

#innovacion
#financiacion
#asesoramiento
#internacionalizacion



CDTI Centro para el
Desarrollo
Tecnológico
Industrial

@CDTIoficial



Security Scrutiny and Classified Information in H2020 proposals

Dr. Marina Martínez

marina.cdti@sost.be



@EsHorizonte2020

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

First things first...

What is “classified information” in the EU... and in H2020

EU Classified Information (EUCI)

Definition of EU Classified Information (EUCI)

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

Legal framework

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

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

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

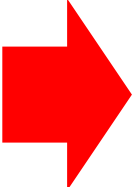
What is “classified information” in the EU... and in H2020

Also “secure sensitive information” DOES NOT ONLY relates to national security BUT ALSO to:

- ☐ **Security recommendations**
- ☐ **Dual-use goods or dangerous materials & substances** (subject to export or transfer control)
- ☐ Or the **use of data or information coming out from a previous research project** which is protected against unauthorised disclosure.

So, where can you find “Classified Information” in H2020 projects?

EUCI in research projects

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

The sensitive information regards not only to the activities & research done, but also to the consortia!!!

EUCI and proposals involving participants from third countries

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

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



ENGLISH الإنجليزية الإصدارات والتقارير البرامج والمشاريع الأنشطة والمشاركات نبذة عامة الصفحة الرئيسية



ASSOCIATION FORUM DES SCIENCES SOCIALES APPLIQUEES

Tunisia

Address

Rue De Damas Le Belvedere 6
1002 Tunis

Activity type

Other

E.P.E.



@CDTIoficial

... let's start at proposal level

Security Sensitive aspects in a proposal...

... they regards both to the “**subject of research**” as well the “**type of research**” in your project...

Potential sensitive **subject of research**:

- ☐ explosives & CBRN
- ☐ infrastructure & utilities
- ☐ border security
- ☐ intelligent surveillance
- ☐ terrorism & organised crime
- ☐ digital security
- ☐ space

Potential sensitive **type of research**:

- ☐ 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 H2020 the common situation in projects is that only deliverables may be classified.**

The best orientation is to use the “Guidelines for classification of information in R&D projects”

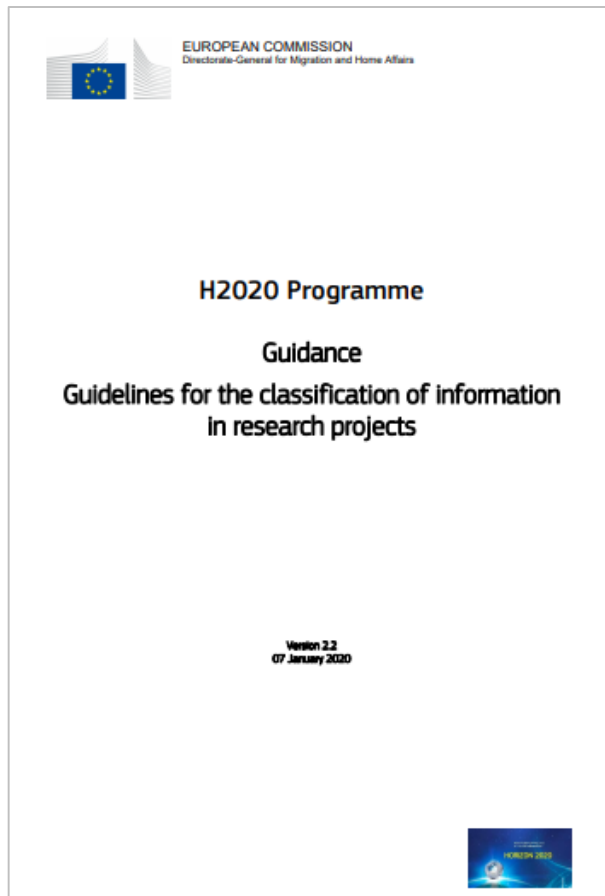


TABLE OF CONTENTS

1. When and for how long must information be classified?	4
2. Classification levels	4
3. How to classify information?	5
3.1 Explosives research.....	7
3.2 CBRN research.....	9
3.3 Critical infrastructures and utilities research.....	11
3.4 Border security research.....	13
3.5 Intelligent surveillance research	15
3.6 Terrorism research.....	16
3.7 Organised crime research	18
3.8 Digital security research	20
3.9 Space research.....	21

Let's put an example! →

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

Example of the “H2020 guidelines” regarding a project focus on “Critical Infrastructures”

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, social well-being).

How to deal with deliverables and R&D&Innovation activities on:

❑ **threat assessments?** Analyses of man-made threats to infrastructure = **EU RESTRICTED**.

If they add value (e.g. by prioritising threats), then, **EU CONFIDENTIAL**.

❑ **vulnerability assessments?** Detailed gap analyses, etc... = **EU RESTRICTED**.

If they add value (e.g. by including criticality analyses, highly detailed case studies, ...), then, **EU CONFIDENTIAL**. In case of **aviation infrastructure**, passenger and cargo security solutions = **EU CONFIDENTIAL**.

❑ **specifications?**

EU RESTRICTED if they are:

- ✓ The design, specifications and operation of software tools and platforms to prevent and detect attack, ...
- ✓ Detailed detection techniques for early-warning and event analysis, ...
- ✓ Information on sensor networks...
- ✓ Automated analysis of sensor data, the algorithms to detect security threats,...
- ✓ Detailed specifications of organisational and operational processes,...

EU CONFIDENTIAL if you are treating the design, specifications and operation of beyond the state-of-the-art screening and detection systems for **aviation**.

At level of proposal...



Part-A

Administrative information
On-line formulaire

Sections in the template...



Part-B

Technical description

ATTENTION: Download the pdf,
make a Word file and follow the
main sections!

At level of proposal...

- ❑ Fill correctly **Part-B Section -3 → table 3.1.e: “List of deliverables”**, where for each deliverable it is necessary to define its dissemination level.

Key for classification of deliverables indicating the **TYPE** and the **DISSEMINATION LEVEL**

TYPE:

- ❑ **R:** Document, report
- ❑ **DEM:** Demonstrator, pilot, prototype, plan design
- ❑ **DEC:** Website, patent filing, press & media actions, videos, etc
- ❑ **OTHER:** Software, technical diagram, etc

DISSEMINATION LEVEL:

- ❑ **PU:** Public, fully open, i.e., web
- ❑ **CO:** CONSORTIUM CONFIDENTIAL, restricted under conditions set in the model GA
- ❑ **CI:** Classified Information as referred in EC Decision 2001/844/EC



Attention: Dissemination level “CO” does NOT mean security concerns always!!!!

Table 3.1.e List of deliverables

Deliverable (number)	Deliverable name	WP number	Short name of lead participant	Type	Dissemination level	Delivery date
D1.1	Report of Kick-off meeting	1	CDTI	R	CO	Month 1
D1.2	Setup and maintenance of the internal project management tool	1	CDTI	DEM	CO	Month 2
D1.3	STCG guidelines	1	SOST	R	PU	Month 2
D1.4	Ethics Manual	1	Univ.Free	R	PU	Month 2
D6.1	Dissemination plan	6	SOST	R	CO	Month 2
D6.2	Exploitation plan	6	Univ.Free	R	CO	Month 2, 15, 24
D6.3	Public project website targeted at different user groups	6	CDTI	DEM	PU	Month 3

Protecting the cruiser and ferry ship passengers



D2.4	SAURON System Architecture and Design	WP2	UPVLC	R	PU	M9
D2.5	Legal requirements specifications	WP2	KUL	R	PU	M12
D3.1	Cyber risks and vulnerability report	WP3	S2	R	CO	M10
D3.2	Advanced User Interface	WP3	UPVLC	R	PU	M20
D3.3	Security monitoring Architecture Description	WP3	S2	R	CO	M20
D3.4	Security Monitoring System	WP3	S2	DEM	CO	M20
D3.5	External Intelligence Gathering Procedure	WP3	S2	R	PU	M20
D4.1	Physical risks and vulnerabilities analysis	WP4	ETRA	R	CO	M10
D4.2	Video analytics development	WP4	MORPHO	R	PU	M20
D4.3	Physical SA application adaptation and integration with existing systems	WP4	UPVLC	DEM	PU	M20
D4.4	Sensors integration and tactical communications	WP4	ETRA	R	PU	M20
D5.1	Cyber/Physical Infrastructures & interdependencies Models	WP5	UPVLC	R	CO	M18
D5.2	Physical and Cyber Situation Awareness fusion models	WP5	MT	R	PU	M21
D5.3	HSA Development and functional validation report	WP5	THALES	DEM	PU	M28
D6.1	Interoperability with the ports vicinity	WP6	ETRA	R	PU	M13
D6.2	Emergency Population Warning Systems analysis	WP6	ETRA	R	PU	M9
D6.3	Innovative population warning techniques development	WP6	ETRA	DEM	PU	M24
D7.1	Validation Plan report	WP7	ISEC	R	PU	M26
D7.2	Integrated System Test bed	WP7	ETRA	R	PU	M35
D7.3	First Pilot summary report and system development	WP7	VPORT	DEM	PU	M32
D7.4	Second Pilot summary report and system development	WP7	VPORT	DEM	PU	M34
D7.5	Evaluation Report	WP7	VPORT	R	PU	M36
D7.6	Risk assessment	WP7	KUL	R	CO	M36
D7.7	Policy recommendations	WP7	KUL	R	PU	M36

At level of proposal...

- ❑ Fill correctly Part-B Section -3 → table 3.1.e: “List of deliverables”, where for each deliverable it is necessary to define its dissemination level.

... but sometimes the deliverable is **“CO”** **BECAUSE** it contains **sensitive information!!!!**



At level of proposal...

- ❑ Fill correctly **Part-B Section -3** → **table 3.1.e: “List of deliverables”**, where for each deliverable it is necessary to define its **dissemination level**.

Table 3.1c: List of Deliverables

Deliverable (number)	Deliverable name	WP no	Short name of lead participant	Type	Dissemination level	Delivery date
D2.1	Identification of the Stakeholders and Practitioners requirements	2	CRBNE	R	CI with CI annex	Month 5
D2.2	Yearly updated counter-tools step-change assessments	2	CBRNE	R	CI	Months 10, 18, 35
D2.3	Final Stakeholder and Practitioners Advisory Members Report	2	CBRNE	R	CI	Month 34
D2.4	Recommendations of OR methods for practitioners	2	FOI	R	PU	Month 36
D3.1	Scenario structuring report on terrorist plots	3	FOI	R	CI	Month 7
D3.2	Detailed historical real cases	3	CAST	R	CI	Month 12
D3.3	Emerging explosive threats	3	CAST	R	CI	Month 24
D4.1	Preliminary to final typology of counter-measures across the timeline	4	FOI	R	CI	Months 9, 20
D4.2	OR toolbox for stakeholders	4	FOI	R	CO	Month 34
D5.1	Categorising of research projects regarding to the countering of explosives misuse in terrorist attacks	5	TNO	R	CO	Month 9

... in very evident sensitive cases, such as explosives, then **“CI” (Classified Information)** is the right choice! → **See the classification Guidance for EXPLOSIVES.**

At level of proposal...

- ❑ **Part-B Section 6 “Security”** when if the “Activities or results raising security issues: YES”, then, a more detailed **Security Classification Guide (SCG)** is necessary to add (6.2), which is a table giving additional information.

It is also necessary to appoint a Security officer (6.3.1), that can be assisted by a SAB (6.3.2), and you can also add any other security measures in section 6.4.

6 Security

Please complete this section if your project will involve:

- activities or results raising security issues: ☒ Yes ☐ No
- ‘EU-classified information’ as background or results: Yes / ☒ No

6.1 Security aspect letter

To be provided by commission service during the Grant Agreement preparation

6.2 Security classification guide

Annex to the Security Aspects Letter (SAL)					
Security Classification Guide (SCG)					
Production of classified results					
Subject	Classification level	Beneficiaries involved in production or wanting to access			
		Name	Responsability	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		

6.3 Security staff

6.3.1 Project Security Officer

Even that the project will follow a Security Scrutiny, it is the applicant's obligation to fill out Section-6 at level of proposal!

E.



@CDTIoficial

6. Security

- Activities or results raising security issues: NO
- 'EU-classified information' as background or results: YES

6.1 Limited dissemination list

The following deliverables are planned to handle as (business) confidential and only disseminated to project partners:

Deliverable No	Deliverable name	WP No.	Lead participant	Type	Dissemination level	Delivery date ^[Error! Marcador no definido.]
D1.1	Internal communication Infrastructure	1		OTH	CO	M2
D1.2	Quality Plan and Project Handbook	1		R	CO	M3
D1.3.1	Work Plan and Financial Reporting – Period 1	1		R	CO	M12
D1.3.2	Work Plan and Financial Reporting – Period 2	1		R	CO	M24

Table 3: List of confidential deliverables

6.2 EU classified information

In general, [redacted] will not involve activities or results raising security issues and does not aim to involve EU-classified (secret; restricted or confidential) information. However, according to the COM Decision 2015/444 and the DG HOME's H2020 Guidelines for the classification of information in research projects, it is foreseen that three deliverables may possibly need classification.

#	Title	Justification	Potential level	Current level
D3.1	End-user needs and operational requirements	In-depth gap analyses, user requirements or detailed inventories of existing capabilities in border security systems, assets, technologies, operations or processes should be classified RESTREINT UE/EU RESTRICTED. If they add value (e.g. by including criticality analyses or highly detailed case studies), they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL	CI (RES-UE or CON-UE)	CO (REC)

6.3 Security staff

6.3.1 Project Security Officer

Dr. [redacted] has significant experience in project control and review having been involved in most FP7 and H2020 projects at the administrative and contractual levels. As an experienced reviewer, he will serve as the **Project Security Officer**, representing the Security advisory at the Management Board meetings. His professional background includes 15 years of law enforcement experience and four years in the role of data protection officer for the border guard unit operated at Budapest Airport. He holds a security clearance for classified materials up to **NATO/EU TOP SECRET level**.

6.3.2 Security Advisory board

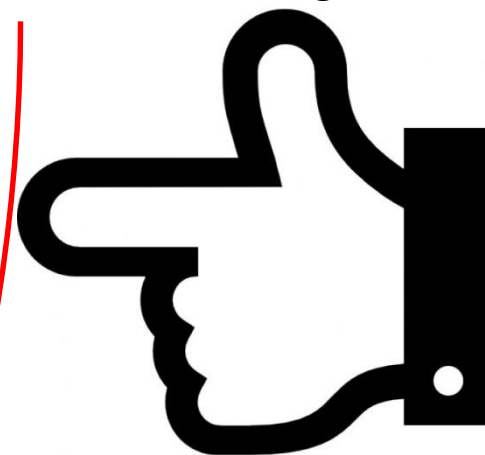
6.4 Other project-specific security measures

The project handbook will contain additional security recommendations, such as:

- password-protected repository;
- electronic signature solutions;

At level of proposal...

For example: Expert with experience, e.g., end-user or LEA, expert with security clearance, expert in data management, etc...



Even that the project will follow a Security Scrutiny, it is the applicant's obligation to fill out Section-6 at level of proposal!

nológico Industrial, L.P.E.

Centro para el Desarrollo Industrial

CDTI

@CDTIoficial

At level of proposal... more examples

6.2.2 Security classification guide (SCG)

The SCG will be updated continually during the project. The periodic reports will include updated SCG showing how EUCI has been exchanged during the period.

6.2.2.1 Classified Background

The below reports are background needed in the

Bond-007 project

Annex to the Security Aspects Letter (SAL) Security Classification Guide (SGC)		
Classified Background of information		
Subject	Classification level	Origin (Organisation/Project)
Gap Analysis-detailed analysis Feasibility study Based on scenarios developed by the expert group on detection of explosives.	EU CONFIDENTIAL (C-UE/EU-C)	DG Home Affairs
Gap analysis Based on scenarios developed by the expert group on detection of explosives	EU CONFIDENTIAL (C-UE/EU-C)	DG-JLS
Detection of explosives – working group on development of scenarios and	EU CONFIDENTIAL (C-UE/EU-C)	DG-JLS

The background
information can be CI **only**
in one country, p.e., UK.

At level of proposal... more examples

6.2.2.2 Classified Foreground

Annex to the Security Aspects Letter (SAL) Security Classification Guide (SCG)					
Production of classified <u>Foreground</u> of information					
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
D2.1 Identification of the Stakeholders and Practitioners requirements	EU RESTRICTED (R-UE/EU-R),	CBRNE	Security manager/main contributor	Month 5	Final dissemination level will be decided by the Security Board
	annex up to EU CONFIDENTIAL (C-UE/EU-C)	FOI	contributor		
		TNO	contributor		
		CEA	contributor		
		ENEA	contributor		

At level of proposal... more examples

6.3 Security staff

Any members **MySuperCarro** project who will require access will have the appropriate level of personal security clearance, and their office or place of work will have the appropriate level of Facilities Clearance, both of which will be issued by the National Security Authority of that country.

6.3.1 Project Information Security Officer

The Project Data Controller **Marina Martinez** [MDM] will also be appointed as Project Security Officer and she/he will be responsible for leading and advising on all security matters relating to the **MySuperCarro** project.

6.3.2 Security Advisory Board

MySuperCarro Security concerns. Nevertheless DC will chair such a Board, composed by 3 external experts who will be designated during the first 2 months of the project, designated to assess security sensitivity issues collaborating also with AB members having this specific skill and knowledge in case of need. The responsibilities of the SAB are: (a) check all deliverables and assess their sensitivity before submitting to EC. Each deliverable's cover page shall contain an indication that it has passed the Security Assessment control and the result of this assessment; (b) Manage the use of security sensitive information within the project tasks; (c) Manage cooperation on security issues among the project partners; (d) Safeguard the non-disclosure of security relevant information within the project interaction with third parties; (e) Report to the PCT regarding the dealing with security sensitive information, if needed; (f) Provide overall conclusions that will be included in a dedicated section

Better if at proposal level it is included a **brief CV of the SAB members and of the SO** in order to demonstrate the capacity of the experts appointed.

6.4 Other project-specific security measures

MySuperCarro consortium will review all potential EU-classified information, throughout the project life, coordinated by the **MySuperCarro** Project Security Officer (the Data Controller Manager) will chair the Security Advisory Board, promoting also collaboration with the Advisory Board, and report at the Project Consortium Board meetings, and such material/deliverable will be included in the data management guidelines (T1.4). Where a deliverable needs to be reclassified, it shall only be undertaken with the approval of the European Commission.



Bruno Halopeau
EUROPOL
O4 - Counter Terrorism Unit
EU-IRU

European Union Classified - Basic Protection Level

EUROPOL

The Hague, 26/06/2015

DIRECTOR

Syed Nazki
Birmingham City University
Millennium Point, Curzon Street,
Birmingham
B4 7XG
UK

Subject: Letter of Intent to support the RED-Alert Project (application for funding under FCT-6-2015)

Dear H. Nazki,

Europol (The European Union's law enforcement agency for law enforcement cooperation), was established to support Member States law enforcement cross-border activities.

The stated objectives of the RED-Alert project are to develop and test a real-time system that is able to facilitate the real-time identification of terrorist-related content by surveilling large amounts of data from social and other online sources (e.g. blogs, forums). The system will use NLP and NLP technologies to detect anomalies in content production, content volume, content spread in order to provide early detection of terrorist activities. The system will also use CSP technologies in order to predict potential threat areas via patterns in content and content production. The system contains these technology building blocks with machine-learning methods (AI) in order to analyse, monitor or take action on terrorist content detected online. By entering this project Europol will benefit from having full access to the tools and software developed as a part of the project as well as being a part of a network of third parties and their research and development programmes.

As a consequence, Europol would like to express its interest in involving the RED-Alert project by becoming part of your Advisory Board. We will contribute manpower towards the project in order to advise you on the law enforcement needs and by providing feedback after testing the product.

Europol anticipates being able to:

- attend 3 meetings of the Advisory Board per year; and
- provide 2 tasks for a period of approximately 2 weeks (when calculated as full time equivalent) for each testing activities.

This is subject to manpower and financial resources being available.

Any public announcement referring to Europol must be agreed with Europol prior to its release.

CONTACTS:

Coordination Unit 1127 AX The Hague The Netherlands	P.O. Box 906 36 2200 LN The Hague The Netherlands	Phone: +31(0)70 352 30 00 Fax: +31(0)70 345 14 90 www.europol.europa.eu
---	---	---

Bruno Halopeau is currently Strategic Advisor in the EU IRU (Internet Referral Unit) in the Counter-Terrorism Unit at Europol in charge of tackling propaganda and radicalisation online. He holds an MSc degree in Computer Science from ESIEA Paris in 1998, and is passionate about challenging engagements particularly on Security and Safety issues; he therefore dedicated his career to the Cybersecurity field & fight against Cybercrime with a particular focus in the last year on Cyber-Terrorism matters and study of Terrorist groups ICT capabilities/skills. His scientific background helped him to build a sound knowledge in Modelling and Social Network Analysis which is of particular interest for this project. He is an international speaker involved in many EU initiatives about EU Security and Safety. He was also invited to write a chapter about "Terrorist use of the Internet" (Akhgar B. et Al, 2014. CyberCrime and CyberTerrorism Investigator's handbook, Elsevier, pp 123-32). Bruno holds an MSc in Strategic Management and Competitive Intelligence from Ecole de Guerre Economique (EGE) in 2010 and having worked equally long both in the private and public sector empowers him to have a sound and broad knowledge on Cyber matters. Finally, he currently pursues an MBA at the Warwick Business School.

Europol O4 (Counter Terrorism Unit) will support the RED-Alert project and attend the main consortium meetings. The role of Europol will be to 1) provide domain-specific feedback about the technologies developed in the project, 2) support the organization of LEA workshops to disseminate project results and 3) contribute to the market adoption of the solution within LEAs once the project is completed.

At level of proposal... more examples

Better if at proposal level it is included a **brief CV of the SAB members and of the SO** in order to demonstrate the capacity of the experts appointed.

Guidelines for researchers on dual use and misuse of research

Institutions and funding bodies aim to raise researchers' awareness of the issues relating to dual use and misuse of research and help them to handle this appropriately. Researchers indeed have a legal and ethical obligation to prevent or mitigate as much as possible the risks and potential damage which may be caused by malicious use of their research results.

1 Responsibility

Handling research responsibly requires the active commitment from research institutions, funding bodies, and others. However, the researchers concerned also play a key role and must take their responsibility. The researcher is indeed best placed to assess the nature and seriousness of potential misuse relating to the intended knowledge, products or technologies and must, if the occasion arises, report this within the research institution and to the funding body (see point 3).



2 Definition of dual use and misuse of research results

In the ethics self-assessment table within the framework of Horizon 2020 the European Commission distinguishes between two concepts: on the one hand, the concept of use for **civil versus**

military purposes (described below as dual use), and on the other hand the concept of **good versus bad** use (described below as misuse).

2.1 Dual use of research

In Article 2 of Council Regulation (EC) No 428/2009 'dual-use items' are defined as *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.*

European legislation on the **export of dual-use items** (EU export control Regulation No 428/2009) requires that the EU countries take appropriate control measures to counter the undesirable and uncontrolled proliferation of dual-use items, software and knowledge specified on the dual-use control list to non-EU countries. This means that the export of such dual-use items to non-EU countries is **subject to authorisation**. In European legislation dual-use items are defined as items which are primarily used for civil (academic or industrial) purposes, but can also be used for military purposes. In accordance with Article 4 of Council Regulation (EC) No 428/2009

(the so-called **catch-all** provision), an authorisation is also required for items which do not feature on the dual-use list, if the country of destination is subject to an arms embargo and the items may be intended, in their entirety or in part, for a military end-use, or if the items may be intended, in their entirety or in part, for the production and proliferation of chemical, biological or nuclear weapons of mass destruction and their means of delivery (e.g. missiles capable of delivering such weapons) (see point c).

The three pillars of the control of the trade in dual-use items to non-EU countries (and for a limited

https://www.uhasselt.be/documents/DOC/2017VLIR003_FolderOnderzoek_EN_DEF_20180212.pdf



División de
Programas de la UE

@EsHorizonte2020

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



CDTI Centro para el
Desarrollo
Tecnológico
Industrial

@CDTIoficial

**... once the proposal is
submitted...**

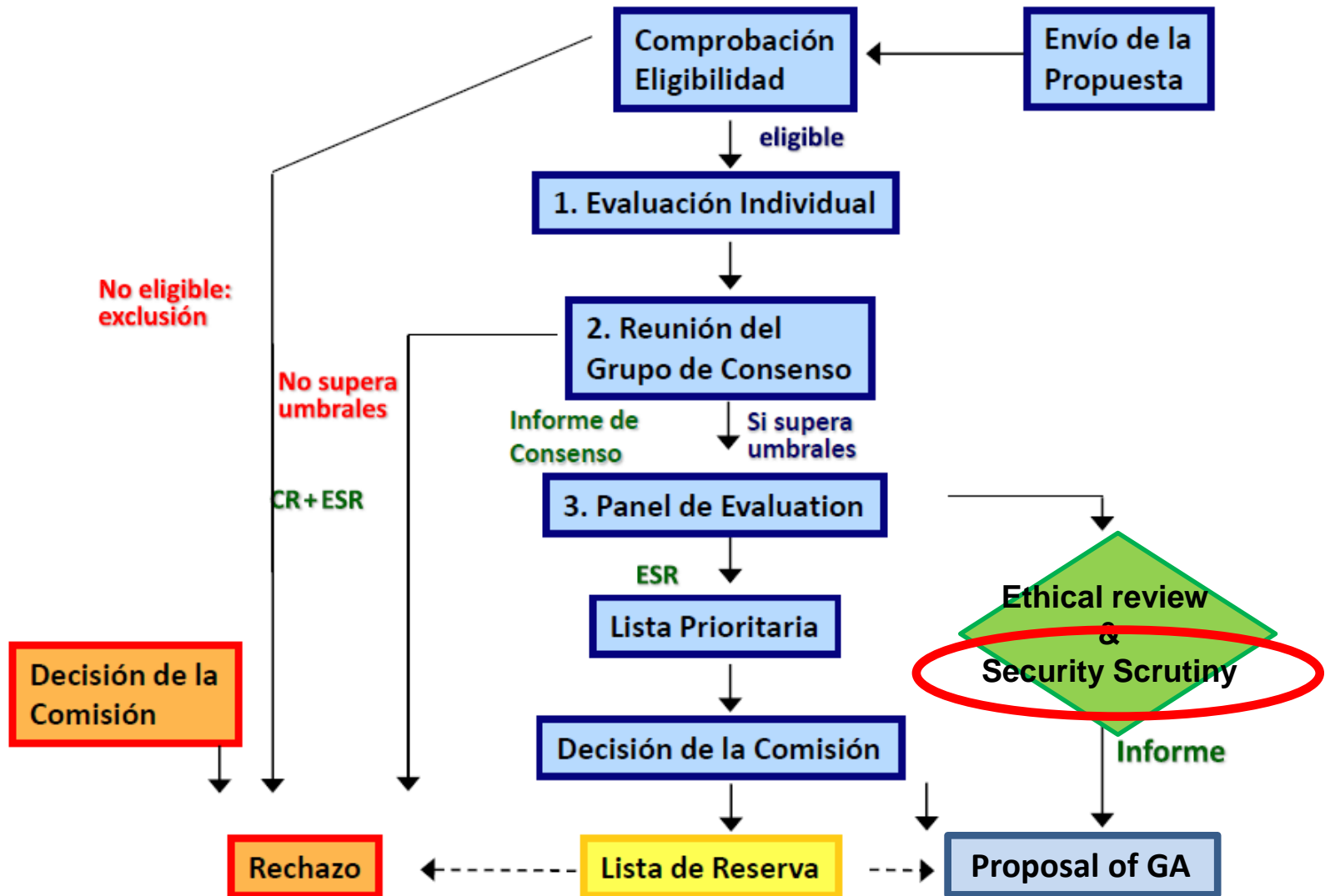
What happens after submission?

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

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

E.g., MSCA projects that the project coordinator would identify as potentially security sensitive... even not noticed by the researcher or the consortia at proposal level!

When is the security scrutiny of proposal taking place?...



Security Scrutiny Process...

❑ **What is? → It consists in the analysis of the deliverables and activities of a proposal regarding the use of background, foreground or management of secure sensitive information from the National Security point of view. → NOT Confidential from the commercial/exploitation point of view!**

Objectives of the Security Scrutiny:

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

It is not a technical re-evaluation of the proposal!!!

Security Scrutiny Process...

❑ **Who** → It is performed by the **Security Scrutiny Group** composed by experts (they may come from the NSAs or may be experts in agreement with their NSAs...) that check the proposals.

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

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

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

- 1) the **subject** of the research results (i.e. explosives, CBRN, infrastructure and utilities, border security, intelligent surveillance, terrorism, organised crime, digital security and space).
- 2) the **type** of the research results (i.e. threat assessments, vulnerability assessments, specifications ,capability assessments, incidents/scenarios) .

Security Scrutiny process...

- ☐ **How** → The experts are looking in the proposals: Nature of the **activities & research** (from the security point of view), nature & content of the **deliverables**, **background information** used, **dissemination** level of the deliverables (**table 3.1.c**), **partners** in the consortium (i.e., nationality for security agreements with MMSS or EU, who has access to what deliverables,...), **Section-6**, ... any other aspect that may raise security sensitive issues according the EU Guidance!

As a result, your proposal will be classified such as:

- ☐ Proposal with **No Security Concerns (NSC)**
- ☐ No classification **but Recommendations for the Grant Agreement** preparation
- ☐ **"Restricted UE"** and recommendations for the grant agreement preparation
- ☐ **"Confidential UE"** and recommendations for the grant agreement preparation
- ☐ **"Secret UE"** and recommendations for the grant agreement preparation
- ☐ **Not to finance the proposal**

Security Scrutiny results...

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

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

→Classification and recommendations for the grant agreement;

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

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

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

→Recommendation not to finance the proposal

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

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

ARTICLE 37 — SECURITY-RELATED OBLIGATIONS

37.1 Results with a security recommendation

[OPTION 1 if applicable to the grant: The beneficiaries must comply with the 'security recommendation(s)' set out in Annex 1.

For security recommendations restricting disclosure or dissemination, the beneficiaries must — before disclosure or dissemination to a third party (including linked third parties, such as affiliated entities) — inform the coordinator, which must request written approval from the [Commission][Agency].

In case of changes to the security context, the beneficiaries must inform the coordinator, which must immediately inform the [Commission][Agency] and, if necessary, request for Annex 1 to be amended (see Article 55).]

[OPTION 2: Not applicable]

37.2 Classified information

[OPTION 1 if applicable to the grant: The beneficiaries must comply with the security classification set out in Annex 1 ('security aspect letter (SAL)' and 'security classification guide (SCG)').

Information that is classified must be treated in accordance with the security aspect letter (SAL) and Decision No 2015/444¹⁰ — until it is declassified.

Action tasks involving classified information may not be subcontracted without prior explicit written approval from the [Commission][Agency].

In case of changes to the security context, the beneficiaries must inform the coordinator, which must immediately inform the [Commission][Agency] and, if necessary, request for Annex 1 to be amended (see Article 55).] *[OPTION 2: Not applicable]*

37.3 Activities involving dual-use goods or dangerous materials and substances

[OPTION 1 if applicable to the grant: 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.]

[OPTION 2: Not applicable]

37.4 Consequences of non-compliance

[OPTION 1 to be used if 37.1, 37.2 and/or 37.3 are applicable: If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).]

Such breaches may also lead to any of the other measures described in Chapter 6.]

[OPTION 2: Not applicable.]

¹⁰ Commission Decision 2015/444/EC, Euronext of 11 March 2015 on the security rules for protecting EU classified information.

Security Scrutiny

Status: Security Issues

1. Are there any security concerns?

Yes

Justification

There are security concerns linked to the point that training program may reveals weaknesses in the LEAs operations.

2. Any recommendations?

Yes

2A. SAB – Security Advisory Board (DoA section 6.3)

Yes

Justification/Recommendation

As foreseen in the proposal, a Security Advisory Board (SAB) will be appointed. The SAB will support the Project Security Officer (PSO). The SAB will consist of representatives from LEAs in the consortium and will have the task of monitoring the dissemination level of the concerned deliverables in table 12.

2B. PSO – Project Security officer (DoA section 6.3)

Yes

Justification/Recommendation

As foreseen in the proposal, a Project Security Officer (PSO) will be appointed.

2C. Limited dissemination (DoA section 6.1)

No

List of deliverables subject to limited dissemination and further recommendations

Not provided

2D. Other recommendation, if any (DoA section 6.4)

Yes

Justification/Recommendation

The following deliverables may only be accessed by the consortium and the EC (CO):

D3.4 Diagnostic assessment and profiling battery

D4.4 Analysis of components of training methods

D4.5 Cyber-experience evaluation assessment requirements and methods

D5.1 Training delivery and authoring Platform architecture and specification

D5.2 Training delivery and authoring Platform - "Field-trials ready" release

D7.3 & 7.4 Results & assessment of the Field Test

A public version of these deliverables, approved by the SAB, may be released to the general public.

Example -1:

NSC but Recommendations

Most of the times it is enough to have a **“limited dissemination list”** to only the members of the consortium & EC, p.e., and to monitor the content of the spotted deliverables by the SAB.

Status: **Security issues**

1. Are there any security concerns?

Yes

Justification

This project contains EU classified information and may therefore raise security issues, in particular regarding threats to the hospital/health infrastructure.

2. Any recommendations?

Yes

2A. SAB – Security Advisory Board (DoA section 6.3)

Yes

Justification/Recommendation

The project must set up a Security Advisory Board (SAB) to address security matters and ensure the proper handling of sensitive and classified information. The SAB should also review deliverables prior to dissemination.

2B. PSO – Project Security officer (DoA section 6.3)

Yes

Justification/Recommendation

The project must appoint a Project Security Officer (PSO) to support the work of the SAB.

2C. Limited dissemination (DoA section 6.1)

No

List of deliverables subject to limited dissemination and further recommendations

Not provided

2D. Other recommendation, if any (DoA section 6.4)

Yes

Justification/Recommendation

*The following deliverables may only be accessed by the EC and the consortium (CO):
D4.3 and D6.2.*

3. Classified information? (MGA article 37.2, DoA annex 6.2)

Yes

3A. Restreint UE/EU Restricted? (DoA section 6.2 - SCG)

Yes

Example-2: EU Restricted

Example-2: EU Restricted

3A. Restreint UE/EU Restricted? (DoA section 6.2 - SCG)

Yes

List of deliverables with Restreint UE/EU Restricted classification and further recommendations

The following deliverables should be classified as EU-RESTRICTED/RESTREINT UE:

D2.2: Description of the operational scenario and user needs

D3.1: [REDACTED] system design

D4.2: Dynamic risk assessment software tool

D5.1: Radar technologies for healthcare infrastructures protection

D6.1: Sensor network for indoor surveillance at the hospital

D7.1: Architecture and design of the cybersecurity subsystem

D7.2: Cybersecurity subsystem

D8.1: Network resilience subsystem design

D8.2: Network resilience subsystem implementation and results

A public version of these EU-RESTRICTED/RESTREINT UE deliverables, approved by the SAB, may be released

3B. Confidential UE/EU Confidential? (DoA section 6.2 - SCG)

No

List of deliverables with Confidential UE/EU Confidential classification and further recommendations

Not provided

3C. Secret UE/EU Secret? (DoA section 6.2 - SCG)

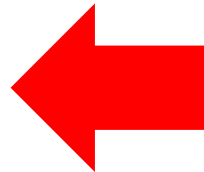
No

List of deliverables with Secret UE/EU Secret classification and further recommendations

Not provided

4. Recommendation not to finance the proposal?

No



Contact your NSA in order to know the security conditions that you have to fulfill at national level!

Example -3: EU Confidential

Security Scrutiny
Status: <u>Security Issues</u>
1. Are there any security concerns?
Yes
Justification
<i>The proposal deals with critical infrastructures which may raise security issues and involves EU classified information.</i>
2. Any recommendations?
Yes
2A. SAB – Security Advisory Board (DoA section 6.3)
Yes
Justification/Recommendation
<i>As foreseen in the proposal, the project must set up a Security Advisory Board (SAB) comprising individuals with experience in security matters, including end-user representatives. The SAB should review all deliverables prior to dissemination. SAB members must have the appropriate security clearance.</i>
2B. PSO – Project Security officer (DoA section 6.3)
Yes
Justification/Recommendation
<i>As foreseen in the proposal, the project must appoint a Project Security Officer (PSO). The PSO should support the work of the SAB. The PSO should have the appropriate security clearance.</i>
2C. Limited dissemination (DoA section 6.1)
No
List of deliverables subject to limited dissemination and further recommendations
<i>Not provided</i>
2D. Other recommendation, if any (DoA section 6.4)
Yes

Special measures should be taken by members of the consortium dealing with **EU-Confidential information** → P.e., special security zones in their premises, encrypted communications, etc... → **Contact your NSA**

Example -3: EU Confidential

Justification/Recommendation

The following deliverables may only be accessed by the consortium and the EC (CO):

D.1.2, 2.5, 2.6, 3.1, 3.2, 3.5-3.12, 4.2-4.4, 5.3, 6.2, 6.3, 8.7, 8.8, 9.1, 9.2, 9.6 and 9.7

3. Classified information? (MGA article 37.2, DoA annex 6.2)

Yes

3A. Restreint UE/EU Restricted? (DoA section 6.2 - SCG)

Yes

List of deliverables with Restreint UE/EU Restricted classification and further recommendations

The following deliverables should be classified **RESTREINT UE/EU RESTRICTED**:

- D1.3 Risks, Threats and Vulnerabilities
- D3.3: Components for information processing and management (interim)
- D3.4: Components for information processing and management (final)
- D4.1 Business Case 1 Scenario Definition
- D4.5 Business Case 1 Performance Evaluation
- D5.2 Business Case 2 Components Customized
- T6.1: Business Case 3 Scenario
- D6.4 Business Case 3 Pilot Execution
- D6.5 Business Case 3 Performance Evaluation
- D7.7: White paper, lessons learnt from [REDACTED] and recommendations for cyber-physical resilience of EU Gas.

3B. Confidential UE/EU Confidential? (DoA section 6.2 - SCG)

Yes

List of deliverables with Confidential UE/EU Confidential classification and further recommendations

The following deliverables should be classified **CONFIDENTIEL UE/EU CONFIDENTIAL**:

- D5.1 Business Case 2 Scenario Definition
- D5.4 Business Case 2 Pilot Execution
- D5.5 Business Case 2 Performance Evaluation
- D7.1: Validation plan
- D7.6: Overall validation and performance evaluation

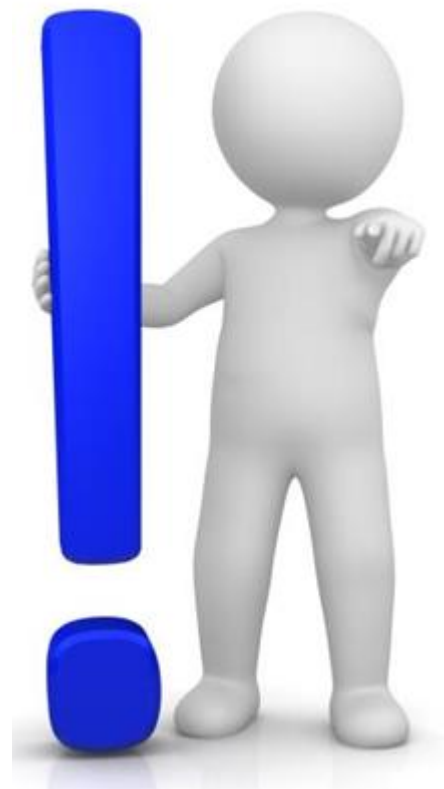
Please note that a personnel security clearance (PSC) is required to handle **CONFIDENTIEL UE/EU CONFIDENTIAL** information.

In case of **EU-Confidential**, the personnel dealing with this information would have **SECURITY CLEARANCE** accordingly... in addition of physical security means of the place of research, data security management and handling, appropriated communication systems,... → **Contact your NSA**

When the participant receives the ESR and the information letter, if the project rises **Classified Information**, that is, **EU-RESTRICTED and above**, you should contact your NSA or your delegate (ask to you NCP), in order to get detailed information of your national security instructions to be fulfilled.

Final recommendation:

If you envision that your project may rise security sensitive information of may have CI, it is worthwhile to **contact your NSA in order to prepare your organisation**, for instance, in case of need specific conditions in your premises, etc...



Many thanks!

Dr Martínez-Garcia

H2020 Programme at SOST-CDTI office

marina.cdti@sost.be