ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI

@CDTIoficial

Apectos de Seguridad e información confidencial…

… a nivel de propuesta

HORIZONTE EUROPA

@HorizonteEuropa

Marina Martínez-Garcia
NCP Cluster-3 Civil Security Horizon Europe
marina.cdti@sost.be

CDTI Centro para el Desarrollo Tecnológico Industrial | E.P.E.

El escrutinio de seguridad en HE sigue igual...

Main novelties in HE

- **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.

Cuestionario en la parte-A de todas las propuestas, así como una sección dedicada en la parte-B, solamente si respondes "YES" en alguna pregunta!

HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices

| Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 4.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply:
	The following additional eligibility criteria apply:
	This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [13] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Security Appraisal in HE: overview of the process

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; **→ Se debe completar part-A & part-B de la template!**

2. The **Security Review** by the granting authority, the Commission and national security experts- a selection of proposals; **→ Para los topics de Cluster-3 & topics de Space the Cluster-4; así como para cualquier otro topic en los que haya una duda potencial! → Proceso posterior a la evaluación técnica y se realiza en paralelo a la revision ética.**

3. The **Security Checks**, by the Commission or the relevant funding body, where appropriate, during or after the life of the project. **→ Comprovación del cumplimiento de todas las condiciones para manejo de información sensible y posibilidad de hacer modificiaciones en la clasificación, si necesario!**

Possibility to flag a **topic as security sensitive** in the Work Programme influences the routing of the process (**p.e., delays in the GA signature**). At present, the security sensitive topics are from the **Civil Security, ICT related topics (p.e. quantum) and the some space calls.**

Security Appraisal in HE: overview of the process
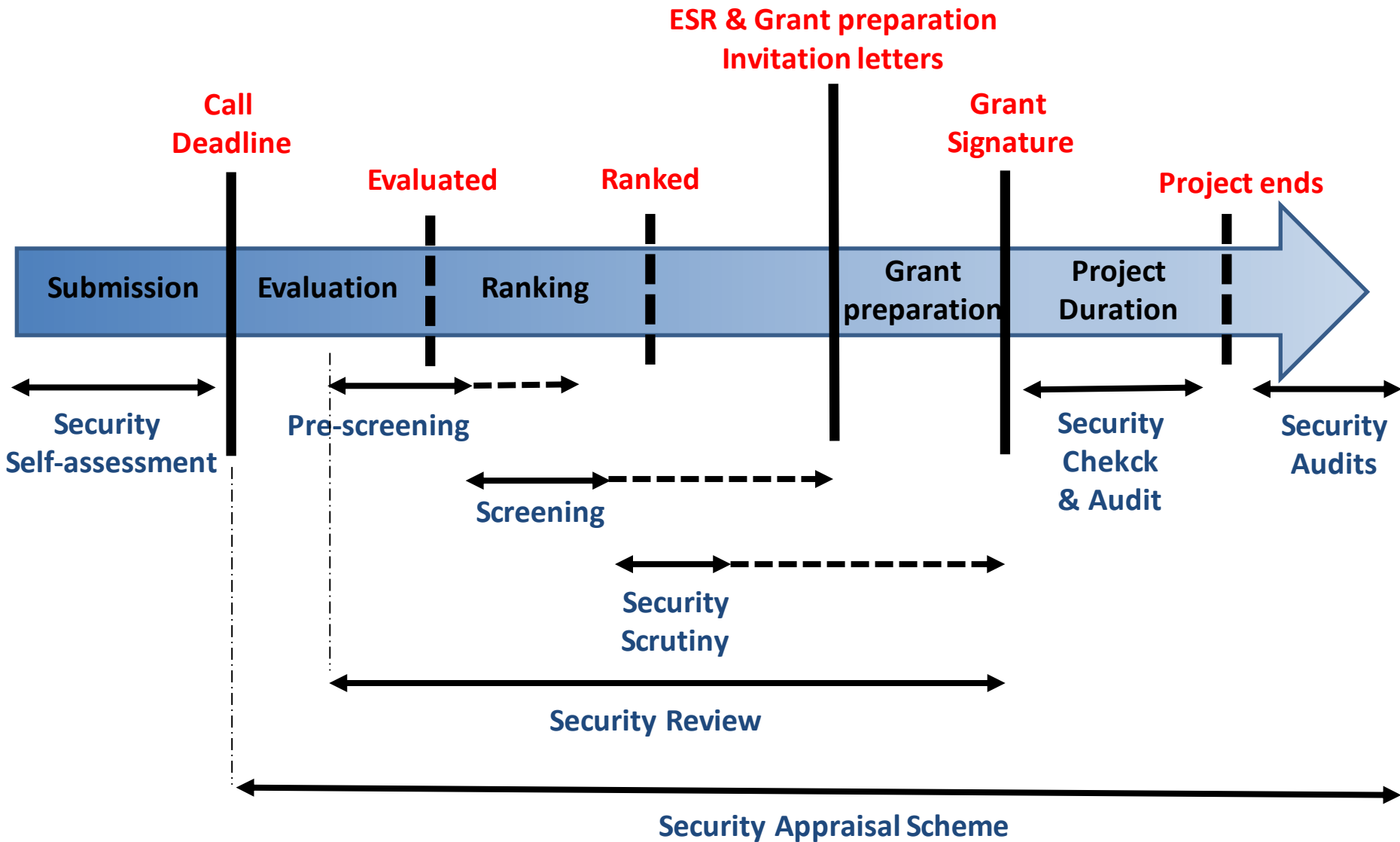
Recordemos cómo es el proceso de evaluación…
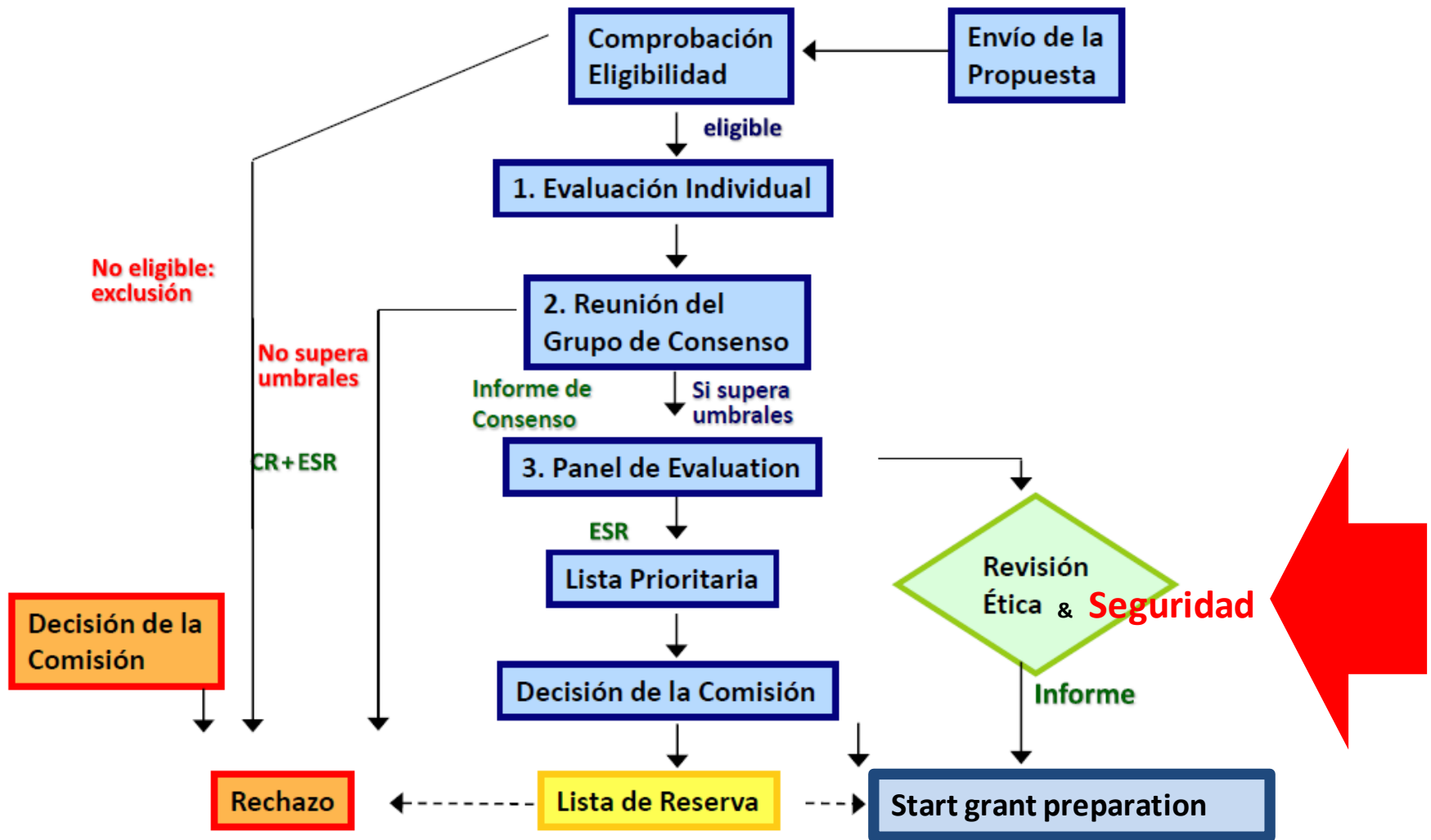
Overview of the process: Security Self-assessment

The **Security Issues Table (part-A)** includes **3 main questions**:

- **Involvement of information/materials requiring protection against unauthorised disclosure** (classified information) and participation of non-EU countries.

- Potential for **misuse of results**.

- **National security restrictions** or other security issues that should be taken into consideration.

Si la respuesta es "YES" en alguna de las preguntas → When preparing a proposal, under a **security sensitive topic**, the applicant is also required to complete a **Security Section in part-B** with more information on specific security issues. Information and guidance can be found in the *Security Section template*.

Attention: The **proposals must not contain** classified information (the IT tool does **NOT** allow applicants to include classified information in a proposal).

Overview of the process: Security Self-assessment

HE proposals will contain a **Security Issues Table, mandatory for all applicants in <u>Part-A</u>.** Information and guidance can be found in the *How to handle security-sensitive projects*.

Security issues table

Please indicate, by answering Yes or No to all of the questions in the below table, if the proposed activity will use and/or generate information which might raise security concerns. If an answer is Yes, then indicate in the adjacent box at which page in your full proposal further information relating to that issue can be found.

1. EU classified information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?		○ Yes ○ No	
If YES:	Is the activity going to use classified information as background[3] information?	○ Yes ○ No	
	Is the activity going to generate EU classified foreground[4] information as results?	○ Yes ○ No	
Does this activity involve non-EU countries?		○ Yes ○ No	
If YES:	Do participants from non-EU countries need to have access to EUCI?	○ Yes ○ No	
	Do the non-EU countries concerned have a security of information agreement with the EU	○ Yes ○ No	
2. MISUSE			Page
Does this activity have the potential for misuse of results?		○ Yes ○ No	
If YES:	Does the activity provide knowledge, materials and technologies that could be channelled into crime and/or terrorism?	○ Yes ○ No	
	Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery?	○ Yes ○ No	
3. OTHER SECURITY ISSUES			Page
Does this activity involve information and/or materials subject to national security restrictions?		○ Yes ○ No	
If yes, please specify: *(Maximum number of characters allowed: 1000)*			

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI

@CDTIoficial
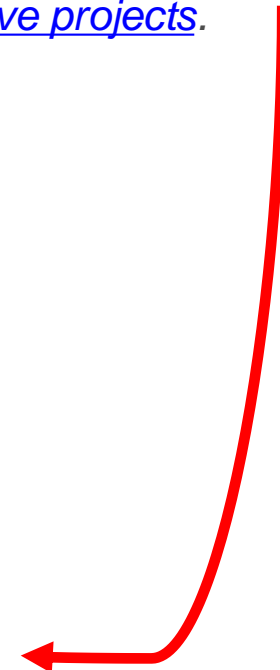
Ejemplo real de si la respuesta es "YES" en alguna de las preguntas en la parte-A…

Administrative forms

Proposal ID: **101070xxx**

Acronym: **FANTASTIC**

Security issues table

1. EU Classified Information (EUCI)[2]			Page
Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)?	● Yes	○ No	14
Is the activity going to use classified information as background[3] information?	○ Yes	● No	
Is the activity going to generate EU classified foreground[4] information as result?	● Yes	○ No	14
Does this activity involve non-EU countries?	● Yes	○ No	1
Do participants from non-EU countries need to have access to EUCI?	● Yes	○ No	1
Do the non-EU countries concerned have a security of information agreement with the EU?	● Yes	○ No	1
2. Misuse			**Page**
Does this activity have the potential for misuse of results?	● Yes	○ No	14
Does the activity provide knowledge, materials and technologies that could be channeled into crime and/or terrorism?	● Yes	○ No	14
Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery?	○ Yes	● No	
3. Other Security Issues			**Page**
Does this activity involve information and/or materials subject to national security restrictions? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	● No	
Are there any other security issues that should be taken into consideration? If yes, please specify: (Maximum number of characters allowed: 1000)	○ Yes	● No	

[2] According to the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, "European Union classified information (EUCI) means 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".

[3] Classified background information is information that is already classified by a country and/or international organisation and/or the EU and is going to be used by the project. In this case, the project must have in advance the authorisation from the originator of the classified information, which is the entity (EU institution, EU Member State, third state or international organisation) under whose authority the classified information has been generated.

[4] EU classified foreground information is information (documents/deliverables/materials) planned to be generated by the project and that needs to be protected from unauthorised disclosure. The originator of the EUCI generated by the project is the European Commission.

EXAMPLE

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI

@CDTIoficial

… Entonces debes rellenar la Security Section en la parte-B

Horizon Europe Programme

Proposal Template (Part B)

Security Section

Version 1.1

16 June 2021

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021

EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

IMPORTANT NOTICE

This Security Section must be completed in accordance with the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects.

If part of your Application Form, this section must be pre-filled already at proposal stage (not counted towards the page-limit). If not part of the Application Form, it will be provided to you during grant preparation.

It will then become part of your Grant Agreement (in Annex 1, Description of Action) and will become binding.

⚠ Do NOT delete any text. All the subsections should remain, but marked as not applicable (N not relevant for your project.

HISTORY OF CHANGES		
Version	Publication date	Changes
1.0	10.03.2021	• Initial version
1.1	16.06.2021	• Formatting and alignment with other security guidance
		•

0

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI
@CDTIoficial

…Entonces debes rellenar la Security Section en la parte-B, que consta de 3 sub-secciones…

Page 1 (left):

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021

EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

1. Summary of the project security issues

After giving due consideration to Horizon Europe guidance for Security aspects for considering relevant security subject matters, CROSSCON has made the assessment that it will NOT:

a) involve information and/or materials requiring protection against unauthorised disclosure (EUCI);

b) only a swiss partner (CYSEC) is involved from non-EU countries;
c) have the potential for misuse of its results (it will not have activities involving or generating materials, methods, technologies or knowledge that could be misused for malevolent purposes);
d) involve information and/or materials subject to national security restrictions.

There will not be other security issues related to CROSSCON that need to be taken into consideration. For this reason, the following sections are not applicable to CROSSCON.

2. Sensitive information with security recommendation

If your project involves sensitive information requiring limited dissemination due to security reasons, fill in the 'Sensitive information with security recommendation' table below.

⚠ In principle, third parties, i.e. outside the consortium and the granting authority, should have no access to sensitive deliverables with security recommendation.
⚠ However, when it is known in advance that a specific pre-identified group of recipients/recipients with an established need-to-know exists, you should insert them in the table.
⚠ You should conduct an assessment of the recipients' need-to-know, which should be at the disposal of the granting authority, if requested.
⚠ The 'Sensitive information with security recommendation' table may be modified throughout the life of the project. Any modification can be done only with the prior formal written approval of the granting authority.
⚠ The table below should not include information that is sensitive for non-security related reasons (e.g. intellectual property or commercial secrets, etc).

Sensitive information with security recommendation			
Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access

Add as many rows as needed.

1

Page 2 (right):

Call: HORIZON-CL3-2021-CS-01 — Increased cybersecurity 2021

EU Grants: Application form (Part B Security): V1.1 – 16.06.2021

3. Classified information

3.1 – Security Aspects Letter (SAL)

If your project intends to use or produce classified information, fill in the SAL provided below, according to your project-specific security requirements. Consult the guidance Classification of information in Horizon Europe projects.

⚠ Choose one or more of the Security of Information Agreements with non-EU Countries and/or international organisations, in case beneficiaries from these countries or international organisations participate in the project.
⚠ If relevant, insert in point 6 of the SAL the beneficiaries that must obtain the Facility Security Clearance (FSC) and in point 7, the beneficiaries that must obtain a Personnel Security Clearance (PSC).
⚠ The insertion in the Grant Agreement (Annex 1- Description of Action) of the completed SAL is mandatory, without any modifications on its other parts.

SECURITY ASPECTS LETTER

This security aspects letter (SAL) is an integral part of the classified grant agreement and describes grant agreement specific security requirements. Failure to meet these requirements may constitute sufficient grounds for the grant agreement to be terminated.

The beneficiaries must comply with the minimum standards as laid down in the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 (hereinafter 'Decision 2015/444') on the security rules for protecting EU classified information, and with its implementing rules.

Without prejudice to Decision 2015/444 and its implementing rules, the beneficiaries should follow the latest version of the Horizon Europe Programme Security Instruction and carry out their responsibilities according to this document.

[If applicable:]

The beneficiaries must also comply with [...]

[If relevant, insert one or more of the following Security of Information Agreements with non-EU Countries and/or international organisations]

- The Agreement between Australia and the European Union on the security of classified information signed on 13 January 2010 as attached to the Council Decision 2010/53/CFSP of 30 November 2009, as well as its implementing arrangements.

- The Agreement between Bosnia and Herzegovina and the European Union on security procedures for the exchange of classified information, signed on 05 October 2004, as attached to the Council Decision 2004/731/EC of 26 July 2004, as well as its implementing arrangements.

- The Agreement between the Republic of Iceland and the European Union on security procedures for the exchange of classified information, signed on 12 June 2006, as attached to the Council Decision 2006/467/CFSP of 21 November 2005, as well as its implementing arrangements.

- The Agreement between the European Union and Israel on security procedures for the exchange of classified information, signed on 11 June 2009, as attached to the Council Decision 2009/558/PESC of 16 March 2009, as well as its implementing arrangements.

- The Agreement between the European Union and the Principality of Liechtenstein on security

2

…Entonces debes rellenar la Security Section en la parte-B, que consta de 3 sub-secciones…

impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

3.2 - The Security Classification Guide (SCG) (appendix of the SAL)

If your project intends to use or produce classified information, fill in accordingly the 'Security Classification Guide' tables below. There are two separate SCG tables, one for the classified background information and one for the EU classified foreground information.

⚠ All classified documents (at EU, national or international level) planned to be used by the project should be listed in the SCG for classified background information.

⚠ All EU classified deliverables planned to be produced by the project should be listed in the SCG for EU classified foreground information.

⚠ Different deliverables of the same project can have different classification levels; the same deliverable can be divided in parts, which can be classified at different level.

⚠ Entities (including from the project consortium) not listed in the SCG for both classified background and foreground information should have no access to the classified information listed.

⚠ The SCG for EU classified foreground information may be modified throughout the life of the project. Any modification of the SCG can be done only with the prior formal written approval of the granting authority.

⚠ In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG for EU classified foreground information. This entity should be listed as 'reader only'. A detailed description of this entity, their established need-to-know and a reference to Facility Security Clearance, when needed, should be included in the relevant column.

Specific instructions for the table 'Use of classified Background information':

Classification Level: mention the existing classification level of the document (EU, national or international classification)

Originator: mention the name of the entity, i.e. EU institution, EU Member State, non-EU country or international organisation, under whose authority the classified information was created and classified

Reference number of the originator's authorisation for the use: you should mention the reference number of the document issued by the originator via which the latter gives authorisation to certain entities of the consortium to use the classified document to be listed in the SCG table. The authorisation letter should be at the disposal of the granting authority, if requested.

Specific instructions for completing the SCG table 'Production of EU classified Foreground information':

Classification Level: indicate the classification level proposed by you. In the framework of EU projects, information can be classified as RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (grant agreements must not involve information classified TRES SECRET UE/EU TOP SECRET). During grant preparation, update the table with the classification levels fixed in the Security Scrutiny Report.

Responsibility: indicate the role of the entity in relation to the deliverable, e.g. 'Security Manager/Main Contributor', 'Contributor', 'Blind contributor' 'Reader only'. When an entity (beneficiary or third party) is listed as blind contributor, it must have no access to the deliverable.

Comments on the need-to-know, purpose of the access and planned use for 'Reader only' role: provide a brief summary of the purpose of the access to the classified deliverable and the planned use. In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG. This entity should be listed as 'Reader only'. A detailed description of this entity, its established need-to-know and a reference to Facility Security Clearance, when needed, should be included in this column. The assessment of the entity's need-to-know, should be made available to the granting authority, if requested.

…Entonces debes rellenar la Security Section en la parte-B, que consta de 3 sub-secciones…

Security Classification Guide (SCG)

Use of classified background information

Reference and name of document	Classification level	Originator (EU institution, EU Member State, non-EU country or IO under whose authority the information was created and classified)	Reference number of originator authorisation for use

Add as many rows as needed.

Security Classification Guide (SCG)

Production of EU classified foreground information

Number and name of deliverable	Classification level (R-UE/EU-R, C-UE/EU-C, S-UE/EU-S)	Beneficiaries involved in production / entities authorised for access			
		Name	Responsibility (security manager/main contributor, contributor, blind contributor, reader only)	Date of production	Comments (need-to-know, purpose of access and planned use for 'Reader only' role)

Add as many rows as needed.

4. Security Staff

5. Project Security Officer (PSO)

If your project involves background and/or foreground classified information you should complete the below table. You should also attach a concise CV with the Project Security Officer's relevant security management experience. One PSO appointed per project is sufficient. The PSO should have the appropriate security clearance.

The role of the PSO is to guarantee that the rules on the handling of EU classified information and applicable security procedures are respected.

Project Security Officer

Name	Nationality	Profession

6. Security Advisory Board (SAB)

If your project involves background and/or foreground classified information you should complete the below table. The SAB should be composed of an uneven number of members (minimum three) consisting of end-user representatives/external reviewer(s) with a good knowledge of the security issues raised by the specific project research field. You should also attach concise CVs describing the SAB members' relevant experience on the security issues in combination with your project's research area. The SAB members should have the appropriate security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc and other timely measures for preventing the misuse of such information.

Security Advisory Board

Member's name	Nationality	Profession	Areas of competence

Add as many rows as needed.

7. Other project-specific security measures

No additional project-specific security measures

7

8

@HorizonteEuropa
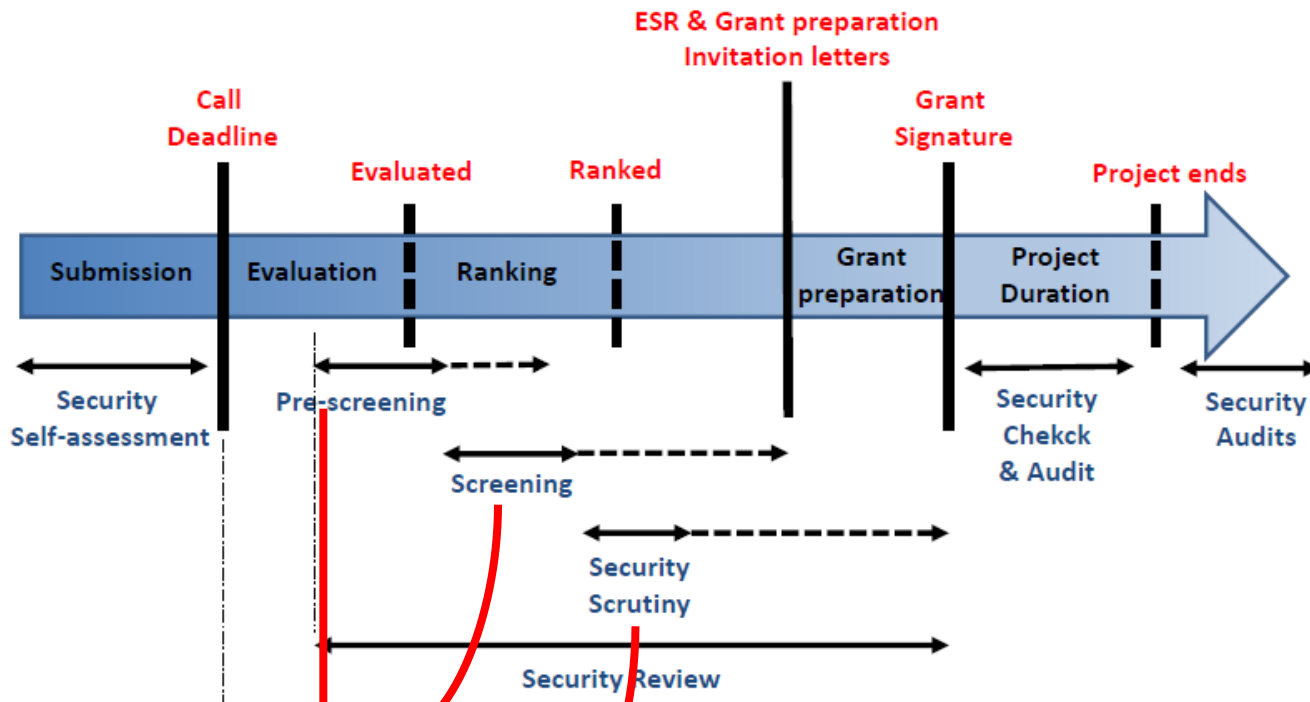
✓ **Security Pre-screening:** during the scientific evaluation or soon after- by **granting authority staff**. For proposals submitted under **non- security sensitive topics** when: the **applicant has replied positively** to the Security issues table or the applicant has replied negatively, but the **granting authority has detected security issues**.

✓ **Security Screening:** after the scientific evaluation and before the signature of the GA - by **EC staff** (DG HOME). **Automatically** performed to all proposals that have gone through the Security Pre-screening. DG HOME will assess the pre-screening results and decide on the possible launch of the Security Scrutiny.

1. **Security Scrutiny:** After the scientific evaluation and before the signature of the GA - by **national security experts (Security Scrutiny Group).** → Only **proposals above threshold and considered for funding**, which can lead to **security requirements** that become contractual obligations. **IS NOT A RE-EVALUATION OF THE PROPOSAL AT ALL!.**

Last considerations regarding the Security Scrutiny…

1. The **Security Scrutiny** will be **carried out in the following cases**:

   ✓ **Automatically,** when a proposal has been submitted under a **security sensitive topic (Cluster-3 & Space calls from Cluster-4)**;

   ✓ In other cases, when the **Security Screening has concluded that the proposal is very likely to raise security issues** for which mitigation measures should be adopted.

2. The **Security Scrutiny will focus ONLY** on the potential **sensitive information (from the security point of view)** related with your project:

   ✓ This type of information requires **limited dissemination** due to **security reasons**.

   ✓ Issues concerning **IPR and commercial secrets fall out of the scope** of this category.

   ✓ Such information will be marked **as 'SEN' and an additional column will indicate the security type**. → REMEMBER: In H2020 it was marked as Confidential (CO).

3. The **Security Scrutiny** is performed by the the HE Security Security Scrutiny Group of 58 experts from EU Member State (experts usually working for the National Security Authority or a ministry, e.g. Home Affairs, Security and Justice). → They follow the "**Guidance on Classification of information in Horizon Europe projects**"

The best orientation is to use the "Guidance on Classification of information in Horizon Europe projects"

![European Commission logo]

Horizon Europe

Classification of information in Horizon Europe projects

Version 3.0
22 July 2021

Table of contents

Let's see the example later on!

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/classification-of-information-in-he-projects_he_en.pdf

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN — CDTI
@CDTIoficial

What is considered EU Classified Information (EUCI)?

Classified information (Art. 13.2 MGA and Annex 5) is information requiring protection against unauthorised disclosure.

➢ A project might **use** classified background information **or produce** classified foreground information.

➢ **Classified background information → I**s information **already classified by the EU entities, nation states or international organisations,** which is used in the frame of a project.

➢ **Classified foreground information →** Is information **produced by a project**, which needs to be designated by an EU classification (EUCI).

    ➢ **EUCI definition in Commission Decision 444/2015**: *"European Union classified information (EUCI) means 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 its Member States".*

        ❖ *Example: some of the information produced by a project could potentially be used to plan terrorist attacks or avoid detection of criminal activities.*

Sort of information that can be "Security Sentitive" in your proposal…

It can refers both to the "**subject of research**" as well the "**type of research**" in your project…

Potential sensitive **subject of research:**	Potential sensitive **type of research results (or input information/documents for your project):**
❑ explosives & CBRN ❑ **infrastructure & utilities** ❑ border security ❑ intelligent surveillance ❑ terrorism & organised crime ❑ digital security ❑ space	❑ threat assessments ❑ vulnerability assessments ❑ specifications ❑ capability assessments ❑ incidents/scenarios based on real-life security incidents and potential threat scenarios

… as a consequence, some of the **deliverables**, **activities** or the whole proposal can be secure sensitive classified! ➔ **In Framework Programme projects the common situation in projects is that only deliverables may be classified.**

Results coming out from the Security Scrutiny of your proposal

- **No security concern -** No security issues were identified in the proposal → No security section in the GA.

- **Security recommendations** - The Security Scrutiny Summary Report (SecScrSR) will list one or more **security requirements** that will be <u>set out in the Security Section of Annex 1 of the GA</u>:

  – security recommendation to **limit the dissemination of sensitive deliverables for security reasons** to the consortium, granting authority staff and potentially to a specific pre-identified group of stakeholders with an established need-to-know;

  – **classification of certain deliverables at a certain level (EUCI);**

  – appointment of a **Project Security Officer (PSO)** in case of classification;

  – establishment of a **Security Advisory Board (SAB)**;

  – **other** security recommendations (e.g. ensuring that personnel has followed trainings on security, adjusting the scope of a certain work package, etc.).

- ✕ **Proposal too sensitive to be funded** - information to be used or generated by the project is too sensitive, or applicants lack the right experience, skills or authorisations to handle classified information at the appropriate level. → Funding is refused and the proposal is rejected.

Levels of classification of Security Sensitive Information, EUCI classification

There are **four levels of EU classification of your activities/deliverables**:

- ✓ **TRÈS SECRET UE/EU TOP-SECRET (TS-UE/EU-TS)** → **ATTENTION:** projects involving information classified TRÈS SECRET UE/EU TOP-SECRET (TS-UE/EU-TS) **cannot be funded under Horizon Europe (as in H2020)**.

- ✓ **SECRET UE/EU SECRET (S-UE/EU-S)**: for information and material the unauthorised disclosure of which **could seriously harm** the essential interests of the European Union or of one or more of the Member States.

  - ✓ *Example: threatening of life or the serious prejudicing of public order or individual security and liberty.*

- ✓ **CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C)**: for information and material the unauthorised disclosure of which **could harm** the essential interests of the European Union or of one or more of the Member States.

  - ✓ *Example: inception of damage to the operational effectiveness or security of a Member State or other State's forces or to the effectiveness of valuable security or intelligence operations.*

- ✓ **RESTREINT UE/EU RESTRICTED (R-UE/EU-R)**: for information and material the unauthorised disclosure of which **could be disadvantageous** to the interests of the European Union or of one or more of the Member States.

  - ✓ *Example: information which could potentially make it more difficult to maintain the operational effectiveness or security of Member States or other State's forces.*

4.3 Critical infrastructure and utilities research

What?

'Critical infrastructures and utilities' are assets and systems (e.g. 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)[4].

How to deal with threat assessments?

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

How to deal with vulnerability assessments?

Detailed gap analyses intrinsic to specific infrastructure and assessments of current security systems, technologies and processes and other extant security solutions should be classified RESTREINT UE/EU RESTRICTED. If they add value (e.g. by including criticality analyses, highly detailed case studies, vulnerability modelling of supply systems or vulnerability assessment methodologies) they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

Given the specific threat of terrorist attacks on aviation infrastructure, vulnerability analyses of both passenger and cargo security solutions and processes should also be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with specifications?

The design, specifications and operation of software tools and platforms to prevent and detect attacks on infrastructure and the design, specifications and operation of architectural security solutions for utilities should be classified RESTREINT UE/EU RESTRICTED.

Detailed detection techniques for early-warning and event analysis (such as those for use in public transport and urban environments) and the definition of the data sources to be used should be classified RESTREINT UE/EU RESTRICTED.

Information on sensor networks (such as those used to identify potential incidents in energy grids, ICT systems or water supply systems) should be classified RESTREINT UE/EU RESTRICTED. Automated analysis of sensor data, the algorithms used and detailed information on other qualitative and quantitative tools to detect security threats should be classified RESTREINT UE/EU RESTRICTED.

Detailed specifications of organisational and operational processes regarding distribution networks and supply chains (such as postal systems) should be classified RESTREINT UE/EU RESTRICTED.

Again, given the higher threat level, the design, specifications and operation of beyond the state-of-the-art screening and detection systems for aviation purposes should be classified CONFIDENTIEL UE/EU CONFIDENTIAL, as should detailed information on airport checkpoint design and procedures. Detailed information on air cargo supply chains should be classified RESTREINT UE/EU RESTRICTED, like other supply chains.

How to deal with capability assessments?

Reports on the performance of systems installed in infrastructure (such as power plants or water treatment plants) should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

The performance of completed detection and security systems in simulated environments (such as demonstrations of early-warning systems or physical security solutions for buildings) should be classified RESTREINT UE/EU RESTRICTED.

The capabilities of aviation detection equipment and processes in simulated environments should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with incidents/scenarios assessments?

Detailed information on scenarios and incidents involving attacks on critical infrastructure should be classified RESTREINT UE/EU RESTRICTED. If it adds value (e.g. by including in-depth quantitative analyses of the potential or actual consequences (human, functional or financial) of such actions), it should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

Example of the "HE guidelines" regarding a project focus on "Critical Infrastructures"

ENERGY   HEALTH   TRANSPORT   FINANCIAL   ICT

WATER   FOOD   PUBLIC & LEGAL ORDER AND SAFTY   CHEMICAL & NUCLEAR INDUSTRY   SPACE AND RESEARCH

HORIZONTE EUROPA @HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN   CDTI @CDTIoficial

Qué sucede con los NON-EU countries?
Third Countries & Associated Countries

- ❑ EU classification is **limited to EU Member States (EUCI deliverables)**.

- ❑ Projects involving classified information can, in principle, include participants from non- EU countries**... HOWEVER, ONLY beneficiaries from countries with a valid Security of Information Agreement with the EU can access and handle classified information used/produced by the project (EUCI deliverables).** → As a consequence:

   ✓ **There is NO restriction for non-EU countries without Security Agreement** to the participate to projects involving classified information**, AS FAR AS THEY DON'T HAVE ACCESS TO EUCI information.** → **No pueden tener acceso a deliverables/tareas/background information EUCI.**

   ✓ The non-EU countries possessing a Security Agreement with the EU are to be found in the **Council document 15035/19 (https://data.consilium.europa.eu/doc/document/ST-15035-2019-INIT/en/pdf) → MOST AGREEMENTS ARE STILL UNDER NEGOTIATION!**

ATENCIÓN… dos ejemplos de EXCLUSIÓN

1.- BIEN DE TODA LA PROPUESTA, es decir, ese partner NO puede formar parte del consorcio… → Mirar si el topic incluye alguna indicación en al tabla inicial sobre si hay algún tipo de EXCLUSIÓN a NIVEL DE CONSORCIO de partners por su nacionalidad…

Por ejemplo: <u>Si el topic indica que SÓLO</u> pueden participar "entities stablished in MMSS or Associated Countries", entonces, p.e.,
Suiza NO podría participar en el consorcio PORQUE NO
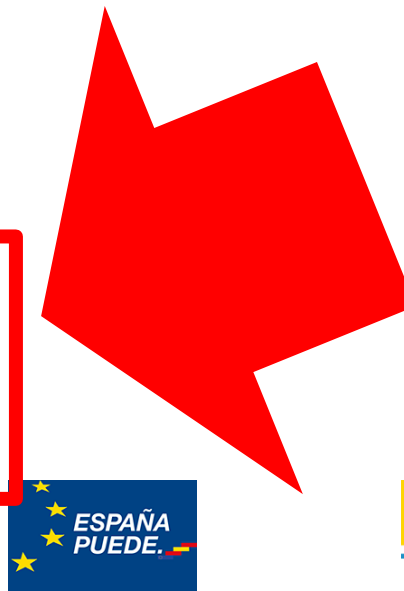**ES UN ASSOCIATED COUNTRY.**

2.- BIEN SÓLO DE LOS DELIVERABLES EUCI, pero pueden formar parte del consorcio! → **Asegurarse que los países incluídos en el consorcio tienen un acuerdo de intercambio de info clasificada en caso que tengan que acceder a algún deliverable o datos EUCI →** ATENCIÓN, UK sí tiene firmado el acuerdo de intercambio de EUCI con la UE…

HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services

En el caso de la call-2023...

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 5.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 government authorities responsible for resilience on national level and / or for overseeing operators, from at least 3 different EU Member States. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, or security, namely to protect and to preserve the confidentiality of risk assessments and of the vulnerabilities of critical entities of Member States, participation is limited to legal entities established in Member States only. Proposals including entities established in countries other than EU Member States will be ineligible.
Technology Readiness Level	Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B.

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI
@CDTIoficial

The EU-UK Security of Information Agreement

The exchange of classified information between partners remains an important tool of cooperation in addressing common security threats.

If a joint security threat makes it necessary, certain EU classified information can be shared with third countries, but only on a case-by-case basis and provided that a dedicated Security of Information Agreement (SIA) has been concluded between the EU and a third country.

Against this background, the EU and the UK have concluded a Security of Information Agreement. The Agreement will allow the EU and the UK to exchange classified information, applying strong guarantees as to the handling and protection of the exchanged information.

The EU-UK Security of Information Agreement was signed on 30 December 2020, was applied provisionally as of 1 January 2021 and entered into force on 1 May 2021

30 APRIL 2021
The EU-UK Security of Information Agreement (all languages)
English (269.06 KB - HTML)

Download ⬇

HORIZONTE
EUROPA
@HorizonteEuropa

División de
Programas de la UE

ESPAÑA
PUEDE.

MINISTERIO
DE CIENCIA
E INNOVACIÓN

CDTI
@CDTIoficial

25

Y cuando estáis escribiendo vuestra propuesta...

EU Grants

How to handle security-sensitive projects

Projects with sensitive and classified information

Version 1.0
01 July 2021

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf

HORIZONTE
EUROPA
@HorizonteEuropa

División de
Programas de la UE

Part-B

Se debe continuar rellenando la tabla de deliverables…

Table 3.1c: List of Deliverables³

Only include deliverables that you consider essential for effective project monitoring.

Deliverable (number)	Deliverable name	Work package number	Short name of lead participant	Type	Dissemination level	Delivery date (in months)

KEY

Deliverable numbers in order of delivery dates. Please use the numbering convention <WP number>.<number of deliverable within that WP>.
For example, deliverable 4.2 would be the second deliverable from work package 4.

Type:
Use one of the following codes:
- R: Document, report (excluding the periodic and final reports)
- DEM: Demonstrator, pilot, prototype, plan designs
- DEC: Websites, patents filing, press & media actions, videos, etc.
- DATA: Data sets, microdata, etc.
- DMP: Data management plan
- ETHICS: Deliverables related to ethics issues.
- SECURITY: Deliverables related to security issues
- OTHER: Software, technical diagram, algorithms, models, etc.

Dissemination level:
Use one of the following codes:
- PU – Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)
- SEN – Sensitive, limited under the conditions of the Grant Agreement
- Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444
- Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444
- Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444

Delivery date
Measured in months from the project start date (month 1)

In the template Sensitive Information will be marked **as 'SEN' and an additional column will indicate the security type (R/C/S)**. → In H2020 it was marked as Confidential (CO).

³ You must include a data management plan (DMP) and a 'plan for dissemination and exploitation including communication activities as distinct deliverables within the first 6 months of the project. The DMP will evolve during the lifetime of the project in order to present the status of the project's reflections on data management. A template for such a plan is available in the Online Manual on the Funding & Tenders Portal.

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN   CDTI   @CDTIoficial

Se debe continuar rellenando la tabla de deliverables...

3.2.3 List of Deliverables
Table 4.1c

Deliverable (number)	Deliverable name	Work package number	Short name of lead participant	Type	Dissemination level	Delivery date (in months)
D1.1	Project and data management plan and activities	WP1		R	SEN	M6
D2.1	Methodology for prevention practice review and establishment engagement model for relevant networks and Knowledge Transfer Workshops'	WP2		R	SEN	M6
D2.2	Gap analysis and evaluative report	WP2		R	SEN	M20
D2.3	Synthesised best practice model for prevention – increasing MAP and IAR engagement.	WP2		R	SEN	M36
D3.1	Establishing a working relationship with European and international stakeholder groups and development the reports on the key findings from stakeholder group discussions based	WP3		R	SEN	M12
D3.2	Two policy briefs and submission of publications	WP3		R	PU	M30
D3.3	Peer-education website and website's key performance indicators	WP3		R + DEC	PU	M36
D4.1	Report on targeted recruitment and deterrence actions	WP4		R	SEN	M18
D4.2	online tools	WP4		R + DEM	PU	M30
D4.3	Recruitment & Platform Evaluation	WP4		R	SEN	M36
D5.1	Training curriculum and risk assessment protocol	WP5		R	SEN	M34
D5.2	Training curriculum and training courses for LEAs	WP5		R	SEN	M33

In the template Sensitive Information will be marked **as 'SEN'** and **an additional column will indicate the security type (R/C/S)**. → In H2020 it was marked as Confidential (CO).

Contenidos de la "Security Section" en la part-B

2. Grant preparation stage: Part B — Security section, Security Aspects Letter (SAL) and Security Classification Guide (SCG)

2.1 Classified information — SAL and SCG

If the project involves EUCI, you will be requested during grant preparation to add the Security Aspects Letter (SAL) and Security Classification Guide (SCG) to Annex 1 of your Grant Agreement.

The SAL lists the project-specific security requirements linked to the EUCI *(e.g. classification levels, access by consortium-members which are international organisations or entities from non-EU countries, etc)*. The SCG describes the classified elements of a grant agreement (deliverables) and their security classification levels (— two separate tables, one for the classified background information and one for the EU classified foreground information).

You must adapt your SAL and SCG to the outcome of the security scrutiny procedure (SecSR).

List all entities that need to know in the SCG (both for classified background and foreground information). Entities not listed there will NOT have access to the classified information listed in the table, even if they are from the project consortium.

⚠️ If you will use classified background, don't forget that you must obtain advance formal written authorisation by the originator *(i.e. the entity under whose authority the information was created and classified)*.

2.2 Other security recommendations

In addition to the SAL and SCG, you will be requested to complete the information regarding other security recommendations *(e.g. sensitive information with security recommendation, security staff, access to IT systems, etc)*.

If your project involves classified background or foreground information, you must appoint a project security officer (PSO). One PSO per project is sufficient. The PSO must have appropriate security clearance.

A security advisory board is needed if your project involves sensitive deliverables with security recommendation or classified background or foreground information.

Summary of the project security issues section

Describe the security issues you identified in your project. Focus on the security subject matters and explain the potential misuse of the research results. Relate to the security-sensitive type of activities as explained in the guidance *(see How to handle security-sensitive projects)*.

1. Sensitive information with security recommendation

If your project involves sensitive information requiring limited dissemination due to security reasons, fill in the 'Sensitive information with security recommendation' table below.

⚠ In principle, third parties, i.e. outside the consortium and the granting authority, should have no access to sensitive deliverables with security recommendation.

⚠ However, when it is known in advance that a specific pre-identified group of recipients/recipients with an established need-to-know exists, you should insert them in the table.

⚠ You should conduct an assessment of the recipients' need-to-know, which should be at the disposal of the granting authority, if requested.

⚠ The 'Sensitive information with security recommendation' table may be modified throughout the life of the project. Any **modification can be done only with the prior formal written approval of the granting authority.**

⚠ The table below should not include information that is sensitive for non-security related reasons (e.g. intellectual property or commercial secrets, etc).

Sensitive information with security recommendation			
Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access

Se puede hacer un resumen explicativo al inicio y se debe incluir la **tabla de "Sensitive Information with Security Recomendations"**

EXAMPLE

PART B SECURITY

1. Summary of the project security issues

As the ▮ project may involve some activities or results which may raise security issues (especially in WP5), one of the key objectives of the Consortium will be to safeguard the material gathered by the partners throughout the research process and protect the outputs generated. It is of the utmost importance that a robust system is in place to ensure the work of the project and its generated outcomes are fully protected. The Consortium has put in place a tried and tested management and security advisory system to protect the outputs of the project.

2. Sensitive information with security recommendation

The consortium acknowledges that certain information managed in the course of the project may be security sensitive and restricted appropriately.

▮ do not foresee to produce any EU-classified information, however the consortium will analyse all information through the life of the project, if any EU-classified information is included. This task will be coordinated by the Project Security Officer (PSO) and reported at Project Board meetings. Where a deliverable needs to be reclassified, it shall be undertaken with the approval of the European Commission.

There are no ▮ deliverables which are classified, however there are 14 deliverables which will be only accessible by the consortium and will be treated with the utmost respect for their potential vulnerability and to ensure maximum measures are taken to preserve ▮ will be flexible in altering the dissemination level of any deliverable to classified, to ensure that the contents are protected.

Any classified deliverables will be treated as containing sensitive information and any data collection associated with them, even at the initial research stage will be required to use PGP encryption standards under AES 256 rounds encryption standards. This encryption standard will protect the file types from being intercepted or read in case of accidental or malicious sending errors. Every effort will be made to delete and remove sensitive information once they have served their project purpose.

List of consortium only deliverables, with sensitive status, NOT with restricted status.

Sensitive information with security recommendation			
Number and name of the deliverable	Name of lead participant	Date of production	Name of entity authorised for access
D1.1 Project management plan and activities	▭	M6	Consortium and EC
D2.1 Methodology for prevention practice review and establishment engagement model for relevant networks and Knowledge Transfer Workshops'	▭	M6	Consortium and EC
D2.2 Gap analysis and evaluative report	▭	M20	Consortium and EC
D2.3 Synthesised best practice model for prevention – increasing MAP and IAR engagement.	▭	M36	Consortium and EC
D3.1 Establishing a working relationship with European and international stakeholder groups and development the reports on the key findings from stakeholder group discussions based	▭	M12	Consortium and EC
D4.1 Report on targeted recruitment and deterrence actions	▭	M18	Consortium and EC
D4.3 Recruitment & Platform Evaluation	▭	M36	Consortium and EC
D5.1 Training curriculum and risk assessment tool	▭	M34	Consortium and EC
D5.2 Training curriculum and training courses for LEAs	▭	M33	Consortium and EC
D6.1 Communication and Dissemination Plan & Strategy and activities	▭	M6	Consortium and EC

HORIZONTE EUROPA @HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI @CDTIoficial

Contenidos de la "Security Section"

2. Classified information

2.1 – Security Aspects Letter (SAL)

If your project intends to use or produce classified information, fill in the SAL provided below, according to your project-specific security requirements. Consult the guidance Classification of information in Horizon Europe projects.

⚠ Choose one or more of the Security of Information Agreements with non-EU Countries and/or international organisations, in case beneficiaries from these countries or international organisations participate in the project.

⚠ If relevant, insert in point 6 of the SAL the beneficiaries that must obtain the Facility Security Clearance (FSC) and in point 7, the beneficiaries that must obtain a Personnel Security Clearance (PSC).

⚠ The insertion in the Grant Agreement (Annex 1- Description of Action) of the completed SAL is mandatory, without any modifications on its other parts.

2.2 - The Security Classification Guide (SCG) (appendix of the SAL)

If your project intends to use or produce classified information, fill in accordingly the 'Security Classification Guide' tables below. There are two separate SCG tables, one for the classified background information and one for the EU classified foreground information.

⚠ All classified documents (at EU, national or international level) planned to be used by the project should be listed in the SCG for classified background information.

⚠ All EU classified deliverables planned to be produced by the project should be listed in the SCG for EU classified foreground information.

⚠ Different deliverables of the same project can have different classification levels; the same deliverable can be divided in parts, which can be classified at different level.

⚠ Entities (including from the project consortium) not listed in the SCG for both classified background and foreground information should have no access to the classified information listed.

⚠ The SCG for EU classified foreground information may be modified throughout the life of the project. Any modification of the SCG can be done only with the prior formal written approval of the granting authority.

⚠ In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG for EU classified foreground information. This entity should be listed as 'reader only'. A detailed description of this entity, their established need-to-know and a reference to Facility Security Clearance, when needed, should be included in the relevant column.

Pueden sufrir modificaciones después del escrutinio de Seguridad debido a indicaciones concretas del SG!
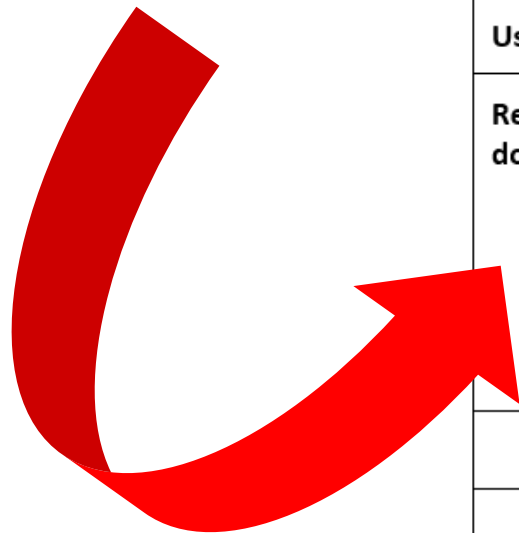
Specific instructions for the table **'Use of classified Background information'**:

Classification Level: mention the existing classification level of the document (EU, national or international classification)

Originator: mention the name of the entity, _i.e._ EU institution, EU Member State, non-EU country or international organisation, under whose authority the classified information was created and classified

Reference number of the originator's authorisation for the use: you should mention the reference number of the document issued by the originator via which the latter gives authorisation to certain entities of the consortium to use the classified document to be listed in the SCG table. The authorisation letter should be at the disposal of the granting authority, if requested.

Security Classification Guide (SCG)			
Use of classified <u>background</u> information			
Reference and name of document	**Classification level**	**Originator** (EU institution, EU Member State, non-EU country or IO under whose authority the information was created and classified)	**Reference number of originator authorisation for use**

Specific instructions for completing the SCG table '**Production of EU classified Foreground information**':

Classification Level: indicate the classification level proposed by you. In the framework of EU projects, information can be classified as RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (grant agreements must not involve information classified TRES SECRET UE/EU TOP SECRET). During grant preparation, update the table with the classification levels fixed in the Security Scrutiny Report.

Responsibility: indicate the role of the entity in relation to the deliverable, e.g. 'Security Manager/Main Contributor', 'Contributor', 'Blind contributor' 'Reader only'. When an entity (beneficiary or third party) is listed as blind contributor, it must have no access to the deliverable.

Comments on the need-to-know, purpose of the access and planned use for 'Reader only' role: provide a brief summary of the purpose of the access to the classified deliverable and the planned use. In case an entity (beneficiary or third party) with an established need-to-know exists, it can be included in advance in the SCG. This entity should be listed as 'Reader only'. A detailed description of this entity, its established need-to-know and a reference to Facility Security Clearance, when needed, should be included in this column. The assessment of the entity's need-to-know, should be made available to the granting authority, if requested.

Security Classification Guide (SCG)

Production of EU classified foreground information

Number and name of deliverable	Classification level (R-UE/EU-R, C-UE/EU-C, S-UE/EU-S)	Beneficiaries involved in production / entities authorised for access			
		Name	Responsibility (security manager/main contributor, contributor, blind contributor, reader only)	Date of production	Comments (need-to-know, purpose of access and planned use for 'Reader only' role)

Security Classification Guide (SCG)

Production of EU classified foreground information

Number and name of deliverable	Classification level (R-UE/EU-R, C-UE/EU-C, S-UE/EU-S)	Beneficiaries involved in production / entities authorised for access			
		Name	**Responsibility** (security manager/main contributor, contributor, blind contributor, reader only)	**Date of production**	**Comments** (need-to-know, purpose of access and planned use for 'Reader only' role)
D6.2 Final version of pilot implementation and evaluation, end user training and innovative curricula	R-UE/EU-R	Participant 1	Main Contributor	M36	WP lead; Deliverable lead;
		Participant 2	Contributor		Technical Input
		Participant 3	Contributor		Task Leader & Contributor
		Participant 4	Contributor		Technical Input
		Participant 5	Contributor		Technical Input
		Participant 6	Contributor		Operational input
		Participant 7	Contributor		Technical Input
		Participant 8	Contributor		Expert's Input on X-ray scanning
		Participant 9	Contributor		Operational input
		Participant 10	Contributor		Operational input; protection of identified gaps in current LEA operational delivery.
		Participant 11	Contributor		Operational input;

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI

@CDTIoficial

3. Security Staff

3.1 - Project Security Officer (PSO)

If your project involves background and/or foreground classified information you should complete the below table. You should also attach a concise CV with the Project Security Officer's relevant security management experience. One PSO appointed per project is sufficient. The PSO should have the appropriate security clearance.

The role of the PSO is to guarantee that the rules on the handling of EU classified information and applicable security procedures are respected.

Project Security Officer		
Name	Nationality	Profession

3.2 - Security Advisory Board (SAB)

If your project involves background and/or foreground classified information you should complete the below table. The SAB should be composed of an uneven number of members (minimum three) consisting of end-user representatives/external reviewer(s) with a good knowledge of the security issues raised by the specific project research field. You should also attach concise CVs describing the SAB members' relevant experience on the security issues in combination with your project's research area. The SAB members should have the appropriate security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc and other timely measures for preventing the misuse of such information.

Security Advisory Board			
Member's name	Nationality	Profession	Areas of competence

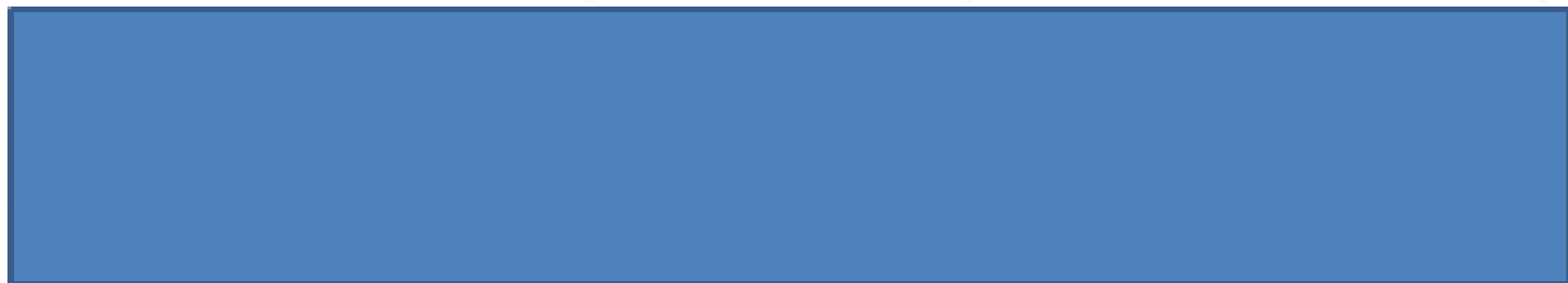# Ejemplo de Contenidos de la "Security Section"

4 SECURITY STAFF

4.1 Project Security Officer (PSO)

Given the nature of the topic addressed by ▓▓▓▓ the Consortium has planned to nominate a Project Security Officer (PSO) to assess the security sensitivity of some of the project results and guarantee that the rules on the handling of EU classified information and applicable security procedures are respected, in case some ▓▓▓▓ will be used or produced by the project.

The following table provides information about the ▓▓▓▓ PSO.

Project Security Officer		
Name	**Nationality**	**Profession**
▓▓▓▓	▓▓▓▓	Director of the Defence, Space and Homeland Security ▓▓▓▓
CV: ▓▓▓▓ (male) is the Defense, Space and Homeland Security Business Unit Technical Director in Engi- ▓▓▓▓		

Ejemplo de Contenidos de la "Security Section"

4.2 Security Advisory Board (SAB)

Given the nature of the topic addressed by ▮▮▮▮ the Consortium has planned to establish a Security Advisory Board (SAB) to assess the security sensitivity of some of the project results.

The ▮▮▮▮ Consortium includes several partners that can bring the necessary expertise and experience to provide the resources needed to conform the SAB. The SAB will be an integral part of the project's management structure.

The proposed initial members of the SAB are listed in the table below. All members have sufficient experience / knowledge of security issues related to the project activities. The responsibility of the SAB is to assess the emergence of sensitive information handled by participants and, in case, propose – if appropriate – corresponding measures for preventing misuse of such an information.

Security Advisory Board			
Member's name	Nationality	Profession	Areas of competence
▮▮▮▮	▮▮▮▮	Information Security Senior Research Scientist ▮▮▮▮	Dr. ▮▮▮▮ received his ▮▮▮▮

5. 3.2 - Security Advisory Board (SAB)

If your project involves background and/or foreground classified information you should complete the below table. The SAB should be composed of an uneven number of members (minimum three) consisting of end-user representatives/external reviewer(s) with a good knowledge of the security issues raised by the specific project research field. You should also attach concise CVs describing the SAB members' relevant experience on the security issues in combination with your project's research area. The SAB members should have the appropriate security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc and other timely measures for preventing the misuse of such information.

Security Advisory Board			
Member's name	**Nationality**	**Profession**	**Areas of competence**
	Spain	Compliance officer	Senior Policy Advisor Knowledge Safety and Export Control
	France	Manager capacity development	Project management, capacity building, data security
	Netherlands	Lawyer	Contracts, IPR, data security.

4. Other project-specific security measures

Describe, if relevant, the project security management and other measures intended to safeguard security during the project's life, such as:

- Project staff with a Personnel Security Clearance (PSC) from one organisation without a Facility Security Clearance (FSC) working in the premises of an organisation holding a FSC;
- Specific measures for access to IT systems;
- Other types of measures (technical, operational, etc.)..

6.4 OTHER PROJECT-SPECIFIC SECURITY MEASURES

In order to be compliant with GDPR art.32 – Security of processing personal data, and with legal obligations with regards the protection of the rights and fundamental freedoms of people, ▮▮▮▮▮▮ will use state-of-the-art technologies for secure storage, delivery and access of personal information, as well as managing the rights of the users. In this way, there is complete guarantee that data will be accessed, delivered, stored and transmitted by the right person, with well-defined rights, at the right time. Specific access policy will be defined for this purpose and will be supported by State-of-the-art firewalls, network security, encryption and authentication will be used to protect collected data. Firewalls prevent the connection to open network ports, and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible (depending on the facilities of each partner) the data will be stored in a locked server, and all identification data will be stored separately.

Intrusion Detection systems will monitor anomalies in network traffic and activate restraint policy if needed. A metadata framework will be used to identify the data types, owners and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms. A Data Management Plan will be released at the early stage of the project (M6) in order to provide consortium with guidelines for applying the suitable security measures for data management throughout the project duration.

EXAMPLE

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI
@CDTIoficial

In particular, but not exclusively, the following security requirements must be complied with:

1. The grant beneficiaries must comply with additional instructions provided by their respective national security authorities (NSAs). […]

2. A list of all the elements to be classified during the performance of this GA as well as the specific applicable security classification levels are contained in the security classification guide (SCG). […]

3. Classified information generated when performing the grant agreement must be marked as EU classified information (EUCI) at security classification level as determined in the SCG. **Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the granting authority.**

4. **The rights pertaining to the originator of any EUCI created during the performance of the classified grant agreement are exercised by the Commission.**

5. Without the written consent of the granting authority, **the beneficiary or subcontractor must not make use of any information or material** furnished by the granting authority or produced on behalf of that authority **for any purpose other than that of the grant agreement.**

6. A **Facility Security Clearance (FSC)** is required for the beneficiaries involved in the classified part of the project at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET UE/EU SECRET.

Where an FSC is required for the performance of a grant agreement, the beneficiary must ask the granting authority to proceed with the FSC request.
For the performance of this grant agreement, at least the below beneficiaries must obtain the FSC:
- Name of the beneficiary/Abbreviation/Country
- Name of the beneficiary/Abbreviation/Country
- Name of the beneficiary/Abbreviation/Country

7. A **Personnel Security Clearance (PSC)** is required for the beneficiaries' personnel involved in the classified part of the project at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET UE/EU SECRET.

Where a PSC is required for the beneficiary's personnel, **the beneficiary must directly request its NSA or DSA to initiate the procedure to this effect. The beneficiaries concerned shall maintain records of their employees taking part in the project and who have been cleared for access to EUCI.**
For the performance of this grant agreement, the below beneficiaries must obtain the PSC:
- Name of the beneficiary/Abbreviation/Country
- Name of the beneficiary/Abbreviation/Country
- Name of the beneficiary/Abbreviation/Country

8. The beneficiary or subcontractor must have **business contingency plans (BCPs) to protect any EUCI handled in the performance of the classified grant agreement in emergency situations and must put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI.** The beneficiary or subcontractor must inform the granting authority of its BCP.

Tienen que estar actualizadas en el momento de comienzo del WPs correspondiente.

@CDTIoficial

Para finalizar la parte pre-award...

When the participant receives the <u>ESR</u> and the <u>information letter</u>, if the project rises **EUCI Information**, that is, **EU-RESTRICTED and above**, **you should contact your NSA** in order to get detailed information of your national security instructions to be fullfiled…
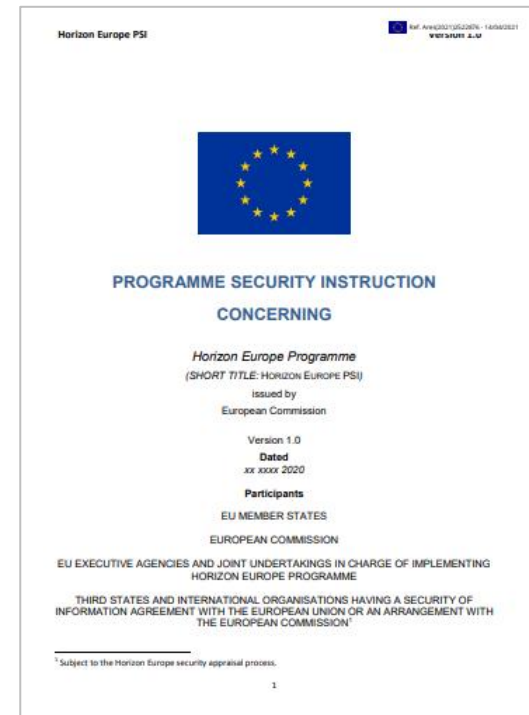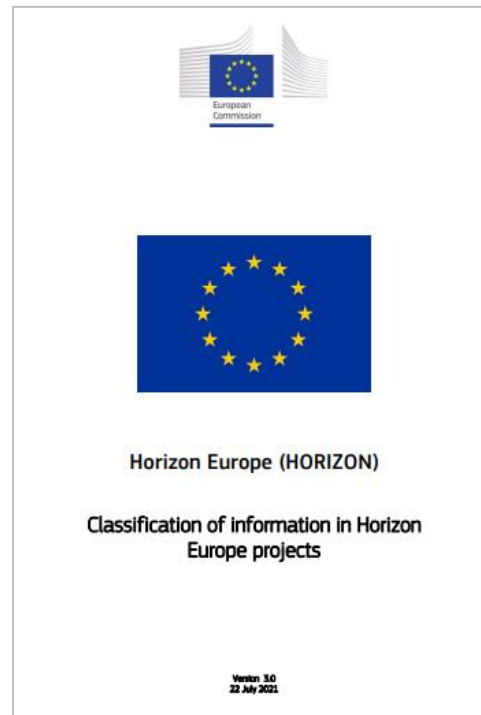
Reference documents

✓ **Regulation establishing Horizon Europe**: Security (Art. 20)

✓ **Model Grant Agreement**: Confidentiality and security (Art. 13 and Annex 5)

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

✓ **Commission Decision 2021/259** laying down implementing rules on industrial security with regard to classified grants.

✓ **Guidelines for Security Experts on the Security Scrutiny Procedure** (coming soon).

✓ **Guidance on the 'classification of information in Horizon Europe projects' (July 2021).**

✓ **Guidance on 'How to handle Security sensitive projects' (July 2021).**

✓ **Horizon Europe Programme Security Instruction (PSI) (Version 1.0, June 2021).**

✓ **HE Programme Guide (June 2021).**

✓ Guidance note on 'potential misuse of research'.

✓ Guidance note on 'research with an exclusive focus on civil applications'.

✓ Security section of the HE proposal template, including the template of the Security Aspects Letter (SAL) and its annex (Security Classification Guide (SCG)).

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

ESPAÑA PUEDE.

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI
@CDTIoficial

✓ **Guidance on the 'classification of information in Horizon Europe projects'** (July 2021).

✓ Guidance on **'How to handle Security sensitive projects'** (July 2021).

✓ Horizon Europe **Programme Security Instruction** (PSI) (June 2021).

Seguridad a nivel nacional...

En España…

… INFORMACIÓN CLASIFICADA

**Información Clasificada es todo material que debe ser protegido
ya que su pérdida, difusión no autorizada o modificación
puede causar un daño serio
para los intereses y/o seguridad nacional o internacional**
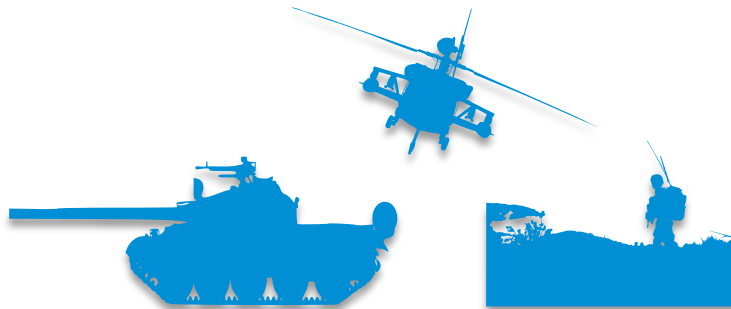
NORMAS DE SEGURIDAD
APLICABLES A UN PROGRAMA

- **UE - 444/2015 y normas complementarias**

- **Decision 2021/259 de la Comisión Europea**
  (Subvenciones)

- **Norma específica internacional de seguridad:**
  PSI o Instrucciones de seguridad del programa.

- **Y normativas nacionales → ANPIC**

INSTRUCCIONES DE SEGURIDAD DEL PROGRAMA   - PSI -

01

HSEM / HSES / HPS

Regulan en qué situaciones es necesario o no las habilitaciones de seguridad de las entidades participantes

02

TP o planes de transporte

Regulan los medios de transporte físico de la documentación y piezas componentes del programa que no son de libre circulación

03

Anexo COMSEC

Regulan la transmisión electrónica de la información entre las entidades participantes en el consorcio

04

***Releases* o cesiones**

Regulan los procedimientos de cesión a terceros estados de los items clasificados, bien con motivo de exportación bien para garantizar el suministro

05

Incidentes de seguridad

Indican los procedimientos para notificar los incidentes de seguridad en el seno del programa, generalmente reportando al grupo de seguridad del programa.

GUÍA DE CLASIFICACIÓN
SCG

Anexo a la PSI

Indica el grado de clasificación de cada elemento, item, deliverable, etc. de un determinado trabajo en un programa clasificado.

Cuanto más detallada mejor para las entidades desarrolladoras

Table 3.1c: List of Deliverables[7]

Deliverable (number)	Deliverable name	Work package number	Short name of lead participant	Type	Dissemination level	Delivery date (in months)

30 o 40 entregables... hasta 832... cada uno con su posible clasificación

Se debe clasificar de forma justa, ni sobreclasificad ni subclasificar.

Atención con los NIVELES DE CLASIFICACIÓN

ONS — Oficina Nacional de Seguridad / Centro Nacional de Inteligencia

TABLA DE EQUIVALENCIAS entre países!

- EU TOP SECRET
- EU SECRET
- EU CONFIDENTIAL
- EU RESTRICTED

Clasificación UE	Très secret UE/EU Top Secret	Secret UE/EU Secret	Confidentiel UE/ EU Confidential	Restreint UE/EU Restricted
Clasificación OTAN	COSMIC Top Secret	NATO Secret	NATO Confidential	NATO Restricted
Clasificación ESA	ESA Top Secret	ESA Secret	ESA Confidential	ESA Restricted
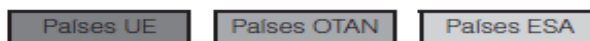
Países UE | Países OTAN | Países ESA

País	UE	OTAN	ESA				
Albania		■		Tepër Sekret	Sekret	Konfidencial	I Kufizuar
Alemania	■	■	■	Streng Geheim	Geheim	VS[1] – Vertraulich	VS – Nur für den Dienstgebrauch
Austria	■		■	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Bélgica	■	■	■	Très SecretZeer Geheim	SecretGeheim	ConfidentielVertrouwelijk	—[2]
Bulgaria	■	■		Строго секретно	Секретно	Поверително	За служебно ползване
Canadá		■		Top Secret Tres Secret	SecretSecret	ConfidentialConfidentiel	—[2]
Chipre	■			Άκρως ΑπόρρητοAbr: (ΑΑΠ)	ΑπόρρητοAbr: (ΑΠ)	ΕμπιστευτικόAbr: (ΕΜ)	Περιορισμένης ΧρήσηςAbr: (ΠΧ)
Croacia	■	■		Vrlo Tajno	Tajno	Povjerljivo	Ograničeno
Dinamarca	■	■	■	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Eslovaquia	■	■		Prísne tajné	Tajné	Dôverné	Vyhradené
Eslovenia	■	■		Strogo tajno	Tajno	Zaupno	Interno
España	■	■	■	Secreto	Reservado	Confidencial	Difusión Limitada
Estados Unidos		■		Top Secret	Secret	Confidential	—[2]

*EU RESTRICTED: Hay países con tratamiento especial al no tener el nivel: Francia, Israel, Bélgica, Canadá, EE.UU…

SOCIOS / PROVEEDORES / CLIENTES DEL CONSORCIO

No hay ABPIC con todos los países

ABPIC

Acuerdo Bilateral para Protección de Información Clasificada.

Sin ABPIC no hay programa clasificado

No se puede intercambiar IC en el programa sin acuerdo, salvo excepciones

Continua negociación para ABPIC

Para conformar un consorcio internacional

Siempre hay que revisar /consultar los ABPIC antes de formar un consorcio

INCIDENTE DE SEGURIDAD

Entidades ajenas al propietario de la IC quieren acceder a ella.

Interés comercial

Mayor riesgo para la IC

Parámetros que se deben asegurar

CONFIDENCIALIDAD

DISPONIBILIDAD

INTEGRIDAD

DATOS DE CONTACTO

Oficina Nacional de Seguridad

Muchas gracias por su atención

Programas Int.	**programas@ons.cni.es**
Sector público	**sectorpublico@ons.cni.es**
Empresas	**empresas@ons.cni.es**
Seg. personas	**segper@ons.cni.es**
Acredit. TIC	**acreditacion@ccn.cni.es**

Muchas gracias!

Marina Martínez-Garcia

Framework Programme officer at SOST-CDTI Brussels

Cluster-3 Horizon Europe National Contact Point

marina.cdti@sost.be

ESHORIZONTE**2020**

Portal español del Programa Marco de Investigación e Innovación de la Unión Europea

+ info sobre programas y ayudas
para la
internacionalización de la I+D+I española

www.eshorizonte2020.es - www.cdti.es

@EsHorizonte2020 - @CDTIoficial

HORIZONTE
EUROPA
@HorizonteEuropa

División de
Programas de la UE

ESPAÑA
PUEDE.

MINISTERIO
DE CIENCIA
E INNOVACIÓN

CDTI
@CDTIoficial