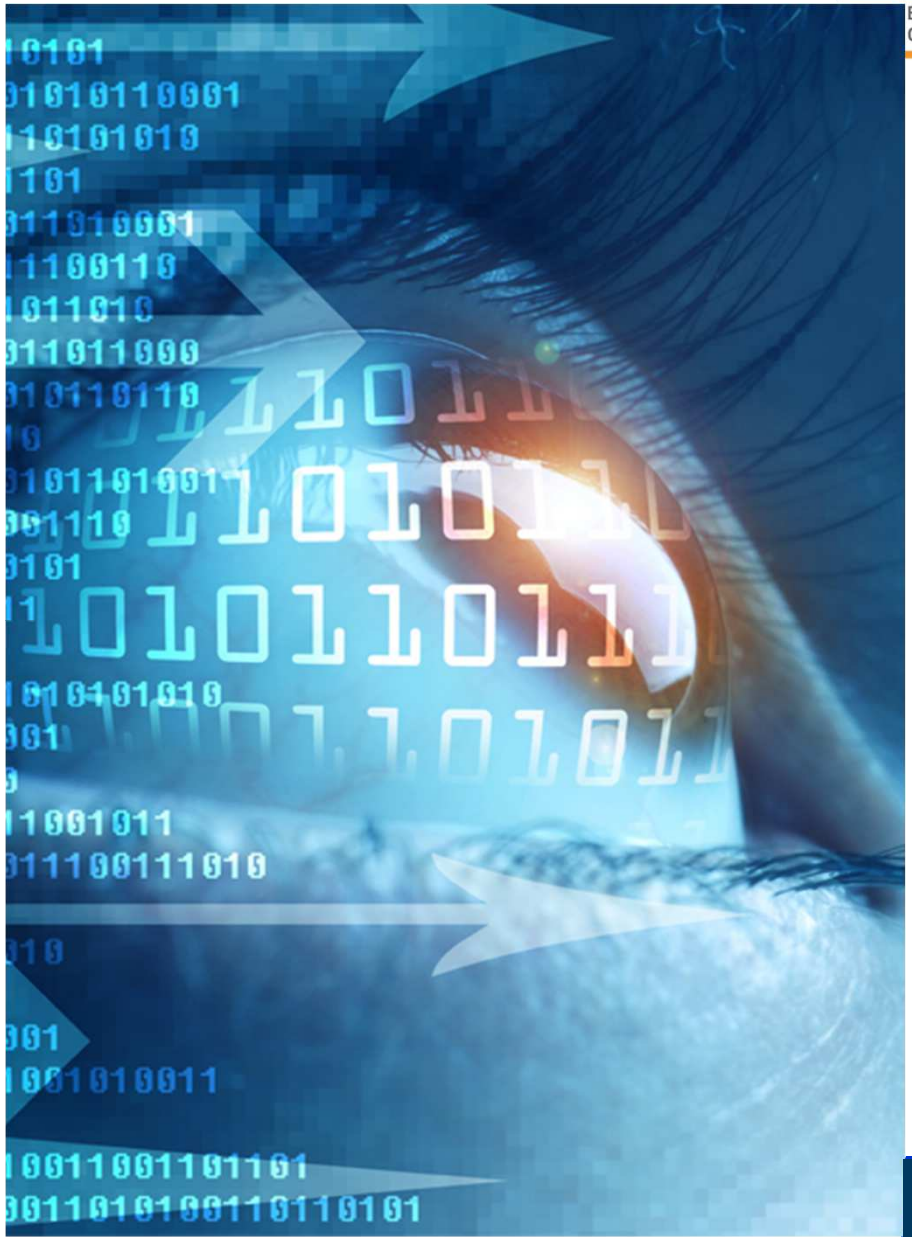


European Commission

DG Migration and Home Affairs

Security-Related Obligations

Infoday
6 March 2017

Brussels

Annieke LOGTENBERG

Legal Officer
DG Migration and Home Affairs

Security-related obligations concern:

- Security recommendations
- Data or information used or produced by a research project which requires protection against unauthorised disclosure (*classified information*)
- Dual-use goods or dangerous materials and substances (subject to export- or transfer control)
- Information or materials subject to national security restrictions

Security Recommendations

- Security recommendations: a variety of measures aimed at improving security (e.g. limited dissemination of deliverables, creation of a Security Advisory Board, etc.)
- Security recommendations may be the result of the Security Scrutiny, or reflect the project proposal
- In case of security recommendations optional article 37.1 will be inserted in the Grant Agreement
- Non-compliance with the security recommendations may lead to reduction or termination of the grant and/or sanctions (Art. 37.4)

EU Classified Information (EUCI)

Definition of EU Classified Information (EUCI)

EUCI: any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

Legal framework

- Commission Decision 2015/444/EC on the security rules for protecting EU classified information

- National laws

Applicants are already asked at the proposal stage if their project uses/produces EUCI. The Security Scrutiny Group may also request classification.

Applicants cannot submit a "classified proposal" (the IT tool does **NOT** allow applicants to include classified information in a proposal)

EUCI in research projects

- Projects may use EUCI as **background** and/or produce EUCI (**foreground**) – in both cases classification is necessary!
- Classification is always specified at deliverable-level. Different deliverables in one project can have different classification levels:
  - RESTREINT UE/EU RESTRICTED
  - CONFIDENTIEL UE/EU CONFIDENTIAL
  - SECRET UE/EU SECRET
  - TRES SECRET UE/EU TOP SECRET *(not applicable)*
- Classification has implications: classified deliverables require a special treatment, beneficiaries need to meet certain conditions and optional Article 37.2 will be inserted in the Grant Agreement
- Non-compliance with Art. 37.2 may lead to reduction or termination of the grant and/or sanctions (Art. 37.4)

EUCI and proposals involving participants from third countries

- General rule: EUCI is limited to EU Member States
- Projects using/producing EUCI can include participants from associated or third countries
- Countries having a security agreement with the EU (Council level) could refer to that security agreement for handling EUCI
- *Special MoU (Memorandum of Understanding) could be agreed between the countries involved in the handling of sensitive information of a project limited to that project*

➢ Participants from associated countries and/or third countries without a Security Agreement with the EU can participate in projects involving/producing EUCI <u>if no access to sensitive information has been foreseen</u>

What happens after submission?

As stated in the H2020 Grants Manual, the following proposals will be subject to security scrutiny:

- ✓ **All proposals belonging to topics in the Secure Societies WP**
- ✓ **All proposals belonging to calls or topics marked potentially security sensitive**
- ✓ **Proposals of any other WP, call and topic marked as raising (potential) security issues by the applicant**
- ✓ **Proposals identified as raising (potential) security issues by the responsible Project Officer or Call Coordinator**

What is the Security Scrutiny Procedure?

Proposals that might raise security concerns undergo an extra check before the start of the Grant Agreement Preparation: the Security Scrutiny

Objectives of the Security Scrutiny:

- Identify security concerns
- Assess if classified information will be used/produced, and specifying which deliverables are concerned at which classification level is required
- Verify if the security issues have been properly addressed by the applicants

The outcome of the Security Scrutiny is a recommendation from the experts to the Commission. Based on the opinions of the experts, the Commission decides on the security recommendation/classification. Applicants receive the results of the Security Scrutiny with the "information letter".

The Security Scrutiny is NOT a technical re-evaluation of the proposal

Who carries out the Security Scrutiny?

The Security Scrutiny is done by the Security Scrutiny Group, a group of security experts nominated by the EU Member States and H2020 associated countries, chaired by the European Commission (DG HOME).

Each proposal is scrutinised by the experts representing the EU Member States and Associated Countries involved in the proposed project.

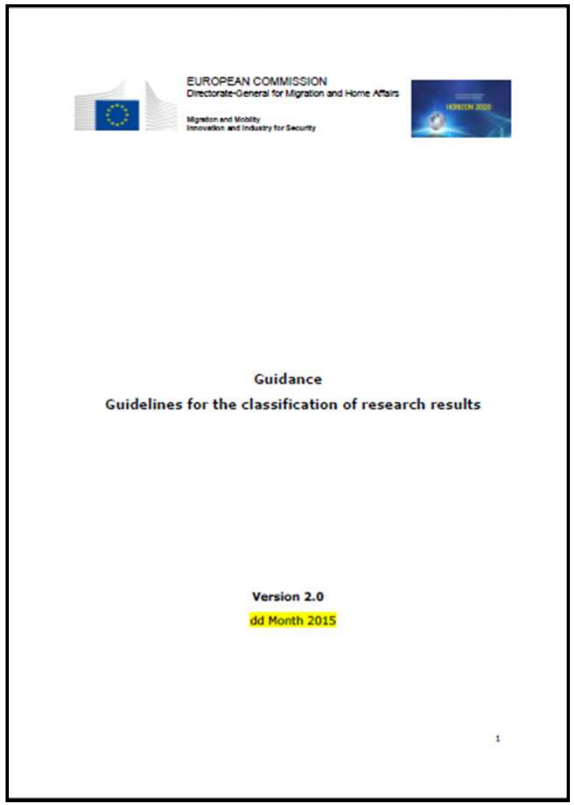
Experts use the **Guidelines for the classification of information in research projects** to guide them during the procedure. Classification of information used in and/or produced by research projects will normally depend on two parameters:

1) the **subject** of the research results (i.e. explosives, CBRN, infrastructure and utilities, border security, intelligent surveillance, terrorism, organised crime, digital security and space).

2) the **type** of the research results (i.e. threat assessments, vulnerability assessments, specifications ,capability assessments, incidents/scenarios) .

European Commission

Guidelines for the Classification of Information in Research Projects


EUROPEAN COMMISSION
Directorate-General for Migration and Home Affairs

Migration and Mobility
Innovation and Industry for Security

Guidance

Guidelines for the classification of research results

Version 2.0

dd Month 2015

1

Content

Example:

Subject: ***'Critical infrastructures and utilities' are assets and systems (eg buildings and urban areas; energy, water, transport and communications networks; supply chains; financial infrastructures, etc) which are essential for maintaining vital social functions (health, safety, security, economic or social well-being).***

Type: ***How to deal with threat assessments?***

Analyses of man-made threats to infrastructure should be classified RESTREINT UE/EU RESTRICTED If they add value (eg by prioritising threats), they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

DG Migration and Home Affairs

Outcome of the Security Scrutiny

The result of the security scrutiny for a given proposal may be:

→No security concerns (NSC): go ahead with grant agreement preparation;

→No classification, but recommendations for the grant agreement preparation (REC);

→Classification and recommendations for the grant agreement;

Classification at RESTREINT UE/EU RESTRICTED level (UE-RES)

Classification at CONFIDENTIEL UE/EU CONFIDENTIAL level (UE-CON)

Classification at SECRET UE/EU SECRET level (UE-SEC)

→Recommendation not to finance the proposal

In this extreme case, a very clear justification must be provided and demonstrated (eg because some participants do not have the necessary experience and skills for the management of expected EU classified information)

Applicants receive the results of the security scrutiny procedure together with the "Information Letter" via the Participant Portal.

Security-related obligations: Grant specificities

For projects with security recommendations:

→ Optional Article 37.1 will be inserted in the GA

For projects with classified deliverables (EUCI):

→ Optional Article 37.2 will be inserted in the GA
+ Annex 1 (DoA) part B - section 6:

- SAL (Security Aspect Letter)
- SCG (Security Classification Guide)

For projects involving dual-use item:

- Optional Article 37.3 will be inserted in the GA

If any of the abovementioned Articles are inserted in the GA, an additional article on compliance (37.4) will also be inserted.

Tips and Instructions for Applicants

- Carefully read the text of the WP, call and topic. Is there any information on EUCI or security risks?
- If you are using Classified background information, make sure you clearly highlight this in the proposal. Specify the classification level and which deliverables are concerned.
- Check the 'Guidelines for Classification of Information in Research Projects' to see if your project might involve EUCI
- Does your project use or produce EUCI? Reply "YES" to the question on security issues and classified information in section 6 ("Security") in part B.
- Mark classified deliverables (CI) in the table of deliverables in part A and specify the level of classification of each classified deliverable.
- Check if your project partners have the appropriate security clearances. Indicate this in the proposal.
- For third country partners: check if there is a security agreement
- Describe any measures you are taking to promote security (e.g. creating a security advisory board) in the relevant section (6) in part B.

References

- Guidelines for the classification of information in research projects:

https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/secur/h2020-hi-guide-classif_en.pdf

- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0444

- All sections on the Security Scrutiny Procedure in the Online Manual:

http://ec.europa.eu/research/participants/docs/h2020-funding-guide/index_en.htm