Ministry of Defence

Industry Security Notice

Number 2014/01

Subject: Government Security Classification Scheme

Introduction:

1. This Industry Security Notice is re-issued to include a new version of Annex A.

2. On the 2 April 2014 the United Kingdom Government will move to the new Government Security Classification (GSC) policy which will replace the existing Government Protective Marking Scheme (GPMS). This Industry Security Notice provides information on various aspects of the application of the GSC and how it impacts on Ministry of Defence (MOD) national and international industrial security processes and procedures currently applied under the GPMS.

Issue:

3. The GSC introduces a 3 tier security classification policy of OFFICIAL, SECRET, and TOP SECRET identified as below:

OFFICIAL	SECRET	TOP SECRET
This category is for the majority of information created or processed by government and includes both routine business and some sensitive information.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats	This category of information is the most sensitive requiring the highest levels of protection from the most serious threats.

4. The changes in the security requirements to the SECRET and TOP SECRET tiers are minimal, however, the changes to the lower tier are more significant as the new policy consolidates national NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED, and some CONFIDENTIAL information under GPMS into the single 'OFFICIAL' tier. In general MOD will not require its contractors to routinely mark OFFICIAL information under GSC; however there are some exceptions to this rule which are outlined in this Industry Security Notice.
5. The OFFICIAL tier allows for particularly sensitive OFFICIAL information to be identified using an additional handling caveat "SENSITIVE" all such information must be marked OFFICIAL-SENSITIVE.

6. There is no direct correlation between the GSC classification policy and that applied under GPMS. When classifying information under the new scheme, the MOD originator will determine the potential consequences of compromise or loss, to ensure heightened protective security controls are applied as appropriate.
7. The security requirements to be applied for the protection of OFFICIAL-SENSITIVE and for what the MOD will be calling Reportable OFFICIAL information will be defined in a security Condition that will be attached or provided with contracts involving such information.

8. **Aim**

8.1. The aim of this Industry Security Notice and the attached "GSC Guide for Non List X Defence Contractors" at **Annex A** is to provide MOD contractors undertaking contracts involving classified information up to the level of OFFICIAL-SENSITIVE with practical advice and guidance on some of the processes that will continue to be applied under the GSC.

9. **National Security**

9.1. **Contracting**

New Invitations to Tender (ITT) and Contracts

9.1.1. From the 2 April 2014 new ITTs and contracts shall be managed as follows and this Industry Security Notice may be taken as formal authority for this:

9.1.2. The requirements applicable for OFFICIAL information may be included in a future new DEFCON. In the interim contractors should adhere to the provisions under DEFCON 531 and apply sensible "best practice" measures to protect OFFICIAL information which is not identified by the MOD as Reportable OFFICIAL or OFFICIAL-SENSITIVE. Guidance on this can be found in the Cabinet Office document "Working with OFFICIAL information" at the following link below[1].

9.1.3. ITTs and contracts involving OFFICIAL-SENSITIVE information and where there is a requirement to report the loss or compromise of certain types of OFFICIAL information (reportable OFFICIAL) will contain a new narrative clause (to be converted into a DEFCON in due course) and a Security Condition (**Annex B**) that confirms to the contractor the security requirements expected to be applied to protect and handle this level of information. It is anticipated that the Security Condition will be amended in the future to include technical controls for Computer Information Systems and a requirement for the contractor to undertake "good practice" that ensures the early identification of risks and assurance that the risks are being proportionately managed.

[1].https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251475/FAQ1-Working-with-Official-Information-v1.2-Apr-2013.pdf

9.1.4. Security Aspects Letters (SALs) will define the security aspects of the contract in accordance with those applicable under the GSC policy and will be issued for all contracts involving OFFICIAL-SENSITIVE aspects and where MOD specifically require the reporting of the loss or compromise of Reportable OFFICIAL information. SALs will not however be issued where the contract involves information which is OFFICIAL-SENSITIVE (COMMERCIAL) where the sensitivity is only of a commercial nature.

Existing Invitation to Tender and Contracts

9.1.5. From the 2 April 2014 existing ITTs and contracts shall manage the transition as follows and this Industry Security Notice may be taken as formal authority for this:

9.1.6. The security aspects defined in SALs and security requirements will remain extant until an agreed ITT or contract amendment is issued.

9.1.7. The MOD Project Teams will be required to review the security aspects of a contract at the next contract amendment point, SAL annual review or, at the latest, by 1 April 2015. A specific requirement will be placed on the MOD contracting authority to undertake this review by that deadline.

9.1.8. The MOD will endeavour to issue an amendment to SALs issued with ITTs to re-classify and change to GSC before contract placement.

9.1.9. ITT/contract amendments will include changes (if applicable) required to SALs and security requirements and the addition of the new Reportable OFFICIAL and OFFICIAL-SENSITIVE Security Condition as referenced in paragraph 8.1.3.

9.1.10. From the 2 April the MOD will classify information produced as a consequence of an existing NOT PROTECTIVELY MARKED or RESTRICTED contract by default as OFFICIAL and OFFICIAL-SENSITIVE. The MOD will mark RESTRICTED information with the dual marking “RESTRICTED/OFFICIAL-SENSITIVE”. Contractors shall continue to produce and handle classified information as specified under the contract but shall also dual mark any RESTRICTED aspects produced with “OFFICIAL-SENSITIVE” (e.g. RESTRICTED/OFFICIAL-SENSITIVE) until informed otherwise through an agreed contract SAL amendment.

9.1.11. MOD information previously marked PROTECT (with or without a descriptor) should be handled from the 2 April under the requirements for OFFICIAL and apply sensible best practice and appropriate access limitations.

9.1.12. Classified information relating to closed contracts or other legacy information held by contractors which is not altered after the 2 April 2014 should continue to be protected under the extant security requirements and Security Aspects Letter.

Sub-contracts

9.1.13. Currently under the provisions of the Security Conditions included in contracts at GPMS RESTRICTED level, contractors are required to notify the MOD Contracting Authority about any sub-contracts awarded to UK contractors and seek prior approval before sub-contracting to contractors overseas. Such notifications/approvals will continue to be required. For **all** overseas sub-contracts that involve the release of Reportable OFFICIAL or OFFICIAL-SENSITIVE information we aim to streamline and standardise this process. The MOD is proposing a new version of Appendix 5 (Form 1686) to the Contractual Process Chapter of the Security Policy Framework (SPF)[2] - **Annex C;** to be used in all circumstances where contractors wish to place a sub-contract with a contractor overseas where the release of either Reportable OFFICIAL or OFFICIAL-SENSITIVE information is involved. The process will require submission of the single page document either directly to the MOD Project Team or, where specified, to the DE&S Security Advice Centre. The process for such applications is detailed in the flow chart at **Annex D**. The benefit to industry with this is that approved applications will remove the requirement for obtaining individual export licences and support the wider use of open licensing such as OGELs. Such applications will not be required for "off the shelf" purchases where no Reportable OFFICIAL or OFFICIAL-SENSITIVE information is to be released to the overseas sub-contractor or where it has already been determined by the MOD that the prior approval to sub-contract is not required.

9.2. **Access**

9.2.1. Whilst the GSC policy recommends a minimum requirement for appropriate recruitment checks (e.g. the Baseline Personnel Security Standard (BPSS) or equivalent) for personnel accessing OFFICIAL information the MOD will be adopting a risk management approach and will not be mandating recruitment checks for access to MOD information only at the OFFICIAL level. However, as is currently the case for access to RESTRICTED, the MOD will require a Baseline Personnel Security Standard (BPSS) for access to OFFICIAL-SENSITIVE material.

9.3. **Computer Information Systems**

9.3.1. Contractor Computer Information Systems (CIS) used to hold or process classified information at the level of Reportable OFFICIAL and/or OFFICIAL-SENSITIVE will require to compliant with the criteria specified in the Reportable OFFICIAL and OFFICIAL-SENSITIVE Security Condition at **Annex B**.

[2] https://www.gov.uk/government/publications/security-policy-framework

9.4. **Private Venture Grading**

9.4.1. Extant Private Venture (PV) should be classified as detailed below and this Industry Security Notice may be taken as authority for this:

i. NOT PROTECTIVELY MARKED extant PV gradings contractors should classify information by default as OFFICIAL.

ii. Extant PV gradings at RESTRICTED contractors should classify information by default as OFFICIAL-SENSITIVE.

9.4.2. From 2 April 2014 where there is no MOD relationship to the PV activity (i.e. not a variant or derivative of a MOD equipment, and without the possibility to reveal sensitivities relating to a MOD equipment), MOD will notify in the grading response that there is no justification for UK MOD to allocate a security classification to the equipment. In these cases, there will not be any MOD requirement for the application of any security controls.

9.4.3. In cases where a contractor considers that the default attribution of an OFFICIAL or OFFICIAL-SENSITIVE classification is inappropriate, the contractor may seek an updated PV grading.

9.5. **MOD Form 680 Approvals**

9.5.1. Extant MOD Form 680 (F680) approvals will run to the end of their expiry date. There will remain the option for renewals to be made under the legacy GPMS grading of the items concerned; however, where items have been formally re-graded under GSC, this is the classification that should be used.

9.5.2. After 2 April 2014, the entry classification requirement for F680s will be OFFICIAL-SENSITIVE.

9.6. **Exhibition Approval Letters**

9.6.1. Exhibition approval letters only require updating where the equipment concerned materially changes and are therefore unaffected by the introduction of GSC. Contractors need take no action for extant exhibition approval letters.

9.7. **Form 1686 Approvals**

9.7.1. Extant MOD Form 1686 (F1686) approvals will run to the end of their expiry date. Renewals where necessary, or new applications, after 2 April 2014 should be under the classifications identified in the current contract SAL at that time, which may be either GPMS or GSC.

10. **Cryptography**

10.1. Cryptographic items should continue to be managed in accordance with existing procedures. Any queries should be directed to Crypto Services for Defence; email: DESISSCC-CSDPolicyGroup@mod.uk, Telephone: 03067 702 565.

11. International Security

11.1. Protection of International Partners' Classified Information

11.1.1. The UK will continue to protect classified information that it receives from international partners to agreed standards. International partner classified information at the level of RESTRICTED should be protected in accordance with any requirements specified in contract or documentation provided by the international partner and to a standard no less stringent than that applied to UK OFFICIAL-SENSITIVE information

11.1.2. Whilst OFFICIAL-SENSITIVE is identified as the equivalent to international partners' RESTRICTED information, there are some aspects of the security controls for OFFICIAL-SENSITIVE that fall below the minimum requirements generally applied by international partners for their RESTRICTED information. For example, it is not acceptable in any circumstance to email international partners' RESTRICTED information in clear text over the Internet and appropriate encryption must be used. Further details of such requirements are at **Annex D**. These security requirements will be identified in the International Classification Policy chapter of the SPF[3] **must** be applied in addition to those for OFFICIAL-SENSITIVE information.

11.1.3. MOD OFFICIAL information provided to an international partner or overseas contractor may be provided either unmarked, marked 'OFFICIAL', or marked 'UK OFFICIAL'.

11.2. US/UK Defense Trade Cooperation Treaty

11.2.1. The Defense Trade Cooperation Treaty (DTCT) is intended to facilitate the movement of certain categories of equipment and information between pre-approved US and UK government and contractor facilities, and their personnel, (known as the "Approved Community") when destined for certain US or UK government end-users without the requirement for a US export licence or other written authorisation under the U.S. International Traffic in Arms Regulations (ITAR). The DTCT is not directly affected by the GSC and any US defense articles received by Approved Community members at the level of RESTRICTED USML/REL USA and GBR Treaty Community

[3] https://www.gov.uk/government/publications/security-policy-framework

should be protected as advised by the MOD when Approved Community status was granted.

11.2.2. Access to US Defense Articles, including that marked RESTRICTED USML/REL USA and GBR Treaty Community, will continue to require individuals to be granted a personnel security clearance.

Action by Industry:

This Industry Security Notice is issued for information and guidance for MOD contractors for internal use and promulgation as appropriate.

Validity / Expiry Date:

There is no expiry date to this Industry Security Notice.

MOD Points of Contact Details:

MOD
DBR-Def Sy STInd
Zone I
Main Building
Whitehall
London
SW1A 2HB

Email: DBR-DefSy-STIndAH@mod.uk or DBR-DefSy-STind1@mod.uk

17 February 2014

Ministry of Defence

The New Government Security Classification System -

Annex A - A Guide for Non List X Defence Contractors

Unclassified
Protect
Restricted
Confidential
Secret
Top Secret

Official
Secret
Top Secret

02-04-2014

Who should read this?

All personnel working for MOD contractors undertaking defence contracts on their own premises. Everyone working for MOD contractors that handles information needs to understand this change.

Contractors performing work on MOD establishments work to separate security requirements as expressed by the establishment or local security officer and will have access to separate guidance.

Why this guide is important

From 2 April 2014 the Government is simplifying the way the UK classifies its information. This will involve new ways of working with information below SECRET level. All such information will now be classified OFFICIAL.

The introduction of OFFICIAL will take some getting used to, but the MOD strongly support the new approach to classification because it will help improve the way sensitive information is protected in the MOD and by defence contractors.

The key change is that individuals are expected to take more personal responsibility for thinking about the security of the information they handle.

The new approach is called the Government Security Classification (GSC) System

This guidance is accompanied by additional industry communications providing more detailed information on managing the implementation of GSC.

It provides the basic guidance and tips to work the new system, including a one-page summary of the key points on page A2.

Contents

Government Security Classification System - **Key points on One Page**

Why

- The change is being introduced on 2 April 2014 to enable a more flexible approach to security, while improving the security of government information by encouraging everyone to think more about how best to protect it.

What

- The old six classifications are reducing to three: OFFICIAL, SECRET, TOP SECRET.
- Nothing is changing about dealing with information at the level of SECRET and TOP SECRET.
- The old classifications of RESTRICTED, PROTECT and UNCLASSIFIED are no longer to be used.
- From April 2014, all information below SECRET will automatically be classified OFFICIAL.
- **Although there are important changes at the OFFICIAL level, none of these are particularly difficult.**
- Information classified with the old marking RESTRICTED does **not** need to be reclassified unless it is added to with new information – if not it should continue to be protected according to the previous rules.

How to Handle

- Unlike some other government departments, MOD policy is that MOD information below SECRET should not be routinely marked OFFICIAL unless it is sensitive – in which case it should be marked (as you would expect) OFFICIAL SENSITIVE; in some cases there may be a descriptor as well (see page A4 and A5). OFFICIAL SENSITIVE is a security marking, not a classification (which is OFFICIAL).
- Under GSC there is no such thing as UNCLASSIFIED information. Unmarked information is all OFFICIAL.
- OFFICIAL information without a security marking still needs to be protected. It may be shared with recipients in the UK (including over the internet) but only if there is no handling instruction against this. Also providing you have no reason to think it needs greater protection or have been advised otherwise by the MOD (for example if it contains private personal data). So you just need to think whether you are aware of any sensitivity; this is a matter of common sense. MOD OFFICIAL information should not be released to the public without the prior approval of the MOD Contracting Authority.
- MOD OFFICIAL SENSITIVE information should broadly be treated to the same standard as RESTRICTED information, with the important exception that subject to certain strict rules (pages A8 to A9) it can be sent unencrypted over the internet and even worked on using personal computers.

Government Security Classification (GSC) - **Some Common Questions**

Why are these changes being made?

- So that the government genuinely has a single, shared approach to classification – it has not until now.
- To provide a simpler system – in today's world we just don't need six categories of classification.
- To improve information security by encouraging individuals to take more personal responsibility for the security of the information they handle, particularly at the OFFICIAL level.

Surely all this change and personal judgement/discretion increases the risk to sensitive information?

- At the OFFICIAL level, any increased risk from relying on personal discretion (e.g. two people marking the same information differently) will over time be offset by the new business flexibilities GSC enables, and also its focus on individual understanding and responsibility.

What does it all mean for people on the ground?

- This change will affect everyone in the MOD and defence contractors, but the impact on most people will not be great.
- The main changes are to do with:
  - the way we think about classifying and marking information – see pages A5 to A6; and
  - the way we share and transmit OFFICIAL information, particularly over the internet - see pages A7 to A8.

Given the increased personal responsibility, what happens if there are breaches of security at OFFICIAL level?

- Within the MOD, individuals will be more personally accountable for information security under GSC.
- MOD looks to its Industry Partners to follow our principle of taking firm action if individuals:
  - have been careless or reckless with information they knew to be sensitive;
  - breach one of the clear mandatory rules (e.g. emailing MOD OFFICIAL SENSITIVE information unencrypted across the internet without the approval of the originator); or
  - deliberately compromising the information (e.g. passing government information to a journalist without authorisation).

So material can be sensitive but not security marked at all.

Yes. MOD's expectation is that over 80% of OFFICIAL information will not have a security marking. Some of this is bound to be sensitive to a degree – just not enough to pass the test for OFFICIAL SENSITIVE (see pages A6 to A7).

Remember: Handling instructions can be applied to documents that have no security marking, and can be very effective in protecting information that is sensitive (see page A4).

Why have both Security Markings and Handling Instructions?

Having OFFICIAL SENSITIVE as a recognised security marking (with pre-defined rules) allows significant amounts of sensitive information to be shared and protected consistently across MOD, the government and industry as a whole. Bespoke handling instructions allows individual documents to be given added, or different, protection if justified by their contents. Both are needed to protect OFFICIAL level information effectively and efficiently.

Government Security Classification (GSC) – **Understanding classification and marking**

All Government **information** (whether written down or not) is **classified**. Under the GSC, there are only three UK government classifications: TOP SECRET, SECRET or (if neither of these) OFFICIAL.

Some **documents** (including electronic documents) carry **security markings** to indicate the sensitivity of the information they contain. The following rules for applying security markings apply to standard documents, in both paper and electronic form (see page A7 for slightly different rules for emails).

- The **only** permitted security markings are: TOP SECRET, SECRET, and OFFICIAL SENSITIVE (which may or may not be followed by one of three authorised 'descriptors' indicating why it sensitive – COMMERCIAL (or COMRCL), LOCSEN, PERSONAL – see page A5).
- Security markings should appear (in full) at the very top and bottom of each page of the document.
- Apart from the three authorised 'descriptors' (see above) **no** additional wording is to be applied alongside the marking OFFICIAL SENSITIVE, but this can be added on the next line down – see below.

Documents at OFFICIAL level may carry prominent **handling instructions** if the author considers that this is necessary to protect sensitive information. The following rules apply to standard documents.

- Handling instructions (if used) should define how the author wishes the document to be protected, including limits on its distribution, transmission and/or storage. They should be clear, unambiguous and to the point.
- To avoid confusion with security markings, they should be clearly labelled as handling instructions, **not** be written in capitals, and appear only at the top of the document. You should avoid authorised wording for security markings, new or old.
- On documents marked OFFICIAL SENSITIVE, the handling instruction should appear on each page on the line immediately underneath the security marking at the top (only).
- On 'unmarked' OFFICIAL documents (i.e. those without the security marking OFFICIAL SENSITIVE), the handling instruction should appear on the top line (only) of each page.
- Examples of handling instructions:
  - *Handling Instruction: Not to be copied further without the author's approval.*
  - *Handling Instruction: Do not store on open computer folders or teamsites.*
  - *Handling Instruction: Not to be shared outside of recipient organisation.*

Classification and Marking Emails

- The security marking (if any) of an email is dictated by its content or that of any attachments. It should be recorded at the end of the title using the abbreviations: TS, S, OS, OS PERSONAL, OS LOCSEN, OS COMMERCIAL (or COMRCL). E.g.
  - *Discussions with Defence Industry – OS COMRCL.*
- Any handling instructions should be summarised, or at least referred to, in the email title; in the latter case the handling instruction should form the first line of the email. E.g.
  - *Discussions with Defence Industry – Handling Instruction applies – OS COMMERCIAL*. Followed by (on the first line of the email): *Handling Instruction: Not to be shared with industry until after [date].*

Government Security Classification (GSC) – **How to Classify Information**

Some things that the MOD Contracting Authority will think about when classifying information

As advised previously, defence contractors will classify material according to the aspects defined in the latest version of the contract SAL issued by the MOD. The following provides some guidance on how the MOD may determine the appropriate classification:

1. If information does not meet the tests for SECRET or TOP SECRET, then it is automatically **classified** as OFFICIAL.

2. Unlike some other departments, MOD policy is that OFFICIAL information should not be marked unless it is sensitive, in which case it should be **marked** OFFICIAL SENSITIVE. In some cases a **descriptor** can be used following this marking. The only allowed descriptors are COMMERCIAL, LOCSEN (location sensitive) and PERSONAL.

3. Things that will be considered by the MOD in deciding whether to mark information OFFICIAL SENSITIVE.

- Across the board, MOD would expect more than 80% of information to fall into the OFFICIAL category and therefore not be marked.
- If warned about the harm that could result from compromise to a foreign intelligence service or hostile forces, then it should probably not be classified OFFICIAL.
- What the potential harm is, and who poses the threat is not about following some vague instinct. The information should be looked at on its own, and not how a foreign intelligence service, terrorist organisation, or other 'threat actor' could put it together with other information obtained from different sources. Classification should not be driven by arguments based on 'what if everybody did this'.
- Consider if it were to come to light that the information had fallen into the into the wrong hands, would this lead to significant criticism of the MOD at the national level? If so, then a marking of OFFICIAL SENSITIVE is probably right.

Government Security Classification (GSC)
– **How to Classify Information**

These are the main principles to be taken into account:

1. All information needs to be protected according to its sensitivity, but equally it can and should be shared (within the rules below) where this is sensible and helps deliver Defence business.

2. Use judgement and common sense in storing, working on and sharing information.

3. Think who the information might be at risk from, and protect accordingly.

4. Occasionally, you may have grounds to think information is sensitive even if it is unmarked (for example if it includes private personal information). If so, treat it as OFFICIAL SENSITIVE and alert the originator to your concerns.

5. There are new flexibilities in sharing OFFICIAL information, which can be used if this helps deliver business more effectively.

Handling MOD OFFICIAL information

Unless you have reason to believe, or have been notified by the MOD Contracting Authority, that the content is sensitive (for example if it includes private personal information), documents or emails that have originated within the MOD and have no marking can be:

- emailed freely within the company.
- emailed unencrypted over the internet to third parties, provided you ensure that they understand any limitations that the MOD has determined needs to be applied to publication or further circulation of the information.
- discussed freely on all types of phone.
- physically taken and worked on at home and in public places.
- left unsecured when you leave your place of work, unless you judge this inappropriate (use common sense) or your business area has a 'clear desk' policy.
- disposed of in normal waste/recycling bins at work or at home.

If you are not sure whether the information is sensitive or not, you should treat as if it were OFFICIAL SENSITIVE and seek advice from the MOD Contracting Authority.

Government Security Classification (GSC)
– **Working with OFFICIAL Information**

Handling OFFICIAL SENSITIVE information

Physical documents or emails with the OFFICIAL SENSITIVE marking must be:

- locked in a secure container when not in use or you leave your place of work for more than half an hour.
- disposed of in a manner to make reconstruction unlikely, for example by shredding or burning.

They can be:

- emailed within the company and to the MOD across secure systems including the RLI and GSI.
- **on an exceptional basis,** emailed over the internet to third parties provided there is a business need, and subject to the prior approval of the MOD Contracting Authority (see page A8).
- physically taken and worked on at non-company locations but not read or worked on in public or otherwise in the sight of unauthorised people.
- discussed on all types of phone, but not with (or within earshot of) unauthorised persons.
- There are special rules for OFFICIAL SENSITIVE information released to international partners and overseas contractors. Overseas, OFFICIAL SENSITIVE will be handled to the standards applied to the recipients' RESTRICTED information. The approval of the MOD Contracting Authority is required prior to its release. Where the release is a consequence of a sub-contract, the request for approval should be in accordance with the process described in the OFFICIAL SENSITIVE Contract Security Condition.
- Security Aspects Letters (SALs) issued by the MOD Contracting Authority will define the specific nationally classified OFFICIAL SENSITIVE aspects of the contract. SALs however will not be issued where the contract involves OFFICIAL SENSITIVE - COMMERCIAL information, where the sensitivity is only of a purely commercial nature e.g. pricing.

Finally, if following the marking of OFFICIAL SENSITIVE there is also a descriptor, the information must be stored electronically in locked down IT folders where access to it is limited to only those persons authorised to have such access.

Top Tips

- **If you treat MOD OFFICIAL SENSITIVE material as you used to treat RESTRICTED material you will avoid security breaches. But remember the two are not the same and there are new flexibilities you can use if this helps deliver your business.**
- **If in doubt about any aspect of handling MOD OFFICIAL information, protect it as if it were RESTRICTED and seek early guidance from the MOD Contracting Authority.**

Sending MOD OFFICIAL SENSITIVE information unencrypted over the internet

- This will be permitted to recipients located in the UK, but only in **exceptional circumstances.** By definition, material with this marking needs careful protection and there is a risk that it could be compromised if transmitted unencrypted over the internet.
- However, internet transmission can be allowed provided there is a demonstrable and pressing business benefit, steps are taken to minimise the risk, and certain rules are followed:
  - there is no reasonable alternative and more secure means of achieving the business benefit.
  - the MOD Contracting Authority has given prior approval and when it is known that the intended recipient has been made aware of, and will comply with the requirements to protect MOD OFFICIAL SENSITIVE information .
  - there is also appropriate company authorisation, normally by your Senior line manager.
  - the covering email makes clear what the recipient can and can't do with the information, and you must have confidence that this will be followed.
  - you must not send private personal information (in practice details going beyond standard information on a business card) without the person's agreement.
- OFFICIAL SENSITIVE information must NOT be transmitted unencrypted to recipients located overseas as international partners will treat such information to their standards for national RESTRICTED information which does not permit transmission in clear text.
- If you receive MOD OFFICIAL SENSITIVE information over the internet you should ensure that it is handled in accordance with the provisions detailed on page A7. You should not assume that you may send it over the internet to a third party. To do so requires the prior approval as described above.

- **Top Tip: Think before you press send.** If the information you are about to email is compromised you will be asked to account for your actions and judgements and prove that you had the required approvals to send it this way. Are you sure you have identified the benefits, weighed the risks and followed the rules?

Government Security Classification (GSC) – **Working with OFFICIAL Information**

GSC on the GOV.UK website:

https://www.gov.uk/government/publications/government-security-classifications

Working on MOD OFFICIAL information on personally owned computers

- One of the aims of GSC is to help people work more flexibly if they want to and if there is a business need.
- Some people may wish to work on MOD OFFICIAL information at home. Ideally this should be done on company issued and accredited Computer Information Systems but there will be times when this is not possible, and people may wish to work on MOD OFFICIAL information on personal computers or tablets.
- Under GSC, this will be allowed on an exceptional basis.
- The main rule is that this does not become 'routine'; that there is always a clear business need, that produced or amended information is returned to the individual's office within 5 days, and that the information and emails are deleted immediately thereafter, as fully as possible, from your personal machine (in case it is stolen or hacked).
- **If the information is marked OFFICIAL SENSITIVE, even tighter rules will apply.** The main ones will be that:
  - there must be an exceptional compelling business need and the MOD Contracting Authority has given its prior approval in writing.
  - the user's personal computer is compliant with the criteria in the MOD OFFICIAL SENSITIVE Contract Security Condition.
  - the rules for emailing such material (see page A8 to A10) must be followed.
  - you must not process someone else's personal information on your personal computer without their explicit permission.
- There are liabilities on anyone wishing to use personal devices for working on OFFICIAL documents.
  - You must report if your device is lost, stolen, or if you have reason to believe it has been hacked.
  - Before disposing of the device (by sale or destruction) the internal storage must be wiped thoroughly: this is sensible practice in order to remove your own private personal information.
- Remember, if the information is compromised (e.g. if the device is stolen) you are accountable for how it was handled.

Working with 'legacy' information

- Information from before April 2014 with the markings PROTECT, or RESTRICTED should be protected under the old rules (which remain valid for this purpose).
- Existing information does not need to be reclassified unless it is amended or incorporated into new material.
- If circulating material with legacy markings, any covering paper/emails should be marked (or not) according to the new GSC system.
- Unmarked legacy material, or material marked UNCLASSIFIED should be treated as if it were OFFICIAL, with no security marking. If it is emailed over the internet, any UNCLASSIFIED marking should be removed if possible, but this is not mandatory.

GSC Summary Table

GSC Classifications Information (whether written or not) can only be classified three ways	**Security Marking** The list below shows all the allowable security markings for documents. Documents may also have handling instructions (**see page 5**)	**DOs, DON'Ts and MAYs**	**How it's Different**
OFFICIAL Government information that does not meet the tests for SECRET or TOP SECRET is automatically classified OFFICIAL. In MOD there are three Marking Options for what appears at the top of an OFFICIAL document.	**No Security Marking** - Any information that doesn't meet the test for OFFICIAL SENSITIVE. Over 80% of MOD OFFICIAL material is expected not to be marked, including material that is sensitive to a degree, but not enough to justify OFFICIAL SENSITIVE (see page A6). - Some other Departments will mark such information OFFICIAL.	**DO** – remember that unmarked information may still be sensitive and give it the protection you think it merits. And respect any handling instructions which have been added. **DON'T** assume that it can be freely shared just because it isn't marked. Think: Is it sensitive? Does it need protecting? Against what? How? Provided you do this, you **MAY:** ● Share it with people inside your company facility ● Email it to third parties over the internet or discuss it on any phone. ● Remove it from company premises. ● Dispose of it with normal waste. ● Work on it on personal computers, subject to certain rules – see page A9.	- Under GSC, there is no such thing as UNCLASSIFIED information. It's all OFFICIAL. - Documents without a security marking or handling instruction may still be sensitive and need protection. - If you fail to take reasonable care of information, it will not be a defence simply to argue it was unmarked.
	Marked: **OFFICIAL SENSITIVE** Information which in the wrong hands could cause significant harm to the work or reputation of Defence or the government more widely. Useful test – could its loss lead to significant criticism of MOD at the national level? (see page A6).	**DO** – give it appropriate protection and comply with the handling rules. But always think whether it may need stronger protection. For example, **DON'T** – circulate it internally to more people than really need to see it. If you follow the appropriate rules you **MAY:** ● Share it with people inside and outside company facility on secure systems. ● Discuss it on any phone, but not within earshot of unauthorised persons. ● Remove it from company premises, provided you take care to ensure it is not seen by unauthorised persons. ● Subject to certain strict conditions and approvals, email it over the internet and work on it on personal computers.	- OFFICIAL SENSITIVE information is similar to the old RESTRICTED, but there are significant differences. - In particular, it is permitted, subject to certain strict rules, to email it over the internet and work on it on personal computers.
	Marked: **OFFICIAL SENSITIVE** Plus one or more of the following permitted 'descriptors' (see page A4) **COMMERCIAL (or CMRCL), LOCSEN, PERSONAL**	As for OFFICIAL SENSITIVE, but there are tight restrictions on emailing sensitive personal information over the internet and working on it on personal computers.	As for OFFICIAL SENSITIVE

Sponsored by DBR-DefSy-STIndAH

Published by the Ministry of Defence UK

Designed by DMC Secretariat Graphics
Ref: DMC00716 13/14

Reportable OFFICIAL and OFFICIAL- SENSITIVE Security Condition for UK Contracts

Definitions

1. The term "Authority" means a Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.

Security Grading

2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL-SENSITIVE and Reportable OFFICIAL information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL-SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL-SENSITIVE classification. However, the Contractor is not required to mark information/material related to the contract which is only OFFICIAL.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of Reportable OFFICIAL and OFFICIAL-SENSITIVE Information

4. The Contractor shall protect Reportable OFFICIAL and OFFICIAL-SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. Reportable OFFICIAL and OFFICIAL-SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

6. All OFFICIAL-SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL-SENSITIVE documents/material shall be stored under lock and key. As a minimum, when not in use, OFFICIAL SENSITIVE material shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

7. Disclosure of OFFICIAL-SENSITIVE information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

8. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 30.

Access

9. Access to Reportable OFFICIAL and OFFICIAL-SENSITIVE information shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of his or her duties.

10. The Contractor shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the Gov.UK website at: https://www.gov.uk/government/publications/security-policy-framework.

Hard Copy Distribution of Information

11. Reportable OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in a single envelope. The words Reportable OFFICIAL or OFFICIAL-SENSITIVE shall **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent.

12. Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

13. Reportable OFFICIAL information may be emailed unencrypted to recipients over the internet when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions. OFFICIAL-SENSITIVE information shall be emailed unencrypted over the internet **only** where there is a strong business need to do so and only with the **prior** approval of the Authority. It shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

14. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot of) unauthorised persons.

15. OFFICIAL-SENSITIVE information may be faxed to UK recipients.

16. Reportable OFFICIAL information may be discussed with and faxed to recipients located overseas.

Use of Information Systems

17. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

18. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

19. The following describes the minimum security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.

a. Access Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of "least privilege" will be applied to System Administrators. Users of the IT System (Administrators should not conduct 'standard' User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems shall have the following functionality:

1. (1) Up-to-date lists of authorised users.

2. (2) Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most ID&A, Security Measures. Passwords shall be 'strong' using an appropriate method to achieve this, for example including numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, OFFICIAL-SENSITIVE information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the UK MOD. Advice on encryption requirements for the transmission of OFFICIAL-SENSITIVE information shall be sought from MOD CIO-InfoSy Pol via the Authority.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

I. All log on attempts whether successful or failed.

II. Log off (including time out where applicable).

III. The creation, deletion or alteration of access rights and privileges.

IV. The creation, deletion or alteration of passwords.

3. (2) For each of the events listed above, the following information is to be recorded:

I. Type of event,

II. User ID,

III. Date & Time

IV. Device ID

4. The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

5. If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures shall be implemented:

1. Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)

2. Defined Business Contingency Plan

3. Data backup with local storage

4. Anti Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).

5. Operating systems, applications and firmware should be supported

6. Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

h. Logon Banners Wherever possible, a "Logon Banner" shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

A suggested format for the text depending on national legal requirements could be:

(a) "Unauthorised access to this computer system may constitute a criminal offence"

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems shall not be connected direct to the Internet or 'untrusted' systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority's Principal Security Advisor.

k. Disposal Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

Laptops

20. Laptops holding any MOD supplied or contractor generated Reportable OFFICIAL and OFFICIAL-SENSITIVE information are to be encrypted using a Foundation Grade product equivalent, for example FIPS 140-2 approved full disk encryption.

21. Unencrypted laptops not on a secure site[4] are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

22. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

23. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and Incident Reporting

24. The contractor shall immediately report any loss or otherwise compromise of Reportable OFFICIAL and OFFICIAL-SENSITIVE information to the Authority.

25. Any security incident involving any MOD owned, processed, or contractor generated Reportable OFFICIAL or `OFFICIAL-SENSITIVE information defined in the contract Security Aspects Letter shall be immediately reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC). This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the MOD's Chief Information Officer (CIO) and, as appropriate, the

[4] Secure Sites are defined as either Government premises or a secured office on the contractor premises

company concerned. The MOD WARP will also advise the contractor what further action is required to be undertaken.

JSyCC WARP Contact Details

Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations
Email: For those without access to the RLI: CIO-DSAS-JSyCCOperations@mod.uk
Telephone: Working Hours: 030 677 021 187
Out of Hours/Duty Officer Phone: 07768 558863
Fax: 01480 446328
Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton, Huntingdon, Cambs PE28 2EA.

Sub-Contracts

26. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom notifying the Authority. When sub-contracting to a Sub-contractor located in the UK the Contractor shall ensure that these Security Conditions shall be incorporated within the Sub-contract document. The **prior** approval of the Authority shall be obtained should the Contractor wish to Sub-contract any Reportable OFFICIAL or OFFICIAL-SENSITIVE elements of the Contract to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 form can be found at):
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229422/Contractual_process_-_v6.1_April_2013.pdf.

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

Publicity Material

27. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the MOD, Services or any other government department.

Private Venture

28. Any defence related Private Venture derived from the activities of this Contract are to be formally assessed by the Authority for determination of its appropriate classification. Contractors are to submit a definitive product specification to DBR-DefSy(S&T/Ind) for PV Security Grading in accordance with the requirement detailed at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27647/pv_grading_flyer_v5.pdf

Promotions and Potential Export Sales

29. Contractors wishing to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIAL-SENSITIVE (including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment) are to obtain the prior approval of the Authority utilising the MOD Form 680 process, as identified at: https://www.gov.uk/mod-f680-applications.

Destruction

30. As soon as no longer required, Reportable OFFICIAL and OFFICIAL-SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely , for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the

Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

31. Advice regarding the interpretation of the above requirements should be sought from the Authority.

32. Further requirements, advice and guidance for the protection of MOD information at the level of Reportable OFFICIAL and OFFICIAL-SENSITIVE may be found in Industry Security Notices at: https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

33. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Authority to ensure compliance with these requirements.

Appendix 5

APPLICATION TO SUB-CONTRACT OR COLLABORATE WITH AN OVERSEAS CONTRACTOR ON WORK INVOLVING OFFICIAL-SENSITIVE AND ABOVE CLASSIFIED INFORMATION (ALSO KNOWN AS F1686)

Request:

1	From: full name and address of contractor submitting application Telephone no: Email:
2	Full name and address of selected overseas sub-contractor where work will be undertaken
3	Maximum level of classified material to be released to or produced by the sub-contractor:
4	Description of work to be carried out:
5	Name of Project/Reference Number of prime contract:
6	Full name of point of contact and address of United Kingdom Contracting Authority: Telephone no: Email:

Name: Position in company

Signature: …….. Date:

Response from Contracting Authority:

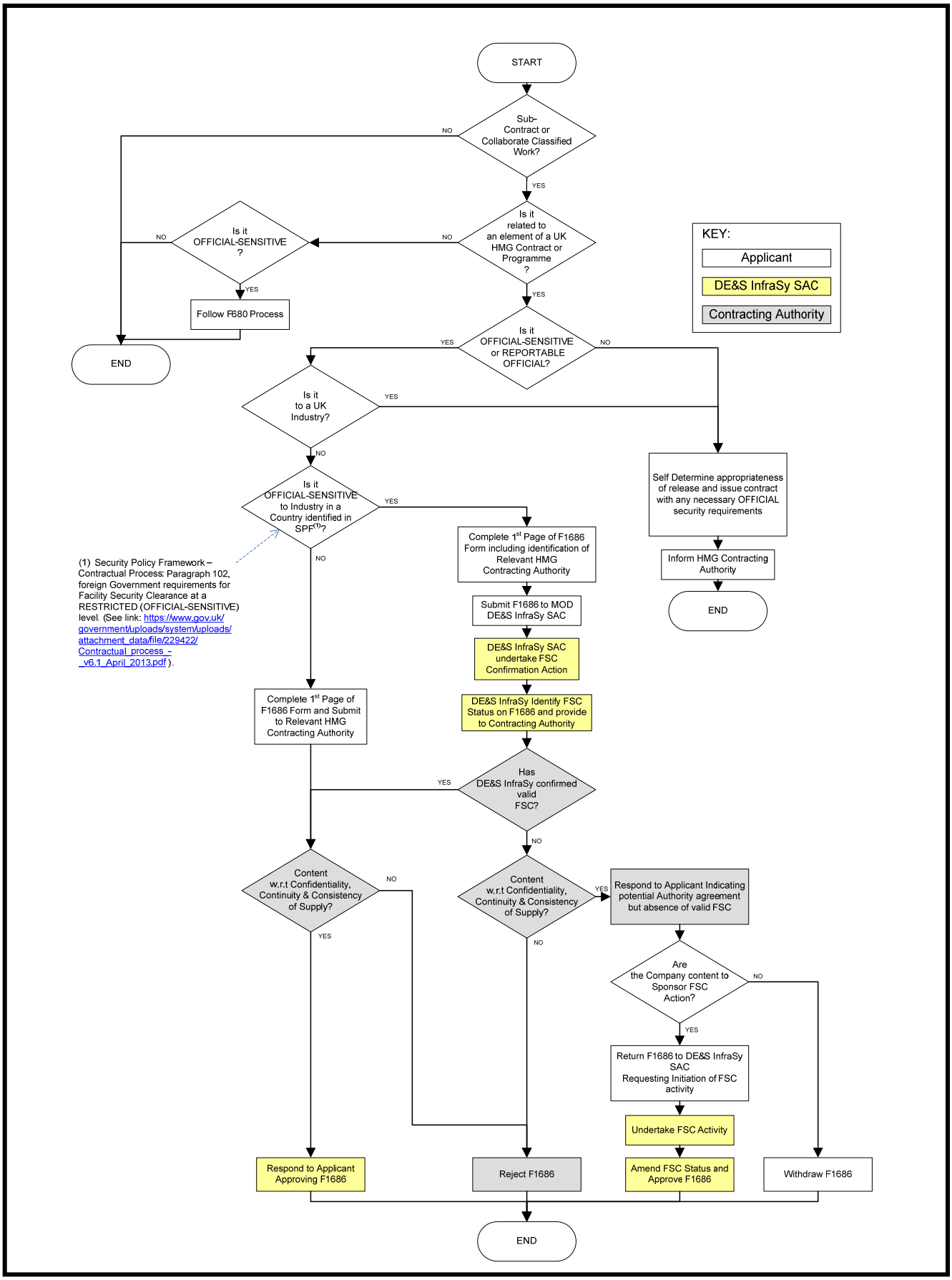
Approval is / is not granted[5] to place the sub-contract detailed above. Further information is attached.[6]

Name: Position/Title:

Signature: …… Date:

Contracting Authority Organisation:

[5] Delete as appropriate
[6] Delete if not applicable


START
Sub-Contract or Collaborate Classified Work?
NO
YES
Is it related to an element of a UK HMG Contract or Programme ?
NO
YES
Is it OFFICIAL-SENSITIVE ?
NO
YES
Follow F680 Process
END
KEY:
Applicant
DE&S InfraSy SAC
Contracting Authority
Is it OFFICIAL-SENSITIVE or REPORTABLE OFFICIAL?
YES
NO
Is it to a UK Industry?
YES
NO
Self Determine appropriateness of release and issue contract with any necessary OFFICIAL security requirements
Inform HMG Contracting Authority
END
Is it OFFICIAL-SENSITIVE to Industry in a Country identified in SPF(1)?
YES
NO
(1) Security Policy Framework – Contractual Process: Paragraph 102, foreign Government requirements for Facility Security Clearance at a RESTRICTED (OFFICIAL-SENSITIVE) level. (See link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229422/Contractual_process_-_v6.1_April_2013.pdf).
Complete 1st Page of F1686 Form including identification of Relevant HMG Contracting Authority
Submit F1686 to MOD DE&S InfraSy SAC
DE&S InfraSy SAC undertake FSC Confirmation Action
DE&S InfraSy Identify FSC Status on F1686 and provide to Contracting Authority
Complete 1st Page of F1686 Form and Submit to Relevant HMG Contracting Authority
Has DE&S InfraSy confirmed valid FSC?
YES
NO
Content w.r.t Confidentiality, Continuity & Consistency of Supply?
NO
YES
Content w.r.t Confidentiality, Continuity & Consistency of Supply?
YES
NO
Respond to Applicant Indicating potential Authority agreement but absence of valid FSC
Are the Company content to Sponsor FSC Action?
NO
YES
Return F1686 to DE&S InfraSy SAC Requesting Initiation of FSC activity
Undertake FSC Activity
Amend FSC Status and Approve F1686
Withdraw F1686
Respond to Applicant Approving F1686
Reject F1686
END

Minimum requirements for protecting international RESTRICTED classified information

Personnel security and access control

Personnel Security Clearance	BPSS is not required for access to international RESTRICTED. Need to know principle applies.
Nationality considerations	Nationality to be considered before authorising access to nationals from a non-Member State (for NATO, EU and ESA) and third State nationals (for GSAs).
Briefing and Awareness training	• Briefing and awareness training required to ensure international classified information is appropriately protected. • NATO and EU - Individuals to acknowledge their security responsibilities in writing
Visits involving international classified information	Visits requiring access to international classified information shall be undertaken in accordance with the relevant international regulations or Security Agreements.

Physical Security

Physical protection for handling international classified assets	• Handled in a facility to which access is controlled and in a manner which prevents unauthorised access. • Individuals not authorised to have access will be escorted or subject to equivalent controls.
Physical measures for storing international classified assets	Stored in suitable lockable office furniture when not in use.
Discussing in public	Not to be discussed in public.
Discussing in offices	Only discuss in areas where individuals without the need to know cannot overhear.
TEMPEST measures	No controls required.
Requirement for a Facility Security Clearance (FSC) for contractors	No requirement.

Information management

Marking of international classified information	International RESTRICTED classified information shall not be remarked with the marking UK “OFFICIAL-SENSITIVE” classification upon receipt.
Contractors producing international classified information	Organisations producing international partner classified information shall assign the classification in accordance with the provisions contained in the Security Classification Guide or Security Aspects Letter.
Use of international classified assets	The recipient shall only use international classified information for the purpose for which it was provided or otherwise as authorised by the international partner.
Copying of physical documents	Reproductions shall be limited to the minimum required for an official purpose, and shall be made only by individuals with a need to know.
Translation of documents	Translations shall be made only by individuals with an appropriate PSC and a need to know. Translations must contain a suitable annotation indicating that they contain classified information of the providing international partner, and be marked with the same classification level as the original.
Registration of physical documents	Not required.
Physical carriage within a building or self-contained group of buildings	Covered from view by a single cover (e.g. opaque envelope or folder).
Physical transmission of classified information within the UK, or overseas to a NATO, EU, ESA Member State, or a nation with which the UK has an General Security Agreement or Security Arrangement	National post, commercial courier service, diplomatic channels/military courier, or authorised personal hand carriage.
Physical transmission of classified information to a nation that is not a NATO, EU or ESA Member State or a nation with which the UK does not a General Security Agreement or Security Arrangement	National post, commercial courier service, diplomatic channels/military courier, or authorised personal hand carriage.
Packaging to be used when sending information within the UK or overseas	Two opaque envelopes or other suitable packing material to be used.
Destruction of physical assets	Destroyed in such a manner that ensures it cannot be reconstructed.

Security Incident - Breach	Security breaches must be investigated and reported to the Departmental Security Officer (DSO) in accordance with internal departmental security procedures. Significant security breaches that may lead to compromise may need to be reported by the DSO to the UK National Security Authority (UK NSA) by the DSO.
Security Incident - Compromise	Suspected or actual compromise to be investigated and reported to the DSO in accordance with internal departmental security procedures. The incident must be reported to UK NSA.
Security Incidents on List X premises	• Security incidents must be investigated and reported to the Facility Security Officer, who will report this to the Security Controller. • Significant security breaches that may lead to compromise must be reported to the UK NSA. • Suspected or actual compromise must be reported to the UK NSA.
Security Incidents on Non-List X premises	• Security incidents must be investigated and reported to the Security Officer, who will report this to the contracting authority. • Significant security breaches that may lead to compromise must be reported to the UK NSA.

Information Assurance

Discussing international classified information over unsecure phone lines	International classified information is not to be discussed on an unsecure phone or mobile line.
Handling and storing on ICT systems	• Must not use unauthorised ICT (e.g. personal devices). • UK ICT used that is approved by HMG to protect UK OFFICIAL-SENSITIVE. • NATO/EU/ESA – Can use an ICT approved by that international organisation.
ICT accreditation	• Accreditation has taken into account any additional threats or increased risks involved in handling international classified information. • NATO/EU/ESA - Accreditation must be compliant with the relevant security regulations and security policies of the international organisation. • Generally, the application of self Accreditation under defined criteria specified in the contract or other documentation will apply.
Sending classified information by email over UK accredited network	Where a cryptographic product is used, it must be CESG approved (CPA or CAPS Baseline), or approved by the international organisation/foreign government concerned.
Sending classified information by email over public networks or un-trusted networks	Must be encrypted with a CESG approved cryptographic product (CPA or CAPS Baseline) or a cryptographic product approved by the international organisation/foreign government concerned.
Handling and storing on removable media (e.g. CD, USB stick)	No mandatory requirement to encrypt. If encrypted, then UK holder must comply with the requirements above for encryption. If not encrypted, UK must handle and protect removable media in same manner as a physical document with same marking. In the latter case enhanced controls must be considered given the large amount of data that removable media can hold.
Reuse, downgrading or disposal of computer storage media	• Foreign Government - Computer storage media, which includes removable media, that has held foreign government classified information can be reused or disposed of in accordance with national policy. • NATO/EU/ESA – Refer to organisations security regulations.

Disclosure

Disclosure of international classified information to the public	UK holders of international classified information shall seek the prior written authorisation from the originator if they want to release this information to the public. If the originator grants written permission then release is permitted, but if the originator declines this must be respected by the UK.
Disclosure of international classified information to a Third Party	UK holders of international classified information shall seek the prior written authorisation from the originator if they want to release this information to a Third Party. If the originator grants written permission then release is permitted, but if the originator declines this must be respected by the UK.