Guidance 1.6: Contractors and Contracting Authorities

Summary

1. Contracting authorities and their contractors which handle, process, move and store HMG information (inclusive of material assets), need to be aware of the updates to the Government Security Classifications Policy (GSCP).

2. For the purposes of this guidance:

    a. “contractor” means any natural or legal person with the capacity to enter into a contract with HMG. Contractor should be treated as the equivalent of a “supplier” as referred to in the Government Commercial Function’s Model Services Contract (available on GOV.UK) and the Mid-Tier Contract (available on GOV.UK);

    b. “HMG contracting authorities” means the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law, and includes central government authorities, but does not include His Majesty in his private capacity. Contracting authorities should be treated as the equivalent of a “buyer/authority” as referred to in the Government Commercial Function’s Model Services Contract (available on GOV.UK) and Mid-Tier Contract (available on GOV.UK);.

3. The GSCP contains updated guidance, minimum baseline security controls and behaviours for the protection of UK information classified as OFFICIAL, SECRET and TOP SECRET. Contractors should read these in conjunction with their existing obligations as detailed within their contract with HMG and the GOV007 Functional Standard.

4. Contractors will handle and protect HMG classified information entrusted to them, or produced by them under contract, in accordance with the GSCP. Unless the HMG contract stipulates more stringent requirements, the provisions of the GSCP are considered the baseline that all contractors should meet.

5. The updated GSCP will come into force on 30th June 2023. A commercial implementation window of 12 months will come into effect from this date until

29th June 2024. This implementation window is to ensure contracting authorities and contractors/suppliers have sufficient time to integrate the new policy in forthcoming procurements.

Guidance for Contracting Authorities

6. The contracting authority should continue to ensure that appropriate protective security controls are in place in new and existing contracts in line with the GSCP for the protection of the assets against compromise. To determine the security controls likely to be required in any given situation, careful consideration needs to be given to the type and value of the assets involved and the nature and scale of threats to them.

7. The contracting authority has a responsibility to notify its existing contractors that the GSCP has been updated and make them aware of any potential changes that might be required and any impacts this may have on the classified information processed under the contract. Key updates to the policy include:

    a. Updated definitions for the three classification tiers OFFICIAL, SECRET and TOP SECRET.

    b. Baseline security behaviours for the three classification tiers and further security controls for when the -SENSITIVE marking is applied to OFFICIAL information. OFFICIAL-SENSITIVE has not been introduced as a new classification tier.

    c. Updated list of principles everyone handling HMG information should follow.

    d. Standardised additional markings (including: handling instructions, descriptors, prefixes and national caveats).

    e. New guidance for remote working when handling HMG information,

    f. Updated guidance on aggregation and further considerations.

8. The majority of these updates are minor changes which will not require a contract variation to existing contracts. However, there might be some instances where specific contracts need to be reviewed.

9. The contracting authority has a responsibility to notify its contractors if they have introduced any new additional markings outside those set out by the

GSCP. The contracting authority should manage any potential changes together with the contractor.

10. If the contracting authority wishes to set additional controls which go above the baseline set out in the GSCP, the contracting authority's intention to do so should be made known during the pre-contract stage. This is so that potential bidders are aware of any additional requirements during the invitation to tender stage. Any additional controls must be proportionate and based on the risk tolerance of the HMG organisation awarding the contract.

11. Any added security controls should meet the contracting authority's personnel, physical, information management and cybersecurity requirements, and should be based upon the principles of risk assessment and management. Specific security controls, which are above the baseline security controls found in the GSCP, must be clearly specified to the contractor.

12. A contracting authority should notify their contractors of the classifications requirements that are in effect for the contract in question where sensitive information is being processed, stored or managed. This document should provide a detailed description of the information, material or data being processed, stored or managed under the contract, the classification for each security aspect and any specific handling requirements.

13. If appropriate, considering the need-to-know principle and as agreed with the contracting authority, instructions (this may take the form of a Security Aspects Letter or similar) should be issued between the contractor and any subcontractor. This document, sent to a subcontractor, should only include the security aspects of the information, material or data which the subcontractor is accessing, managing, storing and/or processing.

Guidance for Contractors

14. For any new contracts awarded, contractors will use the updated GSCP to protect HMG classified information it receives and handles. The classification of historic information only needs to be updated in line with the GSCP upon instruction and agreement with the contracting authority.

15. UK contractors should follow the minimum baseline security requirements for OFFICIAL, OFFICIAL information marked OFFICIAL-SENSITIVE, SECRET or TOP SECRET outlined in the GSCP and the security requirements as set out by the contracting authority.

16. Contractors should contact their contracting authority if they have any questions about the required protective security measures that are required to be compliant with their contract.

17. Should a contractor subcontract all or part of a contract involving classified information, that subcontractor should be expected to follow the GSCP with the same conditions as expected of the prime contractor. Subcontractors' obligations concerning the protection of classified material must be the same as those for the main contractor.