Horizon Europe

Security Appraisal Procedure

Maria Eleni Chondrogianni
Legal Officer/ Security Appraisal
DG Migration and Home Affairs
21/05/2021

Security Appraisal in HE: novelties!

- **Legal basis** in HE Regulation (Art. 20); assessing security issues in research proposals is not only a necessity, but also **a legal obligation**!
- Standardised process for **all activities in HE**.
- **Security Self-assessment** by the applicants in the proposal template for **all HE proposals**.
- Possibility to flag a **topic as security sensitive** in the Work Programme, which influences the routing of the process.
- **Full updated set of guidance material** for all involved actors (applicants, POs, beneficiaries, national experts).

Security Appraisal in HE: Legal Basis

Horizon Europe Regulation Art. 20 on Security:

- **Art. 20 (1)**: *“Actions … **shall comply with the applicable security rules** and in articular rules on **protection of classified information** against unauthorised disclosure, including compliance with any relevant **national** and **Union law**.”*

- **Art. 20 (2)**: “*Where appropriate, proposals shall include **a security self-assessment** identifying any security issues and detailing how these issues will be addressed in order to meet the relevant national and Union law.”*

- **Art. 20 (3):** *“Where appropriate, the Commission or funding body shall carry out **a security scrutiny** for proposals raising security issues.”*

Security Appraisal in HE: overview of the process 1/7

The **Security Appraisal Procedure** concerns all activities funded under Horizon Europe and includes **three main steps**:

1. The **Security Self-assessment** by the Applicant – all proposals;
2. The **Security Review** by the granting authority, the Commission and national security experts- a selection of proposals;
3. The **Security Checks**, by the Commission or the relevant funding body, where appropriate, during or after the life of the project.

Security Appraisal in HE: overview of the process 2/7
Security Self-assessment

- **All HE proposals** will contain a **Security Issues Table**, which is **mandatory** for all applicants.
- When preparing a proposal, the applicant is required to reply to the questions of the **Security Issues Table**. In case the proposal is submitted under a **security sensitive topic**, the applicant is also required to complete a **Security Section** with more information on specific security issues.
- The Security Issues Table includes **3 main questions**:
  - *Does this activity involve information and/or materials requiring protection against unauthorised disclosure (classified information)?*
  - *Does this activity have the potential for misuse of results?*
  - *Does this activity involve information and/or materials subject to national security restrictions?/Are there any other security issues that should be taken into consideration?*
- Information and guidance for the applicants can be found in the *How to complete your security self-assessment and security section guide.*

Security Appraisal in HE: overview of the process 3/7
Security Review

- Only **proposals above threshold and considered for funding** will undergo a Security Review.
- The Security Review is organised based on whether the **topic is security sensitive** or not and it can lead to **security requirements** that become contractual obligations.
- The Security Review focusses on the **compliance with security rules** and in particular, on the **protection of sensitive and classified information** against unauthorised disclosure.
- The **objective** of the Security Review is to identify **security issues** that could emerge from the research and **potential misuse** of research results and address them via appropriate **mitigation measures**.

Security Appraisal in HE: overview of the process 4/7
Security Review

The **Security Review includes three steps**:

1. The **Security Pre-screening** carried out by **qualified staff of the granting authority**, during the scientific evaluation or soon after;

2. The **Security Screening** performed by **qualified staff of the European Commission** (DG HOME), after the scientific evaluation and before the signature of the Grant Agreement;

3. The **Security Scrutiny** conducted by the **Security Scrutiny Group**, comprised of national security experts, after the scientific evaluation and before the signature of the Grant Agreement.

Security Appraisal in HE: overview of the process 5/7
Security Review

The **Security Pre-screening** is carried out in the following cases:

- If the proposal has been submitted under a topic not flagged as security sensitive and the **applicant has replied positively to at least one** of the **questions in the Security Issues table**;

- If the proposal has been submitted under a topic not flagged as security sensitive and the **applicant has replied negatively to all the questions** in the Security Issues table, **but** the **granting authority has**, nevertheless, **detected security issues**.

The **Security Screening** is **automatically performed to all the proposals** that have gone through **the Security Pre-screening**. During this phase, DG HOME will assess the results of the pre-screening and decide on the possible launch of the Security Scrutiny.

Security Appraisal in HE: overview of the process 6/7
Security Review-Security Scrutiny

The **Security Scrutiny Procedure (SSP)** will be **carried out in the following cases**:

- **Automatically,** if the proposal has been submitted under a **topic flagged as security sensitive**;
- In other cases, if the **Security Screening has concluded that the proposal is very likely to raise security issues** for which mitigation measures should be proposed.

Objectives:

- **identify security concerns** in a certain proposal;
- **assess if sensitive or classified information will be used or produced** by a certain project;
- verify whether the **security issues have been properly addressed** by the applicant; and
- **propose recommendations** in order to properly address the identified security issues.

Purpose: to **address potential misuse** of project results (e.g. results that could be channelled into crime or terrorism or results that could adversely affect critical infrastructure).

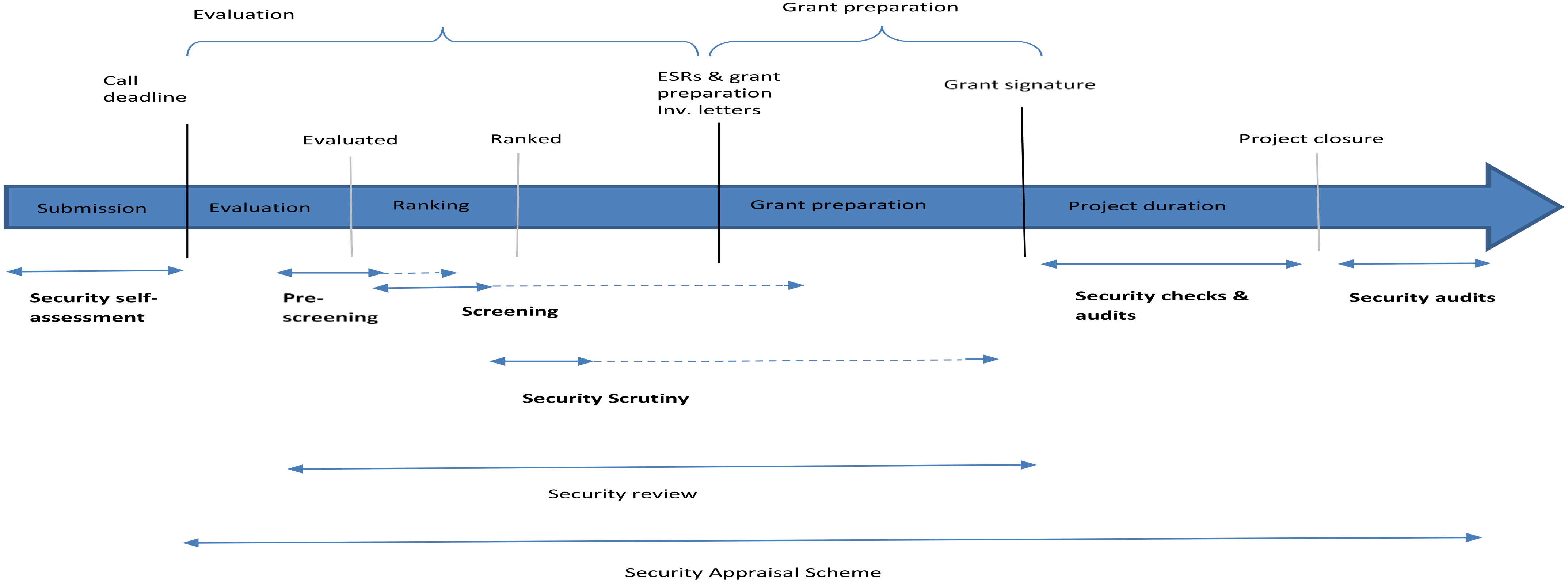
- For additional information see the *guidance note on potential misuse of research*.
- The SSP is **not a technical re-evaluation** of the proposal.

Security Appraisal in HE: overview of the process 7/7
Security Review-Security Scrutiny

The possible **outcomes of the Security Scrutiny** are:

- **No security concern-** No security issues were identified in the proposal. No security section in the Grant Agreement.
- **Security recommendations and/or security classification**- The Security Scrutiny Summary Report (SecScrSR) will list one or more **security requirements** that should be set out in the Security Section of Annex 1 of the Grant Agreement and may include:
  - security recommendation to **limit the dissemination level** of certain deliverables for security reasons;
  - **classification** of certain deliverables at a certain level;
  - appointment of a **Project Security Officer (PSO)** in case of classification;
  - establishment of a **Security Advisory Board (SAB)**;
  - **other** security recommendations.
- **Proposal too sensitive to be funded**- The 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 is rejected.

Security Appraisal Scheme



European Commission

Thank you !

In case of questions please contact:
HOME-SECURITY-APPRAISAL@EC.EUROPA.EU