Security scrutiny

Introduction

Proposals dealing with information that is **EU-classified** under the Commission's internal Rules of Procedure are subject to security scrutiny. For details, see the Commission's security rules, including the Practical Classification Guide (Appendix 2).

When are proposals subjected to security scrutiny?

Security scrutiny takes place periodically.

How are proposals scrutinised for security?

The scrutiny check is not a full security check on all the aspects of a project which might have a bearing on security. It simply identifies projects involving information that is sensitive from the security point of view and, where appropriate, classes their deliverables as 'classified deliverables').

Security scrutiny may lead to '**security requirements**'. If applicable, these will be included in the grant agreement as a **Security Aspect Letter** (SAL) and the annexed **Security Classification Guide** (SCG).

- Security scrutiny does not relate to activities involving dual-use goods or dangerous materials and substances.

Security scrutiny applies to most parts of Societal Challenge 7 (Secure Societies), but it may also apply to other proposals, e.g. if

- the applicants state in the submission forms that the proposal is 'security-sensitive' (i.e. that it involves EU-classified information)
- the work programme flags up the topic as one that could result in security sensitive projects
- the Commission detects or suspects that
    - classified information is being used as background or
    - the project will generate classified information.

How is the security scrutiny process organised?

Scrutiny is the responsibility of the Security Scrutiny Working Group, comprising experts appointed in close cooperation with the relevant Programme Committee and the competent

national security authorities. It is chaired by a Commission representative.

RESULTS OF SECURITY SCRUTINY - IMPLICATIONS

If necessary, your proposal will undergo security scrutiny. In this case the Security Scrutiny Working Group will determine the level of sensitivity of your proposal and check whether all security aspects are being handled appropriately.

We will inform you of the outcome of the security scrutiny at the beginning of the grant preparation phase or as soon as possible afterwards. The possible outcomes are:

- classification is not necessary
- classification is necessary
- the proposal is too sensitive to be funded

Classification not necessary

The project will be handled in the same way as all the others under the same call for proposals. No further action is needed.

Classification necessary

In such cases, security requirements are incorporated in Annex 1 to the grant agreement. These requirements and the project's level of security classification are set out in the **Security Aspect Letter** (SAL) and the **Security Classification Guide** (SCG) annexed to it.

Proposal too sensitive to be funded

Security scrutiny may reveal that the information to be used or generated by the project is too sensitive, or that the applicants lack the right experience, skills or authorisations to handle classified information at the appropriate level.

- In such cases, funding is refused and the proposal rejected.

If this happens, you will be notified of

- the decision to reject your proposal
- the grounds for the decision
- how you can appeal against it.