Cabinet Office

International Classified Exchanges

Version 1.5 – March 2020

Contents

Summary

1. This document is a high level summary of how the UK protects international partners' classified information, and how the UK can exchange HMG classified information with international partners. This document also sets out the various roles, functions and responsibilities of HMG organisations and UK contractors.

2. Separate guidance is also available on gov.uk for those organisations that will handle only international RESTRICTED classified information and no higher.

Section 1: Roles and functions

3. International Organisations, as well as some treaty obligations, require nations to fulfil various roles and functions in order to ensure classified information exchanged between them is protected to agreed minimum standards.

UK National Security Authority

4. Several International Organisations, multilateral fora, and bilateral agreements all require that nations establish a National Security Authority (NSA). The NSA is the Government Authority in a nation with ultimate responsibility for the protection of classified information exchanged internationally. For the UK, the Government Security Group (GSG) in the Cabinet Office is the UK NSA.

Competent Security Authorities and Designated Security Authorities

5. Although the Cabinet Office is designated as the UK NSA, HMG departments and agencies remain individually responsible for the security of the international classified information they and their contractors hold.

6. In various agreements and arrangements the term 'Competent Security Authority' (CSA) is often used. CSAs are responsible for implementing the security measures required to protect classified information held by their organisation. For the UK CSAs are generally considered to be the Senior Security Advisers (SSAs) or Security Advisers (SAs) for HMG departments and agencies, though certain CSA functions can be delegated to other units within organisations.

7. 'Designated Security Authority' (DSA) is another term used internationally, and generally means the primary Security Authority in a nation responsible for industrial security. In the UK there is only one DSA, and that is based in the Ministry of Defence.

Information Assurance

8. The NCSC is the National Crypto Approval Authority (CAA), the National Communication and Information System Security Authority (NCSA) and the National TEMPEST Authority (TA) for the UK.

Section 2: International security obligations

9. HMG is party to various international security agreements and arrangements covering the handling of classified material originated by International Organisations, foreign governments and contractors working on behalf of those government/organisations, including reciprocal arrangements for HMG classified assets provided to those partners. These agreements and arrangements commit the parties to apply mutually agreed security standards for the protection of classified information.

Security Agreements

10. General Security Agreements are legally binding treaties negotiated by the Cabinet Office, as UK NSA, with the support and assistance of relevant HMG organisations. These Agreements apply across HMG, and set out the common minimum standards for the mutual protection of all classified information exchanged between the two governments and their contractors.

11. General Security Agreements are predicated on the understanding that each party will afford the other party's classified information a similar or acceptable level of protection as it gives to its own information at the corresponding level of classification. A list of General Security Agreements can be found in Annex A of this document.

12. Defence Security Arrangements are similar to General Security Agreements in the provisions they include, but are negotiated by the Ministry of Defence and are limited to the protection of defence classified information exchanged between the participants and defence contractors. Such arrangements often have the status of a Memorandum of Understanding (MOU).

International Organisations

13. The UK is required to protect classified information generated by NATO, ESA and other International Organisations to agreed security standards.

14. The security controls and requirements for protecting International Organisation classified information are closely aligned to UK requirements at the equivalent level. HMG organisations and contractors that are required to handle International Organisation classified information should consult Annex B of this document in order to ensure compliance.

Section 3: International Personnel Security

15. This section should be read in conjunction with HMG Personnel Security Controls on gov.uk.

HMG personnel security roles and responsibilities

16. HMG organisations are responsible, through their respective Cluster services, for managing the vetting process to allow their staff and contractors access to UK classified information. Responsibility for providing clearances for their staff and contractors requiring access to international classified assets similarly rests with that employing parent HMG organisation.

17. International Organisations require their staff and contractors to be security cleared when handling classified information at the level CONFIDENTIAL and above. Under international security obligations it is usually the parent nation of the individual that is required to undertake the Personnel Security Clearance (PSC), though occasionally the host nation can consider this.

UK NSA role in international Personnel Security Clearance requests

18. For British nationals working for International Organisations, or as contractors under classified contract, the UK NSA normally acts as the first point of contact for PSC enquiries and requests, although the actual vetting is undertaken by the Foreign & Commonwealth Office or Ministry of Defence through UK Security Vetting (UKSV). The process to follow for requesting PSCs for international purposes is set out in separate guidance on gov.uk.

Personnel Security Clearances required for access to international classified information

19. Access to international classified information at the level CONFIDENTIAL or above requires an individual to hold a valid PSC. The UK has two levels of National Security Vetting which permit access to international classified information. These are:

- **Security Check (SC)** – Permits access to international classified information up to and including the level of international SECRET.
- **Developed Vetting (DV)** – Permits access to international classified information up to and including the level of international TOP SECRET.

20. National Security Vetting can only be carried out in respect of an individual who has a genuine and confirmed requirement to access classified information in order to fulfil their duties. There also has to be a specific obligation under international treaties or arrangements for HMG to consider vetting.

21. Following on from the previous paragraph, any request for a PSC must be accompanied by an official confirmation from the requesting security authority that clearly

sets out the requirement for the PSC. Speculative vetting requests, requests made directly by the subject of the proposed vetting, requests from organisations without the necessary confirmation of a PSC being required, and requests outside the scope of international treaties or arrangements cannot be accepted by HMG.

Nationality Considerations

22. Dual nationality and non-British nationality will need to be taken into account before access to international classified information at the level of CONFIDENTIAL or above is permitted. Dual nationals, where one of the nationalities is British[1], may be granted access to international partners' classified information without prior approval from that partner provided there is no actual or potential conflict of loyalty.

23. Access to international CONFIDENTIAL or SECRET classified information by non-British nationals, or by individuals not holding the nationality of the country of the international partner whose classified information is to be accessed, usually requires the prior written approval of that partner.

24. For access to international partners' classified information at the level of RESTRICTED no nationality restrictions are mandated. However, HMG organisations and contractors will need to be mindful of any potential nationality sensitivities and third party transfer restrictions before authorising access to nationals from a non-Member State (for NATO and ESA information) or nationals from a third State (for General Security Agreements and other information sharing agreements).

NATO and ESA Personnel Security Clearance Certificates

25. PSC Certificates (PSCCs) are documents that may be required by NATO or ESA to verify that an individual has a PSC and has been authorised access to NATO or ESA classified information. PSCCs are only required for access to NATO or ESA classified information at the level of CONFIDENTIAL or above.

26. PSCCs can only be issued by HMG where a subject holds a current SC or DV clearance, and would only be issued in the following instances:

a. HMG organisation or UK contractor personnel who are required to attend NATO or ESA classified meetings;

b. Registry staff handling NATO classified information;

c. HMG officials seconded to NATO or ESA establishments who require access to that organisation's classified information;

d. Individuals hired directly by NATO or ESA, or contractors working for these organisations, who require access to the classified information of that organisation.

[1] http://www.legislation.gov.uk/ukpga/1981/61/contents

27. PSCCs are issued by the HMG organisation which granted the SC or DV clearance. Individual staff and contractors are not permitted to issue PSCCs themselves. Therefore if staff or contractor personnel require a PSCC (as set out in the previous paragraph) they must approach the HMG organisation that granted their SC or DV clearance.

Section 4: General principles for protecting international information

28. Any international UNCLASSIFIED information provided to the UK will need to be protected in accordance with the security controls for the OFFICIAL tier. Unless specifically authorised by the originator this information will not be disclosed to a third party or made public.

29. The UK will only use international classified information for the purpose for which it was provided, unless otherwise authorised by the originator. International classified information in the UK's possession needs to be protected to the corresponding national classification level as set out in the table below:

International classification marking	UK to handle and protect as:
International TOP SECRET	UK TOP SECRET
International SECRET	UK SECRET
International CONFIDENTIAL	UK SECRET
International RESTRICTED	UK OFFICIAL-SENSITIVE

30. Any international RESTRICTED classified information provided to HMG organisations and UK contractors will need to be protected in accordance with the appropriate security controls required to protect OFFICIAL classified information bearing the 'SENSITIVE' caveat (i.e. OFFICIAL-SENSITIVE). That being the case, the UK's obligations to safeguard international RESTRICTED classified information to an agreed and consistent standard may mean that the security controls have to be augmented in certain respects. Annex B sets out the minimum controls to be met by HMG organisations and UK contractors, but the main international RESTRICTED controls to note that are different from OFFICIAL are:

- Cryptographic products used to protect international RESTRICTED classified information must either be NCSC approved or been approved by the other international partner in question.
- International RESTRICTED classified information will not be transmitted over an unaccredited ICT system (e.g. over the open internet) without using an approved cryptographic product or approved secure mechanisms.
- International RESTRICTED classified information cannot be discussed in public areas, over non-secure phone lines, or transmitted over open fax lines.

31. UK entities that will only handle international RESTRICTED classified information and no higher are encouraged to read separate guidance available on gov.uk.

32. HMG does not have a CONFIDENTIAL level under the Government Security Classifications policy. Any information provided to the UK at the international CONFIDENTIAL level will generally be handled and protected by the UK as it does nationally for SECRET. In doing so, UK organisations should be mindful not to take actions that would have unintended consequences for international partners (e.g. requesting an international partner to hold a SECRET level PSC to access their own CONFIDENTIAL material).

33. HMG's security controls for the SECRET tier are largely aligned with the controls required to protect international SECRET classified information, but there are some specific requirements which do differ from UK policy. Annex B sets out the minimum controls to be applied by the UK when handling international SECRET classified information.

34. International TOP SECRET classified information will be handled as HMG would its own TOP SECRET, but certain additional measures will be applied in particular circumstances. Annex B sets out the minimum controls to be applied by the UK when handling international TOP SECRET classified information.

Legal framework

35. The Government Security Classifications policy operates within the framework of domestic law. The most relevant legislation concerning the protection of international classified information provided to the UK is the Official Secrets Act 1989. Section 3 of that Act states that an offence has been committed if a damaging disclosure is made of any confidential information, document or other article obtained from a third State or an International Organisation.

36. Other relevant legislation to consider when handling and protecting international partners' classified information is the Freedom of Information Act 2000, General Data Protection Regulation 2018 and Public Records Act 1967.

Audits and inspections

37. HMG organisations and contractors holding international classified information must be inspected regularly by their security officers to ensure that the information is protected in accordance with HMG policy and any other applicable security regulations. In addition, HMG organisations and contractors handling international classified information at the level of CONFIDENTIAL or higher must also ensure that holdings of this information are audited regularly.

Security incidents

38. UK entities must investigate any case where it is known, or there are reasonable grounds for suspecting, that classified information owned and/or provided by an international partner is the subject of a security breach, loss or compromise.

39. Significant security breaches that may lead to compromise of international classified information, or a security incident where suspected or actual compromise of international classified information has occurred, must be reported to the UK NSA.

Section 5: Providing HMG classified assets to international partners

40. HMG classified assets (i.e. UK classified information) should only be provided to International Organisations, foreign governments, and their commercial or industrial entities, in cases where:

a. There is a demonstrable business requirement to provide HMG assets to the international partner;

b. The intended recipient has a clear Need to Know;

c. The originator of the HMG assets to be provided has given their prior consent;

d. The international partner has the ability and willingness to protect UK classified information; and

e. Appropriate protective security arrangements are agreed with the recipient.

41. Any decision to provide HMG classified assets to an international partner must be taken on a risk management basis. Unless contractual clauses say otherwise, contractors that have a requirement to release HMG classified assets overseas usually will need to obtain the prior approval of the relevant HMG organisation.

42. OFFICIAL will be handled by international partners as they would unclassified information under their system. Although HMG accepts that international partners will treat OFFICIAL as unclassified under their respective classification systems this information should not be released to the public or to third parties unless the UK originator has given its consent.

43. In general terms, any HMG classified assets provided to international partners would be handled and protected as follows :

UK classification marking	International classification marking
UK TOP SECRET	International TOP SECRET
UK SECRET	International SECRET
UK OFFICIAL-SENSITIVE	International RESTRICTED

44. All HMG assets marked OFFICIAL-SENSITIVE, SECRET or TOP SECRET sent to international partners must include the ‘UK’ prefix. Providers of HMG classified assets may also want to apply a suitable caveat setting out any conditions for release. An example of both the prefix and conditions for release caveat follows:

UK SECRET
This information has been communicated in confidence to [the receiving government] and should not be released without the prior written agreement of the UK Government

45. When HMG classified assets are provided to international partners the most appropriate secure transportation or transmission method should be used, depending on the urgency and in accordance with the Government Security Classifications policy. It should be noted that General Security Agreements or other security arrangements may state what transmission methods are permitted or place restrictions on how classified information can be exchanged between the parties.

46. As a general rule UK OFFICIAL-SENSITIVE classified information should be communicated to international partners electronically using appropriate encryption. If exchanges with an international partner are to be frequent HMG organisations can consider establishing a secure bilateral link with the partner or mutually agreeing on the use of an appropriate encryption product. However, UK OFFICIAL-SENSITIVE classified information can be sent to partners without suitable encryption in the following circumstances: (a) if no suitable encryption method or secure mechanism is available; (b) if this method is compliant with local security policy; and (c) the originator of the information is content with using this method.

47. Whilst OFFICIAL information bearing the SENSITIVE caveat may be sent unprotected without suitable encryption, as addressed in the previous sentence, it should be noted this exception generally does not extend to international partners' RESTRICTED classified information. International RESTRICTED classified information is to be communicated and protected as set out in Annex B.

48. HMG classified assets marked UK SECRET or UK TOP SECRET cannot be transmitted to an international partner over an unaccredited ICT system unless it is encrypted using a suitably approved cryptographic product.

Section 6: Industrial Security

49. Industrial security is the application of measures to ensure the protection of classified information by contractors in pre-contract negotiations and throughout the life-cycle of a classified contract.

UK contractors participating in international classified contracts at the level CONFIDENTIAL or above

50. UK contractors can only undertake international classified contracts at the level of international CONFIDENTIAL or above within their facility if that facility has an appropriate FSC (Facility Security Clearance) issued by HMG. In the UK, a FSC is synonymous with a facility holding 'List X'.

51. UK contractors wishing to secure international classified contracts at the level of international CONFIDENTIAL or above can tender for these contracts if the international contracting authority is:

a. NATO, ESA, Eurocontrol, OCCAR or any other International Organisation where classified information provisions have been agreed;

b. A foreign government, or a contractor authorised by that government, with which HMG has a bilateral General Security Agreement or other relevant security arrangement; or

c. A foreign government/International Organisation with which HMG has a project-specific security arrangement.

d. For sub-contracts, a contractor that has been awarded a classified contract listed by an entity in the previous three sub-paragraphs.

52. If a UK contractor is successful in securing an international classified contract, and their facility requires to access, handle, manufacture and/or store classified information, HMG will consider undertaking FSC (i.e. List X) action following a formal request from the international contracting authority.

53. UK contractors can tender for and be awarded classified contracts with other foreign governments or International Organisations not covered by the previous paragraph, but HMG will not be obliged to undertake either FSC (or PSC) action. However, HMG can consider offering advice and support to UK industry so that it is not disadvantaged in being considered for these classified contracts.

UK contractors obtaining FSCs

54. If a UK contractor has a requirement to access, handle and/or store classified information at the level of international CONFIDENTIAL or above at their facility during the tendering process, or to fulfil a classified contract that has been awarded, then the contracting authority may want to confirm with HMG that a FSC is held. Such assurances are communicated on a government-to-government basis, not by contractors, so should a

FSC need to be confirmed the international contracting authority will submit a FIS (FSC Information Sheet) request to the UK NSA or relevant UK DSA/CSA.

55. Upon receiving a FIS request, the UK authorities will check if the contractor has a FSC. If the UK contractor already holds a FSC (i.e. List X) the contracting authority will be notified by that UK authority. In the event that a UK contractor does not hold an appropriate FSC, and if directly requested by the contracting authority in the FIS, HMG can consider starting the FSC accreditation process.

56. If UK contractors do not have a requirement to access, handle, manufacture and/or store classified information at the level of international CONFIDENTIAL or above at their facility, either during the tendering process or to fulfil a classified contract that has been awarded, a FSC is not required under HMG policy and cannot be undertaken. Contractors should not be excluded from tendering for an international classified contract if a FSC is not necessary. If a UK contractor encounters difficulties with an international contracting authority that insists that holding a FSC is a prerequisite for tendering for or undertaking a classified contract, even though no classified information at the level of international CONFIDENTIAL or above is to be accessed, handled and/or stored at their facility, then the contractor is advised to contact the UK NSA or relevant UK DSA/CSA.

57. Under no circumstance will HMG initiate the FSC accreditation process in response to direct requests from a UK contractor, or without there being an established and internationally sponsored requirement for the contractor to access, handle and/or store classified assets at their facility (i.e. undertake speculative clearances).

FSC Certificates

58. HMG does not issue FSC Certificates to UK contractors. Confirmation of an existing FSC for a UK contractor is obtained by the international contracting authority submitting a FIS request to HMG as explained in the previous paragraphs of this section.

UK contractor personnel obtaining PSCs

59. UK contractor personnel who will access and handle international classified information at the level of international CONFIDENTIAL or above must hold a valid PSC.

60. Access to international CONFIDENTIAL or SECRET classified information requires individuals to hold SC clearance, and access to international TOP SECRET requires a DV clearance. A BPSS pre-recruitment check or Counter-Terrorist Check (CTC) clearance does not permit access international classified information at the level to international of CONFIDENTIAL or above.

61. If contractor personnel require a PSC in order to work on an international classified contract there are various ways that a PSC request can be submitted to HMG, depending

on the circumstances of the classified contract. This process to follow and the criteria to meet is outlined in separate guidance available on gov.uk.

62. Under no circumstances will HMG initiate vetting on individuals without there being a genuine and confirmed requirement for the individual to access classified assets (i.e. undertake speculative vetting).

UK contractors engaging in international RESTRICTED contracts

63. Unlike a small number of foreign governments, the UK does not undertake FSC accreditation at the international RESTRICTED level. If a UK contractor is requested by a contracting authority to provide evidence that they hold a valid FSC, and the classified contract is no higher than international RESTRICTED, then they should remind the contracting authority that the UK does not undertake FSCs at this level.

64. The UK does not have a RESTRICTED level within its Government Security Classifications policy. International RESTRICTED classified information will be protected by contractors as set out in Section 4.

UK contractor personnel obtaining PSCs

65. A small number of foreign governments require PSCs at the RESTRICTED level. If UK contractor personnel are requested to provide evidence that they hold a valid PSC they should remind the contracting authority that the UK does not undertake PSCs at this level. However, the overseas Contracting Authority may include specific provisions in the classified contract requiring that individuals having access to its RESTRICTED information should be subjected to a recruitment check. In such cases, the application of the BPSS pre-recruitment check would be acceptable. Guidance on the BPSS is available on gov.uk.

Contractor visits involving access to international classified information

66. Unless alternative arrangements have been formally agreed between the relevant security authorities of the contract/programme, if contractor personnel have a need to visit non-HMG facilities overseas to discuss international classified information at the level of CONFIDENTIAL or above then such visits usually need to be authorised under a Request for Visit (RFV). The RFV process starts by the Facility Security Officer of the UK company completing and forwarding to the UK NSA/DSA/CSA a RFV form. The RFV form will be processed and then sent to the security authority responsible for the host facility. The security authority of the host facility will then either approve or reject the visit. A generic template of the RFV form can be downloaded from gov.uk, although it should be noted that some classified contracts might mandate a different template to be used.

67. Security authorities have different lead times for the submission of RFVs but generally UK contractors conducting visits should aim to submit their RFV applications to the UK NSA/ DSA/CSA 20 working days in advance of the proposed visit.

68. RFVs are generally not required by foreign governments or International Organisations at the international RESTRICTED level, though some may require this.

Annex A: General Security Agreements

List of currently in force General Security Agreements:

Country	Date signed	Date updated (if applicable)
Bulgaria	September 2012	October 2014
Finland	June 2012	April 2014
France	March 2008	September 2014
Germany	May 2003	N/A
Luxembourg	September 2015	N/A
Japan	July 2013	October 2014
Poland	August 2007	February 2017
Spain	February 2015	N/A

Annex B: Minimum requirements for protecting international classified information

Personnel security and access control

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Personnel Security Clearance (PSC)	• Need to know principle applies. • BPSS is not required for access to international RESTRICTED unless a recruitment check is specified by the overseas government.	• SC required. • Need to Know principle applies.		• DV required. • Need to Know principle applies.
Nationality considerations	No nationality restrictions mandated. However, departments, agencies and contractors should be mindful of any nationality sensitivities, and third party transfer restrictions, before authorising access to nationals from a non-Member State (for NATO and ESA) and third State nationals (for GSAs and SAs).	• Nationality to be considered before authorising access to nationals from a non-Member State (for NATO and ESA) and third State nationals (for GSAs and SAs). • Special provisions may need to be met.		• Access likely to be strictly limited to sole-nationals of the Parties. • Special provisions may need to be met.
Briefing and Awareness training	• Briefing and awareness training required to ensure international classified information is appropriately protected. • NATO - Individuals to acknowledge their security responsibilities in writing. For NATO CONFIDENTIAL and above records are to be maintained as to who has been authorised to access NATO classified information.			
Visits involving international classified information	Visits requiring access to international classified information will be undertaken in accordance with the relevant international regulations and/or GSAs and security arrangement .			

Physical Security

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
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.	• For international CONFIDENTIAL and SECRET, UK establishments must apply the same physical protection as applied for UK SECRET, and for international TOP SECRET the same protection as applied for UK TOP SECRET. • Secured areas which are not occupied by duty personnel on a 24-hour basis will be inspected at the end of normal working hours, and at random intervals outside normal working hours (unless an Intrusion Detection System (IDS) is in place).		
Physical measures for storing international classified assets	Stored in suitable lockable office furniture when not in use.	Either stored in a nationally-approved security container (to the level of UK SECRET), or in an open storage area with supplemental controls.		Either stored in a nationally-approved security container (to the level UK TOP SECRET); in an open storage area with supplemental controls; or in an IDS Vault/strong room.
Discussing in public	International classified information not to be discussed in public at any classification level..			
Discussing in offices	Only discuss in areas where individuals without the need to know cannot overhear.	Only to be discussed in secure areas, and where individuals without the appropriate Personnel Security Clearance (PSC) and Need to Know cannot overhear.		
TEMPEST measures	No controls required at this level.	ESA only - Must be protected by TEMPEST measures.	Must be protected by TEMPEST measures.	Must be protected by TEMPEST measures.

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Requirement for a Facility Security Clearance (FSC) for contractors	No requirement.	FSC required for CONFIDENTIAL and above.		

Information management

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Marking of international classified information	International classified information will not be remarked with a UK classification (unless UK classified information is added to the asset, in which case a dual marking can be considered)			
Contractors producing international classified information	Organisations producing international partner classified information will assign the classification marking in accordance with the provisions contained in the Security Classification Guide or Security Aspects Letter.			
Use of international classified assets	The recipient will only use international classified information for the purpose for which it was provided or as authorised by the international partner.			
Copying of physical documents	Reproductions will be limited to the minimum required for an official purpose, and will be made only by individuals with a Need to Know.	Reproductions will be limited to the minimum required for an official purpose, and will be made only by individuals with an appropriate PSC and a need to know.		Approval for reproduction must be sought from the providing international partner. Any reproductions made will be limited to the minimum required for an official purpose, and will be made only by individuals with a DV and a need to know.
Translation of documents	• Translations will 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	Registration not required.	• Registration for ESA only. • Registry staff must hold a SC.	• Registration required. • Registry staff must hold a SC.	• Required. • Registry staff must hold a DV.
Physical carriage within a building or self-contained group of buildings	Covered from view by a single cover (e.g. opaque envelope or folder).	Carried by a SC cleared individual in sealed tamper-evident envelope/container.		Movement must first be approved and documented by senior management. Carried by a DV cleared individual in a sealed tamper-evident envelope/container.

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Physical transmission of classified information within the UK, or overseas to a NATO or 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.	• NATO - Diplomatic channels, military courier, or authorised personal hand carriage (with special handling requirements). • ESA - Commercial courier service (must use approved commercial courier that offers 'track and trace' service), diplomatic channels, military courier, or authorised personal hand carriage. • Foreign government - In accordance with any bilateral General Security Agreement, Security Arrangement, or any other relevant agreement	• NATO - Diplomatic channels, military courier, or authorised personal hand carriage (with special handling requirements). • ESA - Diplomatic channels, military courier, or authorised personal hand carriage. • Foreign government - In accordance with any bilateral General Security Agreement, Security Arrangement, or any other relevant agreement	Diplomatic or military courier only.
Physical transmission of classified information to a nation that is not a NATO 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.	• NATO - Diplomatic channels, military courier or authorised personal hand carriage (with special handling requirements). • ESA – In accordance with any Security Agreement ESA has with a third State. • Foreign government - In accordance with any bilateral General Security Agreement, Security Arrangement, or any other relevant agreement.	• NATO - Diplomatic channels, military courier or authorised personal hand carriage (with special handling requirements). • ESA – In accordance with any Security Agreement ESA has with a third State. • Foreign government - In accordance with any bilateral General Security Agreement, Security Arrangement, or any other relevant agreement.	Diplomatic or military courier only.
Packaging to be used when sending information within the UK or overseas	Two opaque envelopes or other suitable packing material to be used.	• Sealed tamper-evident double envelopes or other suitably secure packing material for transporting UK SECRET. • ESA - Registration and delivery receipts needed.	• Sealed tamper-evident double envelopes or other suitably secure packing material for transporting UK SECRET. • Registration and delivery receipts needed.	• Sealed tamper-evident double envelopes or suitable security containers. Nationally approved security seals for transporting UK TOP SECRET. • Registration and delivery receipts needed.
Destruction of physical assets	Destroyed in such a manner that ensures it cannot be reconstructed.	• Destroyed using HMG approved equipment for UK SECRET by a SC cleared individual and under the supervision of a SC cleared witness. • Destruction certificates are required for: – ESA CONFIDENTIAL and ESA SECRET – NATO SECRET • Destruction certificates to be kept for 5 years.		• Destroyed using HMG approved equipment for UK TOP SECRET by a DV cleared individual and under the supervision of two DV cleared witnesses. • CTS - Destruction certificate required. To be kept for 10 years.

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Security Incident – HMG organisation	• All security incidents must be investigated and reported to the Senior Security Adviser (SSA) or Security Adviser (SA) in accordance with internal departmental security procedures. • Significant security breaches that may lead to compromise may need to be reported by the SSA/SA to the UK National Security Authority (NSA). • Suspected or actual compromise must be reported by the SSA/SA to the UK NSA.			
Security Incident – UK contractor with FSC	• Security incidents must be investigated and reported to the Facility Security Officer, who will report this to their HMG 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 – UK contractor not holding a FSC	• Security incidents must be investigated and reported to the Security Officer, who must report this to the applicable contracting authority. • Significant security breaches that may lead to compromise should also be reported to the UK NSA. • Suspected or actual compromise should also be reported to the UK	Not applicable – A FSC is required for contractors that access, handle and/or store classified information at the level of CONFIDENTIAL or above at their facility.		

Information Assurance

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
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). • Use UK ICT that is appropriately accredited. • NATO/ESA – Can use UK ICT that has been appropriately accredited, or a ICT approved by that international organisation.	• Must not use unauthorised ICT (e.g. personal devices). • Use UK ICT that is approved by HMG to protect UK SECRET. • NATO/ESA – Can use a ICT approved by that international organisation.	• Must not use unauthorised ICT (e.g. personal devices). • Use UK ICT that is approved by HMG to protect UK SECRET. • NATO/ESA – Can use a ICT approved by that international organisation.	• Must not use unauthorised ICT (e.g. personal devices). • Use UK ICT that is approved by HMG to protect UK TOP SECRET. • NATO/ESA – Can use a ICT approved by that international organisation.
ICT risk management	• Any additional threats or increased risks involved in handling international classified information to be taken into account. • NATO/ESA - Accreditation must be compliant with the relevant security regulations and security policies of the international organisation.			
Sending classified information by email over a trusted or accredited network	Where a cryptographic product is used, it must be NCSC approved, or approved by the International Organisation/foreign government concerned.	Where a cryptographic product is required, the product must be NCSC approved or approved by the applicable International Organisation/foreign government concerned.	• NATO/ESA - Where a cryptographic product is required, the product must be approved by the International Organisation concerned. • Foreign Government - Where a cryptographic product is required, the product must be NCSC approved.	• NATO - Where a cryptographic product is required, the cryptographic product must be approved by NATO. • Foreign Government - Where a cryptographic product is required, a NCSC approved cryptographic product must be used.

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Sending classified information by email over public networks or untrusted networks	Must be encrypted with a NCSC approved cryptographic product or a cryptographic product approved by the International Organisation/foreign government concerned.	Must be encrypted with a NCSC approved cryptographic product or a cryptographic product approved by the International Organisation/foreign government concerned.	• NATO/ESA - Must be encrypted with a cryptographic product approved by the International Organisation concerned. • Foreign Government - Must be encrypted with an approved cryptographic product, normally approved by NCSC or the foreign government.	• NATO - The classified information must be encrypted using a cryptographic product approved by NATO. • Foreign Government - Must be encrypted with an approved cryptographic product, normally approved by NCSC or the foreign government.
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 the 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	Computer storage media, which includes removable media that has previously held international classified information can be reused or disposed of in accordance with national policy.			

Disclosure and release

	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Disclosure of international classified information to the public	UK holders of international classified information will seek prior written authorisation from the originator if they want to disclose 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 the public – Disclosure request	The UK NSA must be consulted should a disclosure request (e.g. FOI) be received for international classified information held by a government department, agency or public body.			
Release of international classified information to a Third Party	UK holders of international classified information will seek 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.			

Annex C: Version History

Document Version	Date Published	Summary Of Changes
1.0	April 2014	First version published on GOV.UK.
1.1	July 2014	See 'Version History' in document 1.1 for complete list.
1.2	July 2015	See 'Version History' in document 1.2 for complete list.
1.3	November 2016	See 'Version History' in document 1.3 for complete list.
1.4	May 2018	See 'Version History' in document 1.4 for complete list.
1.5	March 2020	• Section 1 – NSAs, CSAs and DSAs text clarified. • Section 3 – Paragraph amended to reflect that FCO and MoD are responsible for vetting. • Section 4 - Cryptographic products used to protect international RESTRICTED clarified. • Section 5 – UK prefix paragraph simplified. • Section 6 – RFV paragraph clarified. • Annex A – Poland entry updated to show revision date. • Annex B - Copying of physical documents CONFIDENTIAL and SECRET cells merged. References to DSOs changed to SSAs and SAs. • Annex C – Version history now Annex C. • General –References to SPF removed. EU references removed. Several paragraphs redrafted and references amended.

Any enquiries regarding this publication should be sent to us at UK-NSA@cabinetoffice.gov.uk

You can download this publication from www.gov.uk.