

Security Related Obligations

**Information Day
26 March 2015
REA - Brussels**

Annieke Logtenberg

DG Migration and Home Affairs

Directorate "Migration and Mobility"

Unit B.4. Innovation and Industry for Security

“Sensitive” Projects: what is a sensitive project?

A “sensitive” project is handling:

1. Information and materials subject to **export- or transfer-control** or
2. Data or information requiring protection against unauthorised disclosure: **classified information** or
3. Information or materials subject to **national security restrictions**

No “classified” proposals are allowed in the call

*(SEP IT tool **does NOT allow** for classified information in a proposal)*

*BUT: a proposal could lead to a “sensitive” project
(i.e. a project that uses classified/sensitive background
and/or produce classified/sensitive foreground)*



Export-control/Dual uses issues: Principles and Legal basis

- 'dual-use items' shall mean items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.
 - COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.
(Official Journal L143 29/05/2009)
 - Article 4 (428/2009) and National laws (some additional restriction may apply)
- **Please check 428/2009 annexes**
- An explanatory note on the control of export for "dual-use items" will be available on the website

Classification issues (confidentiality of results): Principles and Legal basis

Principles

- Need to know
- Clearance
- Originator (the Commission) consent

Legal basis

- Commission Decision 2015/444/EC
(Official Journal L72, 17.3.2015)
- National laws

Role of the Security Scrutiny Group

- Decision of the H2020 Secure Societies Programme
Committee (defines role, responsibilities & composition)

See also the rules for submission, evaluation, etc.

http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/pse/h2020-guide-pse_en.pdf

Sensitive Projects: Sensitive proposals with non-EU participants

- EU classification is limited to EU Member States
 - Sensitive projects 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 sensitive information and material
 - *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*
- *No restriction for the participation to sensitive projects for associated countries and from third countries without Security Agreement with the EU **if no access foreseen to sensitive information***



"Sensitive" projects: use of classified information

- *Check the "Guidelines for Classification of Research Results"*
- *If known at the proposal stage:*
 - If the use of classified information is known, the answer to the question in part B (section 6) of the proposal should be "YES". The table of deliverables must specify the **level of classification (CI)** for each deliverable (make sure that you do not confuse the level of classification with the level of dissemination)
 - A **draft Security Aspect Letter (SAL)** + a **draft Security Classification Guide (SCG)** should be attached to the proposal

“Sensitive” Projects: Security Scrutiny Procedure

For most of the project's proposals of the selection list:

- The Security Scrutiny Group will be requested (via their national security authority representative) to **verify** that all **security aspects** are properly **addressed** and to **reach an agreement** among themselves.
- the scrutiny procedure is done, in a 2 months period, following the technical evaluation and before the start of the Grant Agreement Preparation of the projects.

The results of the scrutiny could be:

- go ahead with Grant Agreement Preparation;
- recommendations for the Grant Agreement Preparation without classification;
- recommendations for the Grant Agreement Preparation with classification;
- Recommendation not to finance the proposal

*Proposers receive the conclusions of the scrutiny procedure with the
“Information letter” via the Participant Portal*

Sensitive Projects: Some recommendations

- Be **serious** about the sensitivity declaration
- Export-control **risks** have to be described - See note on the Participant Portal
- Consider carefully the requirements for accessing sensitive information/material in a project (**limit** it as far as possible)
- For all partners, check if you have the appropriate **Security Clearances**
- For non-EU countries find out if there are some **security agreement** between your country and EU
- Find references to **all applicable EU and national legislation**
- Contact your National Contact Point (**NCP**) – see the Participant Portal
- Contact your **NSA** for sensitive proposals (OJ L193 of 23.7.2005 p.31-36)

Sensitive Projects: Grant specificities

For projects with classified deliverables:

- Model Grant Agreement:
optional clause 37.1 and/or 37.2
- Annex 1 (DoW) part B - section 6:
 - SAL (Security Aspect Letter)
 - SCG (Security Classification Guide)

For projects involving dual-use item:

- Model Grant Agreement:
optional clause 37.3



“Sensitive” Projects: Grant specificities

ARTICLE 37 — SECURITY-RELATED OBLIGATIONS

37.1 Activities raising security issues (old clause 24)

Before disclosing results of activities raising security issues to a third party (including affiliated entities), a beneficiary must inform the coordinator — which must request written approval from the Commission.

37.2 Classified deliverables (old clause 21 and 22)

Activities related to ‘classified deliverables’ (see Annex 1) must comply with the ‘security requirements’ (Security Aspect Letter (SAL) and the Security Classification Guide (SCG)) set out in Annex 1 until they are declassified.

Action tasks related to classified deliverables may not be subcontracted without prior explicit written approval from the Commission.

The beneficiaries must inform the coordinator — which must immediately inform the Commission — of any changes in the security context and — if necessary — request for Annex 1 to be amended (see Article 55).

37.3 Activities involving dual-use goods or dangerous materials and substances (new clause)

Activities involving dual-use goods or dangerous materials and substances must comply with applicable EU, national and international law. Before the beginning of the activity, the coordinator must submit to the [Commission][Agency] (see Article 52) a copy of any export or transfer licences required under EU, national or international law.

Sensitive Projects: Grant specificities

Annex 1 (DoW) : SAL (Security Aspect Letter)

- The performance of the grant agreement will involve information classified **CONFIDENTIAL UE**.
- **[A Facility Security Clearance is required]**.
- Persons who need to access EU classified information must **[have an EU personal security clearance and]** be briefed as to their responsibility for security^[1].
- The beneficiaries concerned shall take all measures prescribed by the National Security Authority/Designated Security Authority (NSA/DSA) for safeguarding EUCI.
- The beneficiaries concerned shall appoint a Facility Security Officer (FSO).
- The beneficiaries concerned, through the FSO, shall maintain a continuing relationship with his NSA/DSA.
- The beneficiaries concerned shall maintain a record of his employees taking part in the project and who have been cleared for access to EUCI.
- EU classified information for the purpose of these instructions is to be understood as information classified and marked **CONFIDENTIAL UE** or its equivalent national classification.
- Information generated by the beneficiaries concerned will require EU classification and marking.

Continued on next slide

Sensitive Projects: Grant specificities

Annex 1 (DoW) : SAL (Security Aspect Letter – continued)

- The beneficiaries concerned must obtain the approval of the Contracting Authority before beginning Grant Agreement Preparations with a view to subcontract.
- The Commission Security Directorate may - in co-ordination with the responsible NSA/DSA - conduct inspections at beneficiaries' facilities concerned to verify the implementation of the security requirements for the handling of EUCI.
- The beneficiaries concerned shall report all cases of unauthorised disclosure or loss of EUCI to the responsible NSA/DSA, the Commission Security Directorate and the Contracting Authority.
- All EUCI provided or generated under this grant agreement shall continue to be protected in the event of termination of the grant agreement.
- The beneficiaries concerned shall undertake not to utilise the EUCI provided or generated, other than for the specific purpose of the grant agreement XXXXXX
- Handling and storage instructions for information classified **CONFIDENTIAL UE** [2]

[1] Commission Decision (EU, Euratom) 2015/444

[2] Idem above note 1

Annex 1 (DoW) : SCG (Security Classification Guide)

Annex to the Security Aspects Letter (SAL) Security Classification Guide (SCG)

Production of classified <u>results</u>					
Subject	Classification level	Beneficiaries involved in production or wanting to access			
		Name	Responsibility	Date of production	Comments including purpose of the access and planned use
number and name of the deliverable	proposed Classification level	entities name only	security manager/main contributor		
		entities name only	contributor		
		entities name only	contributor		
		entities name only	reader only		
		entities name only	reader only		
number and name of the deliverable	proposed Classification level	entities name only	security manager/main contributor		
		entities name only	contributor		
		entities name only	contributor		
		entities name only	reader only		
number and name of the deliverable	proposed Classification level	entities name only	security manager/main contributor		
		entities name only	contributor		
		entities name only	contributor		
		entities name only	reader only		
number and name of the deliverable	proposed Classification level	entities name only	security manager/main contributor		
		entities name only	contributor		
		entities name only	contributor		
		entities name only	reader only		

Further information

Participant Portal

<http://ec.europa.eu/research/participants/portal/desktop/en/home.html>

- **Work Programme**
- **Call for proposals**
- **Guidance documents**
- **Explanatory notes on specific issues**

All issues:

REA-security-research@ec.europa.eu

Security issues:

home-security-research@ec.europa.eu