Defence and Security Public Contracts Regulations 2011

Chapter 12 - Security of Information

Purpose

1. This guidance explains the security of information provisions of the Defence and Security Public Contracts Regulations (DSPCR) 2011.

2. In particular, it sets out how to protect classified information throughout the award and performance of a contract. It also provides guidance on how to assess the capability of suppliers to meet the procurer's security of information requirements.

What is security of information?

3. By security of information, we mean the protection of all classified information, regardless of its form, during the contract award procedure and the resulting contract.

What is the legal framework?

4. Regulations 10 (Confidential information), 11 (Classified Information), 36 (Conditions for performance of contracts) and 38 (Security of information) set out the provisions that allow us to protect certain types of information during procurement.

5. Regulation 23 (Criteria for the rejection of economic operators) and 25(2)(m) (Information as to technical or professional ability) set the supplier selection criteria related to security of information.

What safeguards protect information?

6. Procurers and suppliers must adequately protect classified information at all times. The ability and reliability of suppliers and their subcontractors to meet their obligations to protect classified information is vital to the United Kingdom's (UK's) national security interests.

7. The DSPCR address the circumstances where a contract involves, requires, or contains, classified information. It allows procurers to impose requirements for the protection of classified information throughout the acquisition process. This covers the entire life cycle of a contract:

a. the publication of the contract notice;

b. the tendering process;

c. the delivery of the contract requirement; and

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

d. the period after expiry or termination of the contract.

8. The DSPCR also establishes the obligations of the procurer to provide potential suppliers with sufficient and timely information on its security of information requirements. This will assist suppliers by:

a. enabling them to assess whether to express an interest in the procurement; and

b. providing them with the necessary information for the subsequent preparation of tenders and performance of the contract.

9. Some contracts could be so sensitive that you may exclude them from the application of the DSPCR, for example, sensitive contracts for the purposes of intelligence activities. The DSPCR, however, contain various protective measures concerning security of information which should limit the need to use the general exclusions in the DSPCR or Treaty exemptions to cases where those protective measures are inadequate.

What is meant by 'classified information'?

10. The DSPCR define 'classified information' as:

> "…any information or material, regardless of its form, nature or mode of transmission, to which a security classification or protection has been attributed and which in the interests of national security and in accordance with the law or administrative provisions of any part of the United Kingdom requires protection against appropriation, destruction, removal, disclosure, loss or access by any unauthorised individual, or any other type of compromise."

11. For procurers in the UK applying the DSPCR, 'classified information' is any information or material that has been assigned, by the Government or other official body of a Nation. In the United Kingdom (UK), the relevant protective markings are 'OFFICIAL'[1] 'OFFICIAL-SENSITIVE', 'SECRET', or 'TOP SECRET' in accordance with the Government Security Classification (GSC) under the Security Policy Framework.

12. Other governments recognise 'OFFICIAL', 'OFFICIAL-SENSITIVE, 'SECRET', or 'TOP SECRET', as these classification levels are identified as relevant in bi-lateral and other international Security Agreements or Arrangements (see paragraph 37).

[1] It is MOD policy not to mark information or assets as 'OFFICIAL', therefore for MOD procurements the definition in the DSPCR of classified information will only be relevant for information or assets marked as 'OFFICIAL-SENSITIVE' or higher. However, it is recognised that Other Government Departments (OGDs) and Agencies do mark information or assets as 'OFFICIAL' as a matter of policy and therefore that (in appropriate circumstances) such information or assets will be classified information for the purposes of the DSPCR.

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

What requirements can procurers impose on suppliers?

13. A procurer can impose on suppliers certain requirements aimed at protecting classified information, both during the contract award phase and as part of the contract performance requirements. This relates to all classified information whether communicated by the procurer or otherwise (e.g. generated by the supplier or provided by a third party).

14. In addition, procurers may require a supplier to ensure that its subcontractors comply with the same requirements to protect classified information as are imposed on the supplier.

15. Procurers may require all tenderers to enter into a confidentiality or non-disclosure agreement to protect certain information during the contract award procedure in addition to their obligations under relevant national security law, such as the Official Secrets Act.

16. Procurers safeguard security of information during contract performance through use of the provisions of Regulation 38 and the application of associated contract conditions.

Selection of Suppliers

17. The contract notice must include the main features of the security of information requirements and the grounds for qualitative selection, i.e. the selection criteria must specify the minimum capability for protecting information which is normally the level of Facility Security Clearance required (see Regulation 25(2)(m)).

18. Procurers may use relevant selection criteria on security of information during the Pre-Qualification Questionnaire (PQQ) process to exclude those suppliers who do not meet certain proportionate or minimum capability requirements. You may also use selection criteria to limit the number of tenderers (e.g. as part of a basic ranking system).

Exclusion of suppliers and tenderers

19. Regulation 23 provides a list of grounds for excluding suppliers and tenderers for reasons of reliability. In relation to security of information requirements, you may exclude a supplier from participation in the procurement procedure if:

a. it has committed an act of grave misconduct in the course of its business or profession. This includes a breach of obligations regarding security of information required by any procurer in accordance with Regulation 38 during a previous contract (Regulation 23(4)(e)); or

b. it has been found, on the basis of any means of evidence, including protected data sources, not to possess the reliability necessary to exclude risks to the security of the UK (Regulation 23(4)(f)).

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

20. Regulation 23(4)(e) applies specifically to breaches of security of information obligations during previous contracts. This also covers contracts let by procurers in other Member States.

21. While Regulation 23(4)(e) does not require a final conviction by a court of law for grave misconduct to be 'proven', a procurer must have objective and verifiable information if it intends to exclude a supplier or tenderer on these grounds. The decision to reject must be a proportionate course of action, taking into account the full circumstances of the case including the nature of the contract and the severity of the breach.

22. Regulation 23(4)(f) deals more broadly with the reliability of suppliers or tenderers. Recital 65 of the Directive explains the rationale behind this selection criterion:

> "… It should also be possible to exclude economic operators if the contracting authority / entity has information, where applicable provided by protected sources, establishing that they are not sufficiently reliable so as to exclude risks to the security of the Member State. Such risks could derive from certain features of the products supplied by the candidate, or from the shareholding structure of the candidate."

23. Essentially, suppliers must be sufficiently reliable to exclude risks to the security of the UK. Risks could arise from, for example, certain features of products previously supplied (such as if the product contains hidden software which tracks the user's data). Procurers may, therefore, question the reliability of a supplier or tenderer even where it holds security clearances from its national authorities.

24. You must only exclude a supplier on reliability grounds because of objective evidence, which you must interpret proportionately and reasonably bearing in mind the subject of the contract and the relevant security of information requirements.

25. In addition, although Regulation 23(4)(f) can be based on 'any means of evidence, including protected data sources', this does not give unlimited discretion to procurers. You must base any exclusion on risks to the security of the UK and a procurer must be prepared to demonstrate and justify, ultimately to the Court, the reasons for, and plausibility of, its decision.

26. Procurers also have the ability to reject subcontractors (see Chapter 14 - Subcontracting under the DSPCR). However, you must only base a decision to reject on the selection criteria used for the main supplier. Therefore, where a subcontractor has committed an act of grave misconduct or does not possess the reliability required, you may reject them in accordance with the same principles.

Criteria of technical and / or professional ability

27. Regulation 25(2)(m) allows an assessment based on evidence of a supplier's technical or professional ability to process, store and transmit classified information at the level of protection required by the procurer (see Chapter 15 –

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

Supplier Selection). This will almost invariably include evidence that the supplier holds a relevant security clearance.

UK Suppliers

28. For UK suppliers, you can find existing UK national provisions on security clearance set out in the HMG Security Policy Framework.

29. Suppliers holding, or who are sponsored, willing and able to gain, a Facility Security Clearance (FSC) or the necessary Personal Security Clearances (PSC), or both, appropriate to the protective marking of the classified information involved, required or contained in the contract award process and subsequent contract, will be able to comply with national security rules and regulations.

30. Similarly, UK subcontractors holding an appropriate FSC and PSC will be able to comply with security clearance requirements. This includes UK subcontractors of suppliers of other Member States who are appropriately security cleared.

31. A FSC is site specific and required only for contracts involving information classified as 'SECRET' or above. It is not required for contracts involving information classified as 'OFFICIAL' or 'OFFICIAL-SENSITIVE'. When the Ministry of Defence's (MOD) Director of Defence Security grants a FSC, the site is added to List X.

32. Suppliers cannot themselves provide an assurance that they have a FSC. Therefore, for contracts involving information classified as SECRET and above, procurers must verify that the proposed supplier holds the necessary FSC by contacting the relevant National or Designated Security Authority to obtain confirmation. If the supplier does not hold the necessary FSC, the procurer may sponsor security clearance action.

33. For OFFICIAL-SENSITIVE only contracts, unless specifically required by national security laws and regulations, suppliers do not need to hold a FSC. In that situation, procurers should include the requirements for the protection of OFFICIAL-SENSITIVE information in the contract documents and obtain a commitment from tenderers that they will protect classified information to that level.

34. Procurers may reject subcontractors chosen at the main contract award stage as long as they base the rejection on criteria applied for selection of the successful tenderer. If the successful tenderer proposes the use of subcontractors, each of these subcontractors should hold a FSC or PSC, or both, appropriate to the level of classified information that they will be handling or they should be capable of obtaining clearance to the appropriate level through sponsorship from either the procurer or the successful tenderer (for MOD procurers, List X contractors may sponsor subcontractors to obtain certain levels of clearance).

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

Foreign suppliers or subcontractors

35. The evidence that suppliers (including subcontractors) of other Member States or Third States have the ability to meet procurers' security of information requirements may include evidence of holding an equivalent security clearance recognised by the UK appropriate to the relevant protective marking.

36. Foreign suppliers are required to comply with their own national laws and regulations. When considering the ability of a foreign supplier to meet UK's security of information requirements, procurers must take account of whether there is a relevant bilateral Security Agreement (or Arrangement) between the UK and the other Member State or the Third State.

37. A bilateral Security Agreement with the other Member State or Third State is sufficient evidence for procurers to recognise the FSC granted to, and the ability of, a supplier in that Member State or Third State to comply with its security requirements to protect classified information to at least an equivalent standard to the UK requirements. In those circumstances, you only require verification that the supplier or subcontractor has an appropriate FSC awarded by its own National or Designated Security Authority.

38. UK national security regulations require suppliers to seek the approval of procurers where suppliers propose to subcontract work to foreign subcontractors at the level of 'SECRET' or above. Procurers are likely to grant approval if the proposed subcontractor holds an appropriate FSC or PSC granted by its own National or Designated Security Authority.

39. The relevant UK National or Designated Security Authority will accept an assurance of the existence of an appropriate FSC or PSC under a bilateral Security Agreement.

40. If the proposed supplier does not hold an FSC, or it is not at the level required for the performance of the contract, you should ask the relevant UK National or Designated Security Authority to request the supplier's own National or Designated Security Authority to initiate FSC action to the equivalent level required.

41. Currently the UK has bilateral Security Agreements that include the protection of defence classified information with all European Union (EU) Member States except the following:

a. Cyprus;

b. Ireland;

c. Latvia (under negotiation);

d. Luxemburg (under negotiation);

e. Malta; and

f. Slovenia (proposed).

42. Despite the absence of a bilateral Security Agreement with these countries, it is possible to obtain assurances of a FSC for suppliers and subcontractors that

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

would be at least equivalent under the scope of the EU Council security regulations (Council Decision 2001/264/EC, as amended).

What contract conditions can procurers impose on suppliers and tenderers?

43. Regulation 38 allows that, where classified information is involved, the procurer may require the tender to contain particulars including, but not limited to, the following:

a. A commitment from the tenderer and the subcontractors already identified to safeguard appropriately the confidentiality of all classified information in their possession or coming to their notice throughout the duration of the contract and after the termination or conclusion of the contract.

b. A commitment from the tenderer to obtain the commitment referred to in sub-paragraph 44a from other subcontractors to which it will subcontract during the execution of the contract.

c. Sufficient information on subcontractors already identified to enable the procurer to determine that each of them possesses the capabilities required to safeguard the confidentiality of the classified information to which they have access or which they are required to produce when carrying out their subcontracting activities – an appropriate FSC may satisfy this requirement.

d. A commitment from the tenderer to provide the information referred to in sub-paragraph 44c on any new subcontractor before awarding a subcontract.

44. Any measures that the procurer specifies to ensure the security of classified information under Regulation 38 must comply with, or be equivalent to, the security clearance provisions of the UK appropriate to the relevant protective marking. In other words, any contract terms relating to security of information obligations must not exceed what the tenderer (or subcontractor) is required to do to obtain the security clearance relevant to the level of protective marking or markings of the classified information which the contract (or subcontract) will involve.

45. Regulation 38 allows procurers to require tenderers to set out their solutions for maintaining the security of the classified information handled during contract performance and afterwards including flowing down those commitments to the supply chain.

46. Regulation 38 also allows procurers to oblige tenderers to provide information on their subcontractors so that the procurer can verify their ability to safeguard classified information where they did not do it as part of the supplier selection or subcontractor selection process or otherwise under Regulation 37 (Subcontracting). It also commits tenderers to provide that information on subcontractors where they have not identified those subcontractors yet.

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

47. The measures and requirements under Regulation 38 are non-exhaustive. The procurer may therefore add to this list, as long as those additions are consistent with the security clearance requirements applicable to the relevant level of protective marking and are proportionate to the subject of the contract.

48. Procurers must of course ensure that they include any commitments or requirements imposed on tenderers, including those it requires the tenderer to flow down the supply chain, as obligations in the final contract.

What are the obligations of procurers to suppliers and tenderers?

49. If invitations to tender or contracts involve, require or contain classified information, procurers must provide a sufficient indication of their security of information requirements to potential suppliers so they are able to decide whether to express an interest in participating in the procurement procedures.

50. Procurers must also provide tenderers with adequate details of their security of information requirements in order for them to prepare their tender. Procurers must provide the necessary level of information in the contract notice, or in the invitation to tender, or both. A decision tree containing the key decision points and an indication of the factors to consider can be found in Annex A.

Contract Notice

51. Procurers must describe in the contract notice sent to Official Journal of the European Union (OJEU) the maximum level of protective marking of the information or material that needs to be protected, processed, stored or transmitted during the contract award procedure and in the performance of the contract (section III.2.3 "technical and / or professional capacity" of the contract notice refers).

52. Procurers must also indicate any specific contract performance conditions on protecting classified information in the contract notice or contract documents.

53. If procurers require evidence that a supplier holds a relevant UK or equivalent security clearance appropriate to the relevant protective marking, the contract notice must specify the nature and form of the evidence you require.

54. You may give suppliers that do not yet hold the necessary clearance additional time to obtain it following sponsorship by the procurer. Where this is the case, Regulation 25(5) requires procurers to indicate this, along with the time limit, in the contract notice.

Invitation to Tender and other Contract Documents

55. If you do not include the full security of information requirements in the contract notice, you must include comprehensive details in the invitation to tender. This must include details of any information or commitments you require the tenderer to provide as part of its tender response and the form in which they must present it.

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

56. Additionally, you must communicate the detailed classified aspects of the contract to the supplier in the invitation to tender documents and in the contract, for example, in the form of a Security Aspects Letter (SAL).

What exclusions from the DSPCR are available on Security of Information grounds?

57. Regulation 7 (General exclusions) provides for general exclusions from the DSPCR. Regulation 7(1)(a) and 7(1)(b) relate to security of information considerations.

Regulation 7(1)(a)

58. Regulation 7(1)(a) provides that the DSPCR do not apply to you seeking offers in relation to a proposed contract or framework agreement where the application of the DSPCR would oblige the UK to supply information the disclosure of which it considers contrary to the essential interests of its security.

59. This exclusion is based on Article 346(1)(a) of the Treaty on the Functioning of the European Union (TFEU). It is applicable to both military and security contracts but is particularly relevant for non-military security contracts and military security contracts where Article 346(1)(b) is not relevant (i.e. the subject matter of the contract is not on the 1958 List nor is a service or work directly related to an item on that List).

60. Regulation 7(1)(a) also covers contracts which are so sensitive that the mere fact of advertising the contract would be contrary to the essential interests of UK security (i.e. their very existence must be kept secret). In those cases, it would be inappropriate to apply the Regulation despite its protections.

61. Recital 27 of the Directive also mentions security activities that are particularly sensitive, and where procurements may be highly confidential. For example, certain purchases intended for border protection, combating terrorism or organised crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces.

62. This list in Recital 27 indicates that Regulation 7(1)(a) essentially allows for the explicit exclusion of these confidential security contracts. This is on the basis that the provisions of the DSPCR to the specific contract, including the ability to exclude and reject suppliers and to ensure commitments and obligations from tenderers to protect the confidentiality of classified information, are not sufficient to safeguard the essential interest of UK security.

63. What this does not mean is that, just because information has a protective marking, you automatically exclude contracts involving this information from the contract award procedures in the DSPCR. You must apply any DSPCR exclusion or treaty exemption proportionately and be able to justify its use. As far as the MOD is concerned, only in exceptional circumstances will the provisions of the DSPCR not be sufficient to safeguard the essential interests of UK security. However, OGDs and Agencies will have different national security concerns,

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

which may not be safeguarded by the security of information provisions in the DSPCR.

64. However Article 346(1)(a) may still apply to the contract but its application does not necessarily mean that the DSPCR can be dis-applied. The best example of this is the additional access restriction caveat "UK EYES ONLY".

65. In contracts involving "UK EYES ONLY" material, only individuals who have a Personal Security Clearance up to the appropriate level of protective marking and who are nationals of the UK can see certain information. However, imposing a UK EYES ONLY caveat is not compatible with EU law.

66. Imposing a UK EYES ONLY caveat is therefore only justifiable on the basis of Article 346(1)(a) or another treaty exemption. You must use a treaty exemption proportionately and take the least restrictive measure(s) necessary to protect that national security interest (see Chapter 4 – Treaty Exemptions).

67. If a contract includes UK EYES ONLY material, procurers should not assume that the DSPCR will not apply. Procurers must consider whether they can award the contract using the DSPCR but ensure added safeguards under a treaty exemption for the UK EYES ONLY element so that foreign nationals cannot access that material. This may be possible if only discrete elements of a contract require the application of a UK EYES ONLY caveat (e.g. if part of the contract has to be performed in a restricted UK EYES ONLY area by a UK contractor or subcontractor).

68. Alternatively, the procurer could award separate contracts:

a. for the UK EYES ONLY work to a UK contractor that has been granted an FSC who can fully apply the UK EYES ONLY access limitations, under a treaty exemption; and

b. for the rest of the work that does not require access to UK EYES ONLY information, under the DSPCR.

However, there is no requirement to split contracts if you can objectively justify the award of a single contract.

69. Use of Article 346(1)(a) and Regulation 7(1)(a) allows procurers to protect information and not use the DSPCR. It does not exempt the procurer from Government policy for competing requirements wherever possible. Consequently, the procurer must use competition among eligible suppliers with suitably cleared personnel on a national basis where this would protect essential security interests.

70. You can also use Article 346(1)(a) to exempt the procurement from certain obligations under the DSPCR, rather than exempting all of it, in order to comply with the "least restrictive measure" principle. See "Disclosure of Information" in Chapter 5 – General Exclusions in the DSPCR.

Regulation 7(1)(b)

71. Regulation 7(1)(b) allows that the DSPCR do not apply where the contract or framework agreement is for the purposes of intelligence activities. This is

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

based on the assumption that contracts related to intelligence activities are by definition too sensitive to be awarded in a transparent and competitive procedure.

72. Again, Recital 27 of the Directive provides an indication of what this Regulation might cover. This includes procurements by intelligence services for the purpose of their own intelligence activities. It also covers procurements where other procurers subject to the DSPCR award contracts to intelligence services for supplies, works or services, for example, for the protection of government Information Technology (IT) networks.

73. Recital 27 also makes it clear that it is up to each Member State to define for itself what constitutes intelligence activities (including counter-intelligence activities). It is important to note the use of the phrase 'intelligence activities' in Regulation 7(1)(b) rather than intelligence 'services' or 'agencies'.

74. Also, there is no common definition of 'intelligence', and the way intelligence activities are organised differs between Member States. Regulation 7(1)(b) takes this into account and covers contracts for the purpose of all types of intelligence activities, no matter who is in charge of the intelligence function. See "Disclosure of Information" in Chapter 5 – General Exclusions in the DSPCR.

75. In summary, this provision covers exclusions intended for procurements in the fields of both defence and security where even the specific provisions of the DSPCR are not sufficient to safeguard the UK's essential security interests. You should note that defining what the essential security interests of the UK are and what 'intelligence activities' consists of is the responsibility of the UK itself.

What do I need to tell an excluded supplier or unsuccessful tenderer?

76. Regulations 30 (Notification) and 33 (Information about contract award procedures) set out the notifications and information procurers must provide to excluded suppliers (i.e. those excluded at PQQ stage or any stage up to final tender stage) or unsuccessful tenderers (i.e. those who submitted final tenders and were unsuccessful).

77. You should also consult Chapter 17 – Standstill Period, Contract Award and Voluntary Transparency in relation to the notification and information requirements you need to set out in a standstill notice for unsuccessful tenderers.

78. If they receive a request in writing procurers must inform excluded suppliers or unsuccessful tenderers of the reasons for their rejection (you should include this information, even if not requested, as part of a standstill notice you send to unsuccessful tenderers). This includes, at Regulation 33(8)(b), any reason for the procurer's decision that the supplier did not meet its security of information requirements as set out in the contract notice or invitation to tender in accordance with Regulation 38.

79. There may be circumstances, however, where full transparency of the reasons for exclusion of a supplier or rejection of a tender might conflict with

Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011

defence or security interests. This may be particularly true where you are basing your decisions to exclude or reject on information from protected sources.

80. Specifically, in relation to security of information, Regulation 33(11)(a) and (b) allow a procurer to withhold any information where the disclosure of that information would impede law enforcement or would otherwise be contrary to the public interest, in particular defence or security interests or both.

81. If the conditions of Regulation 33(11)(a) or (b) are met, procurers may decide not to communicate information, even if this means that you cannot inform the tenderer of the main reason for its rejection. The tenderer concerned, however, would remain free to challenge the rejection if it considers the procurer to be in breach of the duties owed to it under the DSPCR.

What are the key points to remember?

1. Where a procurement process involves access to classified information, you must consider imposing obligations on suppliers and require flow-down of those obligations to subcontractors, to safeguard that information throughout the tendering and contracting procedure. Those obligations must be proportionate and relevant for the particular procurement process.

2. You are allowed to reject suppliers and subcontractors where they:

   a. do not possess the necessary reliability to exclude risks to national security; or

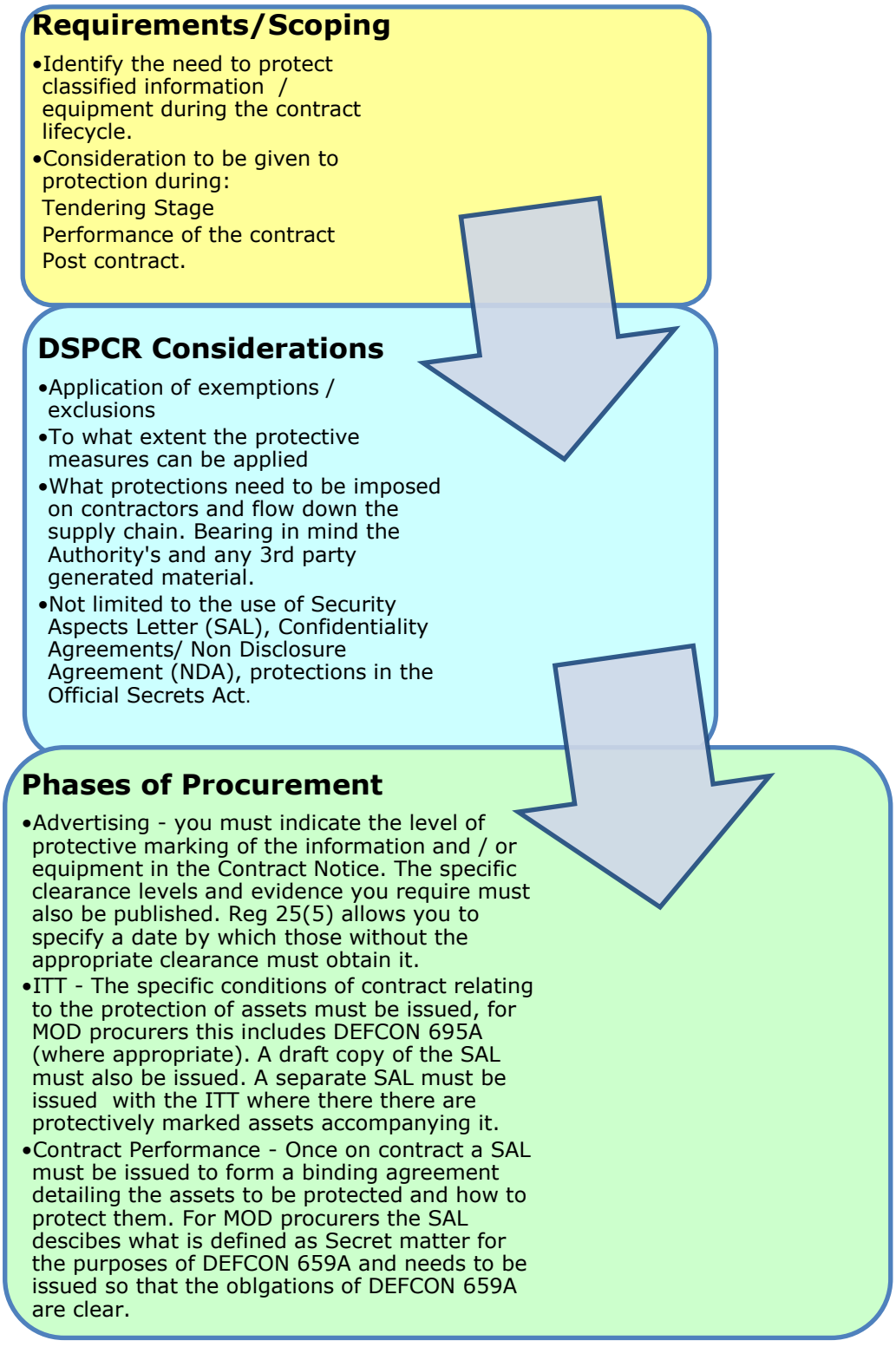
   b. have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.

3. You must request information from suppliers and subcontractors to assess their ability to protect information if they will have access to classified information marked OFFICIAL[2] / OFFICIAL-SENSITIVE or above.

4. You should impose measures to protect information to the required level if suppliers and subcontractors will have access to classified information marked 'OFFICIAL / OFFICIAL-SENSITIVE or above.

[2] MOD procurers must note, that it is MOD policy not to mark material with the 'OFFICIAL' classification. Therefore the requirement applies to material marked as 'OFFICIAL-SENSITIVE' or above.

Annex A – Security of Information Decision Tree



Version 1.1 dated 03/06/2016
Source: www.gov.uk/government/publications/the-european-union-defence-and-security-public-contracts-regulations-dspcr-2011