will be involved in the preliminary discussions or require access to assets classified above OFFICIAL as a result of the tendering process.

11.4 Once these checks have been completed satisfactorily, the ISAC will confirm that the site has been awarded a Provisional FSC, allowing the release of the ITT.

11.5 Where a contract will require the potential Supplier to hold assets classified above OFFCIAL but not at the tender stage, the potential Supplier not holding FSC or Provisional FSC may, with the approval of the relevant CA, be invited to tender for the contract but the Supplier shall be advised in the tender documentation that the facility will be required to be granted FSC should it be selected to undertake the contract and that contract award is subject to FSC being granted.

11.6 The ITT and contract shall include appropriate "Security Measures" and be accompanied by a detailed Security Aspects Letter (SAL). Please see the SAL and Contractual Security Conditions Industry Security Notice for further information.

11.7 On issuing an ITT, the CA shall provide written advice as to the nature of general, and any specific, protective security controls that will be needed before the contract can be awarded. Such advice, where possible, should be clear and sufficient for the Supplier to include in its tender appropriate costs for the installation of required protective security controls.

12 Precontract Award FSC Accreditation Phase

12.1 Should a non-FSC or Provisional FSC Supplier be selected to undertake the contract, the ISAC shall initiate action to grant the Supplier a FSC. The Supplier shall not be awarded the contract until an assurance has been provided that the Supplier's facility has satisfied the due diligence checks and been granted FSC. If FSC is denied the CA shall make a commercial decision as to whether to award the contract to another Supplier who submitted a bid or retender the contractual requirement. Irrespective of that decision the existence of FSC is mandatory before the contract can be awarded.

12.2 In order to initiate FSC accreditation the Supplier shall complete the Government Industry Security Assurance (GISA) Form and submit the form to the ISAC. On receipt of this form, the ISAC shall initiate checks with third party organisations to establish professional competence and reliability of the Supplier.

12.3 The ISAC shall appoint an ISAC Security Advisor to liaise directly with the Supplier to review protective security of the site including physical security, management structures and procedures together with providing advice on what improvements are required to site security infrastructure, processes and documentation to bring the facility up to the standard required for a FSC.

12.4 Once this site review is complete and all necessary measures and procedures are in place, the ISAC shall write to the appointed Facility Security Controller or Board Level Contact, advising that the site has been provided with FSC. The ISAC shall also inform the local Police Service Special Branch and Counter Terrorist Security Advisers (CTSAs). If any of the above checks reveal information about the Supplier or its Directors that raise concerns over the suitability for awarding the Supplier FSC, the ISAC shall carry out a risk-based assessment, consulting as necessary with other relevant authorities, and fully document the reasons for the decision to either grant or deny the FSC. Where an FSC is denied, the ISAC may not be able to reveal the reason to the Supplier due to national security considerations.

12.5 Given the possibility of rapid changes in the Supplier's circumstances, the FSC checks shall be repeated if any changes to the Supplier Ownership or Executive Board structure occur. ISAC Assurance visits to the Supplier's site shall be repeated every two years where assets up to SECRET are held and annually where TOP SECRET assets are held.

12.6 Contracts and ITTs involving assets classified above OFFICIAL shall include security conditions drawing the Supplier's attention of the requirement to protect such information to a degree no less stringent than that required by GovS 007 and to the relevant clauses in the Official Secrets Act and National Security Act. It shall be made clear to the Supplier that information received or generated as a consequence of the contract is not to be communicated to individuals other than those appropriately cleared, with a need-to-know, and authorised to work on it. These conditions provide the legal and contractual backing for the security controls the Supplier will be required to implement.

13 Actions Required following Contract Award

13.1 Once the contract has been signed, but before any work classified above OFFICIAL takes place, the ISAC Security Advisor shall visit the Supplier to brief the Board Level Contact and Facility Security Controller. The ISAC Security Advisor shall provide the Facility Security Controller with detailed security guidance to cover all aspects of protective security controls. The ISAC Security Advisor, in conjunction with the Supplier, and if necessary, consulting the local Special Branch, shall carry out a risk assessment based on the nature and magnitude of the threats relative to the value of the assets at risk. The ISAC Security Advisor shall advise what additional security controls, if any, are required which may include for example structural modifications, new barriers, access controls, detections systems etc.

13.2 The CA in consultation with the Personnel Security Controller shall confirm which employees require Security Clearances and the levels of clearance required. Where SC and DV clearances are required, the CA in consultation with the Personnel Security Controller shall decide who is to be responsible for undertaking the vetting process. The Personnel Security Controller shall be responsible for maintaining a record of security clearances approved for the Supplier's employees and maintaining justification for the clearances based on a role/personnel security risk assessment.

13.3 The ISAC shall take all necessary steps, including site visits to obtain and maintain an assurance that the security conduct of Suppliers and Suppliers is and continues to be adequate for the safeguarding of classified assets in accordance with GovS 007.

13.4 The Supplier shall immediately inform the ISAC and CA, when changes occur which might affect security, for example, changes of company ownership, accommodation, IT, Facility/Personnel Security Controller or Board Level Contact.

13.5 On completion of the contract where there is no further need for the Supplier to hold classified assets on its premises, the CA is responsible for recovering any security equipment loaned to the Supplier and ensuring that all classified assets are removed or securely destroyed. The CA shall advise the ISAC when the Supplier is no longer engaged on classified work.

13.6 Should a contract be terminated for violation of the security conditions, the ISAC, and the Government Security Secretariat (GSSmailbox@cabinet-office.gov.uk) of the Cabinet Office shall be advised of the circumstances.

PART 3 – STANDARDS

14 HMG Oversight and Security Assurance

14.1 Government Departments and Agencies remain the owners of and are ultimately responsible for the protection of classified assets they provide to Suppliers, or which are generated by Suppliers as a consequence of contracts placed with them. Government Departments and Agencies shall ensure any classified assets released to Suppliers or generated by Suppliers under contract, are protected in accordance with the baseline security provisions contained in GovS 007.

14.2 For contracts that involve assets classified above OFFCIAL undertaken by Suppliers, it is the responsibility of each Government Department and Agency to undertake the oversight and security assurance requirements. This includes providing security advice for such requirements and leading on investigations when such assets have been compromised and/or are the subject of a security breach.

15 Foreign Ownership Control or Influence of an FSC Supplier

15.1 To mitigate the possibility of Foreign Ownership Control or Influence (FOCI) being exerted in Supplier organisations that hold FSC and work on classified contracts “Security Measures” shall be included in all contracts where the Supplier will be required to access and safeguard classified assets. Suppliers shall also include these “Security Measures” or similar wording in contracts when subcontracting any elements of classified work in support of HMG programmes.

15.2 To further mitigate the possibility of FOCI being exerted in a Supplier organisation owned by an Overseas Government or Supplier, at least 50% of the Board of Directors or UK Management Board shall legally reside in the UK and be British Nationals, or dual Nationals where one of the dual nationalities is British subject to any restrictions. The ISAC shall ensure that this is the minimum structure both during the FSC accreditation process and whilst the Supplier holds FSC.

15.3 The ISAC shall be satisfied that arrangements within the Supplier’s organisation meet the UK’s national security requirements and obligations under international/bilateral Security Agreements/Arrangements. Therefore, during the FSC accreditation or, as a consequence of any Supplier structural changes, specific consideration is to be given to the ownership of the Supplier’s organisation and an assessment is to be made on the composition and acceptability of the Directors of the Board of the UK Supplier to ensure that FOCI cannot be exerted within the organisation by non-British members of the Board or any Foreign Government or other party that owns the organisation in full or in part.

15.4 A Supplier is considered to be operating under FOCI whenever a foreign interest has the power, directly or indirectly and whether exercised or not, to direct or decide

matters affecting the management or operations of the organisation in a manner which may be contrary to the national security interests of the UK. The following factors relating to the Supplier, the foreign interest and the government of the foreign interest are to be reviewed in determining whether a Supplier is under FOCI:

- any evidence of economic or government espionage against the UK;
- record of enforcement and/or engagement in unauthorised tech transfer;
- the type and sensitivity of the assets that will be held at the facility;
- the nature and extent of the FOCI;
- the level of ownership or control by a Foreign Government or other party (in whole or in part).

16 Notification of Changes in Ownership and Control or Closure of a Supplier with Facility Security Clearances (Responsibilities of the Supplier)

16.1 The Supplier shall notify the CA and ISAC of any change in the circumstances within the Company which may have a bearing on its security status and its ability to carry out its classified contracts. In particular, the following shall be immediately reported and, where possible, in advance:

- proposed change of ownership and control, including any foreign acquisition which will raise the stockholding by any foreign interest to 5% or more of the total company stock;
- any changes to the Board of Directors;
- appointment of a person, who is not a British National, or who holds Dual Nationality, to a position within the Company where that person may be able to influence the appointment of staff to those areas of the organisation which are engaged on classified work or where access to classified assets is needed;
- purchase by a person, who is not a British National, of sufficient shares in the Company which would enable that person to appoint or influence the appointment of individuals to positions where access to classified assets or a secure area is involved.

16.2 In cases where the FSC Supplier is subject to a change of ownership it should not be assumed that any existing government contracts will be automatically novated to the new owners. Before such novation's can take place, the CA and ISAC will need to be satisfied that the new owners meet certain conditions. These include the need to be satisfied that classified assets will continue to be protected to the required standard. Where assets classified above OFFCIAL are involved, the new Company will have to continue to meet the criteria for clearance.

16.3 Any intention to close down a FSC Supplier's site or to transfer classified work from one FSC site to another shall be brought to the attention of the CA and ISAC, so that proper arrangements can be made for the disposal of classified assets and the completion of the necessary security procedures.

17 Responsibilities of the FSC Supplier's Management

17.1 Contractual responsibility for the security of government assets held on the Supplier's premises rests with the Supplier's Board of Directors.

17.2 The baseline controls covered in GovS 007 have been designed to flexibly provide appropriate levels of protection for classified assets, wherever they are held. They can also be used to protect the Supplier's own assets, technology and expertise, on which the integrity, prosperity and security of the Supplier and its employees may depend.

17.3 Senior managers shall emphasise that security is an integral function of line management and security controls are only effective if properly planned, implemented and supervised. They shall insist on the implementation of appropriate levels of security as contractually defined and be seen to give full support to line managers and security staff involved in achieving and maintaining that objective.

17.4 Arrangements to meet the required security controls are for the Supplier to decide but shall always be sufficient to meet the baseline controls contained within GovS 007. The ISAC shall be available to provide advice as to the adequacy of the security controls implemented.

17.5 When deciding such arrangements, the Supplier should bear in mind that HMG will treat any significant lapse in security, leading to the compromise of classified assets, as a serious matter. Failure to fulfil security obligations in breach of contractual conditions could result in contractual penalties, the termination of the contract and where applicable the removal of a FSC from the Supplier, as well as potential prosecution under the Official Secrets Act and/or National Security Act depending upon the severity of the breach.

17.6 The Board Level Contact is specifically responsible for:

- exercising policy control;

- giving appropriate authority and effective support to the Facility/Personnel Security Controllers;
- approving Company Security Instructions generated by the Supplier;
- informing the ISAC and CA of changes to the Supplier's status, that is, ownership, control, closure, etc.

17.7 The Facility Security Controller has overall day to day responsibility for all aspects of security and is specifically responsible for interpreting, implementing, and monitoring security controls for the appropriate protection of classified assets held on the Supplier's site, by:

- liaising within the Supplier's organisation, and between the Supplier and Security Officials of the ISAC and CA;
- advising management on the interpretation and implementation of contractual and, where appropriate, legislative security controls;
- preparing and implementing the Company Security Instructions, and making sure that they are made available to, and understood by all appropriate employees, updating them as necessary;
- being readily available for consultation and giving security advice to the Supplier's management and employees;
- co-ordinating the planning of appropriate security controls for a new contract or for the alteration of buildings where classified assets are to be handled, stored or produced;
- arranging for appropriate security education and awareness training, particularly for new staff, to ensure that they understand the scale, nature of the threats and protective security controls required;
- ensuring that any breach of security is reported immediately to the CA and, if appropriate the regional police and that the circumstances are fully investigated, the outcome is recorded in the breaches register and that a full report and impact analysis is passed to the CA;
- ensuring that any security incident involving classified material is reported in accordance with the Incident Reporting ISN to the CA and MOD Defence Industry Warning, Advice and Reporting Point (WARP) at:

  Email: For those with access to the RLI: Defence WARP (MULTIUSER)
  Email: For those without access to the RLI: DefenceWARP@MOD.Gov.UK
  Telephone: Working Hours: +44 (0) 3001 583 640
  Mail: Defence Industry WARP
  DE&S PSyA Office, MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH.

17.8 It is important for the Facility Security Controller to consult widely within the Company when considering security controls for a new contract or alterations to buildings requiring the co-operation and resources of several departments. Failure to discuss requirements for such controls well in advance may subsequently result in hurried and expensive remedial controls.

17.9 The Facility Security Controller shall, as soon as possible, inform the CA when each contract containing Security Measures have been completed or when the Supplier is no longer undertaking contracts that include such Security Measures. It is important to note, that although the Facility Security Controller's function under the Board Level Contact is an executive one, overall contractual responsibility remains with the Board of Directors.

18 Company Security Instructions

18.1 To fulfil its contractual obligations, the Supplier shall provide guidance to employees in the form of Company Security Instructions. The instructions should:

- be prepared by the Facility/Personnel Security Controller at an early stage and updated as necessary;
- be approved by the Board Level Contact;
- be issued with the authority and signature of the Managing Director;
- be classified as low as practicable, to help ensure full circulation and availability to all involved staff;
- publicise the appointment, details and availability of the Facility Security Controller and their deputy and make it clear that they are available for consultation and advice on any security aspect.

19 Security Advice and Education for Suppliers

19.1 In addition to advice given by the CA and ISAC, FSC Suppliers shall be provided full access to GovS 007 and associated supplementary documents including subsequent amendments. The normal method to access GovS 007 for FSC Suppliers will be via the ISAC Vault to which the Supplier’s Facility Security Controller should arrange to have access.

19.2 The ISAC will promulgate Facility Security Notices (FSNs) which address security issues specifically related to FSC Suppliers for classified contracts and programmes. The method of communication of FSNs and other appropriate security education and awareness materials will normally be via the ISAC Vault or by other appropriate methods.

19.3 The ISAC will also promulgate on the GOV.UK website Industry Security Notices (ISNs). ISNs provide FSC and non-FSC Suppliers advice on security policy, guidance and other information that has an impact on HMG assets classified OFFICIAL. ISNs can be accessed at: https://www.gov.uk/government/publications/industry-security-notices-isns

19.4 Board Level Contacts, Facility Security Controllers and their appropriate security staff shall attend the protective security briefings arranged by the ISAC, as a condition for the award, or continuation of FSC status. These will complement additional training available from the Defence Industry Security Association (DISA) for Facility Security Controllers and their staff (see below).

19.5 Board Level Contacts, Facility Security Controllers and their staff working for Defence Suppliers are encouraged to join DISA. The Association is a private, professional association set up to encourage Facility Security Controllers to exchange security experience. DISA represents to government the security interests and views of its membership and is often consulted on security policy matters which may affect Suppliers. DISA is therefore provided the opportunity to contribute before significant changes to security policy requirements are introduced.

20 Advertisements Questionnaires and Media Enquiries

20.1 No advertisements, including those for the recruitment of staff, shall draw undue attention to classified projects. Where necessary, reference may be made to information already cleared for open publication but otherwise the relevant CA should be consulted before publication.

20.2 No mention of the existence of a Facility Security Clearance, and no reference to the security status of the Supplier or its employees, shall be included in any advertisement, publicity or exhibition material.

20.3 Suppliers receiving requests or questionnaires seeking information about their business from organisations concerned with the compilation or publication of directories, registers, marketing or business surveys, or from the media, shall consider carefully the implications of disclosure and, if necessary, consult their relevant CA or the ISAC before providing details or discussing aspects of classified work or advanced technology.

20.4 This guidance is not intended to discourage contact with the media but only to protect sensitive information or technology, the disclosure of which might be damaging to national security. Where the Facility Security Controller has any doubts about a particular approach, they should consult the relevant CA or the ISAC as appropriate.

20.5 The King's Awards for Enterprise are the most prestigious accolades for businesses and individuals in the United Kingdom. The corporate awards recognise outstanding

achievements by UK Companies in three categories: International Trade, Innovation and Sustainable Development. Winners receive a range of benefits including worldwide recognition and extensive press coverage. Each Award is valid for five years. The Awards Office invites applications from UK 'Industrial Units', annually, for consideration of an Award for technological achievement. Whilst there is no intention of inhibiting FSC Suppliers from making applications for an Award, any submission which has, or may have, security connotations shall be cleared by the CA.

21 Remote Working Guidance for FSC Suppliers

21.1 Remote working has increased significantly in recent years, and it is becoming common for Suppliers to permit individuals to work remotely at varying degrees on information classified up to OFFICIAL (including OFFICIAL-SENSITIVE). Where appropriate safeguards are in place, approval for such remote working can be given by the individual's Facility Security Controller provided that the requirements specified in ISN 2022/10 are fully implemented. Remote working by Supplier Personnel on MOD information classified SECRET or above is rarely permitted based on the Departmental risk appetite and then only with the prior written consent of the ISAC Security Advisor.

22 Controlling Visits to FSC Premises

22.1 Visitors shall not be allowed access to any classified assets or areas, unless the Facility Security Controller is assured that: such individuals have a 'need to know'; hold the appropriate security clearance and that prior release approval has been granted by the relevant authority. Where only part of a Supplier's premises is used for classified work, the arrangements shall limit visitors without security clearance or the need to know to areas used for non-classified work.

22.2 In areas of FSC premises where classified work is undertaken or assets are held, the Supplier shall ensure that visitors do not have access to the areas or information which they have no authority to access. Accordingly, the Supplier shall implement effective arrangements for the identification and control of visitors. Differing security measures are likely to be required, for example, access control systems, doors, locks, escorts, etc.

22.3 The type of visitor who may need access to premises where classified work is undertaken, or assets held include:

- officials sponsored by the Contracting Authority;
- officials from the ISAC;
- other FSC Supplier employees concerned with government programmes/contracts;
- Third-Party Supplier (subcontractor) employees;

- officials with statutory right of entry, for example, health and safety inspectors;
- overseas visitors;
- system and hardware engineers.

22.4 Other visitors may include customers, potential customers, maintenance Suppliers, the constituency's Member of Parliament, or students and journalists etc, who wish to examine working conditions or industrial processes. In such cases, where the disclosure of classified assets may be involved, the Facility Security Controller shall seek prior approval from the CA and ISAC.

22.5 The ISAC Security Advisor and visitors sponsored by the CA, or another FSC Supplier, should present little difficulty as they are generally well known to the Supplier. However, where there is any doubt as to their status, their 'need to know' or security clearance etc., this shall be confirmed with the CA or the appropriate Supplier's Facility Security Controller.

22.6 Where visitors attend meetings or conferences on the Supplier's premises or on premises arranged by the Supplier, it is important that appropriate security controls are in place to safeguard any classified assets involved before, during and after the event. To this end, the Company Security Instructions shall include appropriate guidance to all employees about the implications for security when organising such events, including the following:

- identify the requirement for an individual attending the event to be made responsible for the security controls, even though the Chairperson and others attending may not be employed by the Supplier;
- compiling a list of those attending including their ‘need to know’ and security clearance status confirmed by the Facility Security Controller and passed to the individual responsible for security of the event;
- ensuring the conference room shall not be susceptible to overlooking or eavesdropping - depending on the venue and the level of classified discussion it may be necessary to consider a technical sweep;
- ensuring access control to the meeting place, or conference room, shall be maintained prior to and during the meeting and during breaks;
- identifying that at the start of the meeting, or conference, the Chairperson shall explain any special security arrangements, for example, the taking away of papers, the securing of paper during breaks, the switching off of mobile telephones;
- identifying that during breaks, any classified assets shall be appropriately secured, or the room shall be kept locked and guarded;

- ensuring that after the meeting, or conference, secure arrangements shall be in place for the disposal of the classified assets involved, and where they are to be passed to those attending the meeting, for transit.

23 Visitors with Statutory Right of Entry

23.1 Access to assets, classified above OFFICIAL, by visiting inspectors conducting statutory inspections, shall only be permitted if the inspector cannot carry out his duty without such access, and an assurance has been received from the authority employing the inspector, that the individual holds a Security Clearance or BPSS as appropriate.

23.2 Officials from various Government Departments and Local Authorities, such as Health and Safety Inspectors, HMRC officers, Fire Inspectors etc, are empowered by statute or bylaws to enter factories, laboratories and working environments, for the purpose of inspection. On production of their credentials, issued by the authorities by whom they are employed, these individuals shall be given the access and facilities they require to perform their statutory duties. The problem of Officials requiring access to areas where classified assets are held may often be resolved by escorting such visitors to ensure that they do not have direct access or temporarily securing or covering up the classified assets involved.

23.3 Under the Health and Safety and Work Act, access to FSC Supplier's sites may be required as a statutory right by Health and Safety Inspectors employed by the Health and Safety Executive (HSE) or by the Local Authority. The right of entry to premises accorded to inspectors under the Act does not excuse them from compliance with the Supplier's security measures for controlling visitors, such as identifying themselves and signing the visitor's book. Where the Inspector wishes to take photographs, which are likely to reveal assets classified above OFFICIAL, the Supplier's Facility Security Controller, having advised the Inspector of the fact, shall agree arrangements for the photographs to be processed securely, to be examined and correctly classified prior to distribution. All HSE Inspectors carry credentials identifying them as HSE Officials and are approved/ cleared to the Baseline Personnel Security Standard level with some cleared to SC and DV levels to allow access to the highest level of classified assets. Where the Facility Security Controller assesses that such an inspection causes specific security concerns the ISAC should be consulted, and subject to agreement, the DSO, HSE shall be advised. Where necessary confirmation of the level of security clearance held by HSE Inspectors should be obtained from the DSO, HSE.

23.4 Local Authority Inspectors may require access to some FSC Supplier's sites. The Inspectors are not usually security cleared but do carry credentials, which differ in design from authority to authority. These Inspectors shall not be given access to areas where classified assets are held without prior arrangements having been made. Where difficulties arise over access by the Inspectors, the Facility Security Controller shall contact the ISAC Security Advisor.

24 Visitors from Overseas

24.1 Except where special arrangements have been agreed and communicated to the Supplier visitors from overseas countries shall not be given access to any classified assets, without the prior approval of the CA.

24.2 Under various bilateral Agreements/Arrangements between the UK and Foreign Governments, it is the visitor's responsibility to make appropriate prior arrangements, through their London Embassy or High Commission, to visit a FSC Supplier's site where the visit involves access to classified assets. In the case of an International Defence Organisation (IDO), such as NATO, arrangements are made through the IDO Security Office.

24.3 The MOD DES PSyA International Visits Control Office (hereafter referred to as IVCO) is responsible for coordinating visits by Foreign Nationals who require access to classified assets associated with defence programmes and contracts held by the MOD Suppliers, or protected areas where such activities are being undertaken within a site. MOD FSC Suppliers shall follow the IVCO Guidance Notes which sets out the principles and processes for visit requests.

25 Overseas Visits by FSC Supplier Employees

25.1 FSC Suppliers may undertake government work that requires its employees to make visits overseas, that involves access to UK classified assets, or 'classified' assets belonging to Foreign Governments or International Defence Organisations (IDO's), for example, NATO.

25.2 There are various international/bilateral Agreements/ Arrangements that allow for the exchange of classified assets. Under these Agreements/Arrangements, prior to such visits, the UK is obliged to provide assurances that the individuals involved hold appropriate levels of security clearance and have been briefed on their security responsibilities. For such visits relating to defence programmes and contracts, MOD DES PSyA IVCO is responsible for providing such assurances except in respect of visits to the Parties to the Framework Agreement relating to sharable information for which separate procedures apply. MOD FSC Suppliers shall follow the IVCO Guidance Notes which sets out the principles and processes for outward visit requests.

25.3 Before an overseas visit by a FSC Supplier's employee takes place, the Facility Security Controller shall:

- brief the individuals involved as to the threats they may encounter and the security controls they are required to observe;
- ensure that appropriate written approval is obtained from the CA where it is necessary for the individual to disclose UK classified assets during an overseas visit;

- plan for any classified assets to be sent by approved diplomatic channels to await collection, where the individual is personally carrying classified assets, the procedures for casual couriers should be followed;

25.4 During the visit, the individual shall take care to appropriately protect any classified assets in their safekeeping. Except when they need to have such assets with them for the purposes of their work, they shall arrange to have them stored securely. With the approval of the CA, this may be on the premises of the organisation being visited or the approved Supplier's agent. Classified assets shall never be left unattended in hotel rooms or hotel safes. Where appropriate levels of protection cannot be guaranteed, classified assets shall be left in the care of the nearest UK Embassy, High Commission or Mission.

25.5 Assets classified above OFFICIAL, handed to a visiting individual by the host being visited, shall only be accepted where it is possible to hand it, on the same day, to the nearest UK Embassy, Consulate or High Commission for official transmission to the UK. Where this is not possible the host shall be requested to send the asset through diplomatic channels in accordance with local national security regulations. In exceptionally urgent circumstances where it may be necessary for the visitor to hand-carry assets classified above OFFICIAL to the UK in relation to a defence contract/programme, approval must be sought and granted by the ISAC.

26 Conventional Forces in Europe Treaty - Guidelines for Challenge Inspections of FSC Suppliers

26.1 Under the Conventional Forces in Europe (CFE) Treaty, former Warsaw Treaty Organisation Inspection Teams may carry out Challenge Inspections at UK industrial sites to satisfy themselves that Treaty Limited Equipment (TLE) is not stored there. TLE includes Main Battle Tanks, Armoured Infantry Combat Vehicles, Artillery greater than 100mm calibre, fixed wing permanently land-based Combat Aircraft and permanently land-based Combat Helicopters. Suppliers will receive between 5- and 8-hours' notice of a Challenge Inspection from Joint Arms Control Implementation Group (JACIG), who will send a forward detachment to advise and discuss any relevant issues. An inspection is normally, though not always, carried out during normal working hours and could last up to 8 hours, made up of several visits which could take place on any day of the year.

26.2 The number of visitors involved in an inspection could total up to 35, that is, Inspectors, JACIG's forward detachment and escorts, representatives from the local police and Army District, drivers, interpreters etc. The Supplier will be required to provide an on-site office, or room, for the Inspection Team and JACIG as well as accommodation for the other visitors. Food may be required for all visitors, on repayment.

26.3 At the majority of sites, Suppliers should be able to protect sensitive assets by 'managed access' techniques, such as:

- shrouding classified machinery and equipment - disguising tell-tale bulges and shapes;
- implementing a clear desk policy;
- switching off computer screens;
- providing vantage points from where inspectors can satisfy themselves that no TLE are stored in a building, without giving them the opportunity to explore it.

26.4 Inspection Teams have no right of access to rooms or buildings, with entrances less than 2 metres wide, unless such rooms or buildings contain TLEs. Where 'managed access' cannot adequately protect classified assets, rooms or buildings can be designated Sensitive Points Within a Site (SPWS). When the JACIG escorting team arrives at the site it must be advised of any SPWSs and the justification for their designation. Suppliers shall not declare a SPWS when other safeguarding methods can be used, nor shall SWPS be designated for reasons of purely commercial sensitivity.

26.5 Prior to the visit the Supplier shall consider the following controls:

- keys for every locked building, room or container with an opening more than 2 metres wide shall be made available, if required;
- all Supplier personnel who may come into contact with the visitors shall be fully briefed and thoroughly familiar with the Supplier's site and products, and the location of buildings, rooms and containers liable for inspection;
- removing all information including, notices, posters, telephone directories etc, which could reveal anything about the Supplier or the employees, from the office or room allocated for use by the Inspectors.

26.6 It should be assumed that each Inspection Team (IT) will include at least one intelligence officer, to collect information, unrelated to the inspection, in the defence, commercial and technical fields. It is also probable that one inspector will be a R & D expert familiar with the Supplier's, or equivalent, products.

26.7 Inspection Teams are authorised to use the following equipment during their inspections:

- binoculars;
- still cameras;
- laptop computers;
- passive night vision equipment;
- dictaphones;

- flashlights;
- video cameras;
- magnetic compasses;
- tape measures.

26.8 During the introductory briefing by the Supplier the Inspection Team shall only be given information it has a right to know, or needs for the purpose of the inspection, for example:

- a brief description of the Company;
- the layout of the site, with a site plan;
- the description and location of any TLE stored on the site. (There shall be no mention of equipment exempt from the Treaty because of its R&D or manufacturing status, in the introductory briefing.)

26.9 For the visit the Supplier's employees shall be aware that the Inspectors:

- will have studied the Supplier and its products beforehand and will know exactly what they are looking for;
- may try to catch the Supplier and its employees off guard by varying the time of their arrival, or by returning after they have left the site, where the inspection time does not exceed the stipulated 8 hours;
- may pretend not to understand English, or will understand more than they admit to, so that they can eavesdrop on conversations or internal radio communications;
- will attempt to take surreptitious photographs or video footage;
- Will talk to any employee and will compare notes after the visit, so all employees should expect tricky questions, to which they should respond politely and courteously while not volunteering more information than is necessary.

27 United Nations Chemical Weapons Convention - Guidelines for Challenge Inspections of FSC Suppliers

27.1 Under the United Nations Weapons Convention, which bans the manufacture or possession of toxic chemicals and imposes controls on a range of chemicals, every building in the UK may be subject to a Challenge Inspection at short notice initiated by another Signatory State. Challenge Inspections aim to check the UK's compliance with the Convention and are conducted by international inspectors from the Organisation for the Prohibition of Chemical Weapons.

27.2 Challenge Inspections to industrial sites are most unlikely but cannot be ruled out. Inspections will be penetrating and detailed, although the Convention acknowledges the right of States to protect national security and commercial confidentiality. It is possible that some Inspectors and Observers may attempt to use an inspection for collecting intelligence.

27.3 The Department for Business, Energy and Industrial Strategy (BEIS) is the National Authority for coordination of the UK's response to the Convention. It provides advice to all Suppliers and will help if a Challenge Inspection is mounted. Such advice may be obtained from: The CWC National Authority, Non-Proliferation, and Office of Nuclear Development, BEIS.

27.4 FSC Suppliers need to draw up contingency plans detailing how they will protect classified assets in the event of a Challenge Inspection. They may also wish to include in the plans how to protect sensitive assets. Most classified assets can be safeguarded by 'managed access' techniques, similar to those suggested for dealing with CFE Challenge Inspections. Under the Chemical Weapons Convention, rooms and buildings with entrances narrower than 2 metres are not excluded from inspection.