EUROPEAN COMMISSION
Directorate-General for Migration and Home Affairs

H2020 Programme

Guidance

Guidelines for the classification of information in research projects

Version 2.1
26 October 2016

IMPORTANT NOTICE

This document aims to assist **national experts** with the security scrutiny of H2020 proposals, inform **applicants** on how information will be EU-classified and help **Commission staff** to decide about the sensitivity of their call for proposals.

⚠ This guidance concerns solely protective measures to be taken to preserve the confidentiality of security-sensitive information in H2020 research projects. Other aspects *(e.g. data protection, ethical issues, dual-use, etc.)* are covered in other parts of the evaluation procedure.

⚠ Pending the adoption of implementing rules for Commission Decision 2015/444 on the security rules for protecting EU classified information, certain provisions in this guide are still based on Commission Decision 2001/844. In the absence of new guidelines they should continue to be applied.

Under the new security rules, all classification markings must now be written in FR/EN format *(e.g. RESTREINT UE/EU RESTRICTED)*.

HISTORY OF CHANGES		
Version	**Publication Date**	**Change**
1.0	11.07.2013	▪ Initial version
2.0	23.02.2015	▪ DGT and LS redraft
2.1	21.10.2016	▪ Change of title. Small changes. ▪ LS validation of new sections 3.8 and 3.9

TABLE OF CONTENTS

1. When and for how long must information be classified?

Under the Decision 2015/444[1], information must be classified if its **unauthorised disclosure could adversely impact the interests** of the EU 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*

To minimise costs and restrictions caused by classifying project information, the classification will be for a limited time — after which classification will be reviewed and possibly downgraded, declassified or even extended.

⚠ Classification of information may be combined with other **security recommendations (REC)** *(e.g. limited dissemination, creation of a security advisory group, limiting the level of detail, using a fake scenario, excluding the use of classified information, etc.).*

2. Classification levels

There are four **levels of classification**:[2]

- TRÈS SECRET UE/EU TOP-SECRET **(TS-UE)**

  ⚠ TRÈS SECRET UE/EU TOP-SECRET is NOT used for the security scrutiny of research proposals.

- SECRET UE/EU SECRET (**SEC-UE**)

  Use this classification for information which could *seriously harm* essential EU or national interests.

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

- CONFIDENTIEL UE/EU CONFIDENTIAL **(CON-UE)**

  Use this for information which could *harm* essential EU or national interests.

  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 **(RES-UE)**

Use this for information which could be **disadvantageous** to those interests.

---

1 *See Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p.53.)*

2 *See. Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p.53.)*

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

3. How to classify information?

The classification of information produced by research projects will normally depend on two parameters:

- the **subject-matter** of the research:
  - **explosives**
  - **CBRN**
  - **critical infrastructure and utilities**
  - **border security**
  - **intelligent surveillance**
  - **terrorism**
  - **organised crime**
  - **digital security**
  - **space**

AND

- the **type** of the research/results and whether it is being done in simulated environments (*e.g. serious gaming, etc.)* or in real world experimentation
  - **threat assessments** (i.e. estimation of the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact)
  - **vulnerability assessments** (i.e. description of gaps or weaknesses in networks, services, systems, assets, operations or processes which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses)
  - **specifications** (i.e. exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures)
  - **capability assessments** (i.e. description of the ability of an asset, system, network, service or authority to fulfil its intended role — and in particular the capacity of units, installations, systems, technologies, substances and personnel that have security-related functions to carry these out successfully)
  - **incidents/scenarios** (i.e. detailed information on real-life security incidents and potential threat scenarios:

- on past incidents (often including details not otherwise publicly available, demonstrating the real-life effects of particular attack methods or security gaps which have since been addressed)
- on devised scenarios (commonly derived directly from existing vulnerabilities, but normally with a lower level of detail, particularly of the attack preparation phase)).

⚠ These categories are not exhaustive, and may overlap.

3.1 Explosives research

What?

'**Explosives**' are solid or liquid substances (or mixtures of substances) which are capable — by chemical reaction — of producing gas at such a temperature, pressure and speed as to cause damage to the surroundings.[3]

How to deal with threat assessments?

Information on *e.g. the availability of precursors, the manufacturing capabilities of adversaries and the effectiveness of explosives they produce* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL. If it adds value *(e.g. by prioritising these threats)*, it should be classified SECRET UE/EU SECRET.

How to deal with vulnerability assessments?

Assessments of *e.g. current capacity to detect explosives and mitigate explosions (which may include a critical analysis of existing practices or extant abilities)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with specifications?

Specifications relating to explosives may refer to threat substances or to countermeasures.

Specifications for the manufacture, safe handling or chemical and operational characteristics of threat substances should be classified CONFIDENTIEL UE/EU CONFIDENTIAL. This includes in principle recipes for homemade explosives (HMEs). If the recipes have been validated or experimentally assessed, they should however be classified SECRET UE/EU SECRET. HME recipes that were already publicly available when the applicants applied for funding *(such as manufacturing instructions published on the internet)* do not need to be classified.

The name, chemical characteristics and operation of inhibitors used in countermeasures should be classified CONFIDENTIEL UE/EU CONFIDENTIAL. Research on the removal or attempted removal of inhibitors should be classified SECRET UE/EU SECRET.

The design, characteristics, operation and requirements of, and prototypes for, key functional devices used as components in detection *(such as samplers, sensors, lasers and lidars)* should be classified RESTREINT UE/EU RESTRICTED. Details of soft detection methods, such as data mining, online HME resources discovery and social media analysis techniques, should also be classified RESTREINT UE/EU RESTRICTED.

The design, characteristics and operation of, and prototypes for, chemical or physical mitigation and containment countermeasures should be classified RESTREINT UE/EU RESTRICTED.

Information concerning forensic methods and procedures, such as protocols for forensic sampling, methods of forensic analysis and detailed information on crime scene procedures should be classified RESTREINT UE/EU RESTRICTED.

---

[3] *See Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on Classification, Labelling and Packaging of Substances and Mixtures, Amending and Repealing Directives 67/548/EEC, 1999/45/EC and amending Regulation (EC) No 1907/2006. (O.J. L 35, 31.12.2008, p. 1-1355)*

How to deal with capability assessments?

Detailed information or test reports on the capabilities of beyond the state-of-the-art detection subsystems *(such as spectroscopic subsystems)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL. Demonstrations of systems in selected scenarios, evaluations of detection devices and assessments of the performance of mitigation and neutralisation methods should be classified RESTREINT UE/EU RESTRICTED.

How to deal with incidents/scenarios?

Detailed scenarios (and any risk analysis or guidance tools that feature detailed scenarios), potential consequences or responses should be classified RESTREINT UE/EU RESTRICTED, as should detailed accounts of individual real-life incidents which may contain information not publicly available. Incident information to which value has been added *(e.g. itemised attack databases, matrices of IED events or detailed analyses of numerous incidents)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

3.2 CBRN research

What?

'**CBRN**' means chemical, biological, radiological or nuclear substances and materials.

CBRN research covers research on:

- malicious use of CBRN ('preventive CBRN research') and
- preparedness and response to accidental, man-made or natural incidents.

How to deal with threat assessments?

Threat assessment information, which usually concern the availability of threat substances and the hazard that individual substances pose to European and national security, should be classified RESTREINT UE/EU RESTRICTED.

How to deal with vulnerability assessments?

Vulnerability refers mainly to the ability to detect and neutralise CBRN threat substances; this may include assessments of the susceptibility of certain organisms to particular threat substances. Such research should be classified RESTREINT UE/EU RESTRICTED. Vulnerability assessments that take a system-of-systems approach (incorporating gap analyses of a wide range of infrastructures, countermeasures and operations) should be classified SECRET UE/EU SECRET.

How to deal with specifications?

CBRN research referring to specifications for threat substances (their manufacture, characteristics, operation and effects) or to countermeasures (their design, operation and requirements) should be classified as follows:

Detailed information on threat substances *(e.g. toxicity and dose response information)* that is beyond the state-of-the-art should be classified RESTREINT UE/EU RESTRICTED.

Information on CBRN countermeasures (detection devices, treatment devices and forensic tools) should be classified as follows:

The design, proofs of concept, characteristics, operation and requirements of, and prototypes for, key functional devices for use in detection *(such as samplers, plastic scintillators and sensors)* should be classified RESTREINT UE/EU RESTRICTED. Systems-level information *(such as operating systems, platforms, software and algorithms)* should also be classified RESTREINT UE/EU RESTRICTED.

The design, proofs of concept, characteristics, operation and requirements of, and prototypes for, key functional devices for use in treatment, if precise, should be classified RESTREINT UE/EU RESTRICTED, as should detailed operational information on treatment processes.

The design, proofs of concept, characteristics, operation and requirements of, and prototypes for, key functional devices, tools, processes, protocols or systems with forensic functions *(such as discriminating between strains or determining whether CBRN substances have been intentionally introduced)* should be classified RESTREINT UE/EU RESTRICTED.

How to deal with capability assessments?

Assessments, demonstrations or test reports on the capabilities of beyond the state-of-the-art CBRN detection or neutralisation devices in laboratory or simulated environments should be classified RESTREINT UE/EU RESTRICTED.

Demonstration and test reports, or other detailed information, on the performance of beyond the state-of-the-art CBRN detection or neutralisation devices in real-life environments *(such as identifiable water treatment plants)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

Other capability-related information *(such as analyses of detection limits, evaluations of particular systems software or detailed examples of use cases)* should be classified RESTREINT UE/EU RESTRICTED.

How to deal with incidents/scenarios?

Databases on CBRN incidents, analyses of the factors influencing the impact and course of past CBRN events and detailed information on possible CBRN scenarios should be classified RESTREINT UE/EU RESTRICTED.

Detailed information on possible CBRN scenarios based on specific, identifiable, real-life settings should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

3.3 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

[4] *See Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 77)*

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.

3.4 Border security research

What?

'**Border security**' covers, for instance:

- monitoring of authorised crossing points, including the verification of legal entry of persons into a territory and the inspection of persons, objects and vehicles to detect and prevent threats to security
- monitoring of unauthorised crossing points

⚠ It concerns the EU as a whole, the Schengen area, individual EU countries and possibly associated countries.

How to deal with threat assessments?

Threat analyses should be classified RESTREINT UE/EU RESTRICTED. If they add value *(e.g. by prioritising the threats)*, they should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with vulnerability assessments?

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.

How to deal with specifications?

Detailed information on the design, characteristics, operation and requirements of, and prototypes for, key functional devices for use in border security, such as sensors and radars, should be classified RESTREINT UE/EU RESTRICTED.

Systems information *(such as the functional or technical architecture, operating systems, platforms, software and algorithms)* should be classified RESTREINT UE/EU RESTRICTED.

Information on the design, characteristics, pattern recognition, operation and requirements of X-ray devices, specifically those used on cargo, should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

Detailed information on operational processes should be classified RESTREINT UE/EU RESTRICTED. This includes information on communication and interoperability *(such as frequencies used, data rates and communication protocols)*.

How to deal with capability assessments?

Reports on the performance of key functional devices *(such as sensors or radars)* and of completed systems in simulated environments should be classified RESTREINT UE/EU RESTRICTED. Evaluations of the performance of key functional devices and systems installed in real-life sites should also be classified RESTREINT UE/EU RESTRICTED.

Detailed information on the capabilities of X-ray scanning equipment used on cargo *(such as detection limits)* should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with incidents/scenarios?

Detailed information on previous incidents or in-depth scenarios for potential events should be classified RESTREINT UE/EU RESTRICTED.

3.5 Intelligent surveillance research

What?

'**Intelligent surveillance**' means the use of pattern recognition and other artificial intelligence techniques to analyse data obtained from more conventional security devices, with the aim of identifying behaviour deemed suspicious or anomalous with regard to the given legal and social context.

How to deal with…

⚠ Classification is currently not foreseen in this area. This may change in the future.

3.6 Terrorism research

What?

'**Terrorism**' refers to criminal offences committed with one (or more) of the following goals:

- seriously intimidating a population
- unduly compelling a government or international organisation to perform or abstain from performing any act
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or international organisation.[5]

How to deal with threat assessments?

Threat assessments of terrorist organisations should be classified RESTREINT UE/EU RESTRICTED.

How to deal with vulnerability assessments?

Detailed evaluations of the current capacity of law enforcement staff to predict, detect, understand and respond to terrorist strategies, attacks and activity should be classified RESTREINT UE/EU RESTRICTED. General assessments of the vulnerability of urban locations to terrorist attack should also be classified RESTREINT UE/EU RESTRICTED. *(See also Explosives and CBRN.)*

How to deal with specifications?

Information on four main types of law-enforcement measures to counter terrorism should generally be classified RESTREINT UE/EU RESTRICTED:

- prediction: anticipating the decisions, behaviour, strategies, attacks and other activities of terrorist groups (including any techniques for predicting terrorist actions, *such as decision-making and behavioural models*)
- detection: identifying terrorist operatives and their activities or plans *(e.g. through operational activities such as intelligence-gathering)* and technical information on detection devices *(such as sensors, pattern recognition, algorithms and operating systems)*
- understanding: obtaining detailed information on processes such as radicalisation *(e.g. through case studies of radicalised individuals and conceptual models detailing the radicalisation process, including information such as psychological indicators)*
- response: action based on the three previous categories *(e.g. operational and strategic information)*.

[5] *See Council Framework Decision of 13 June 2002 on Combating Terrorism U.N. Doc. 2002/475/JHA, (OJ L 164 22.6.2002, p. 3-7).*

How to deal with capability assessments?

This covers:

- law enforcement agencies' capabilities to predict, detect and respond to terrorist activities in light of the potential advances detailed in specific projects
- the capabilities of individual state-of-the-art prediction and detection techniques and systems
- the capabilities of intervention programmes, particularly with regard to radicalisation
- the technological and operational ability of law enforcement personnel to respond to terrorist activities.

Detailed information on the performance of integrated systems to predict, detect, understand and respond to terrorism, in simulated environments, should be classified RESTREINT UE/EU RESTRICTED, as should information on the operating and technological capabilities of law enforcement personnel.

Information on the performance of integrated systems to predict, detect, understand and respond to terrorism, in real-life environments, should be classified CONFIDENTIEL UE/EU CONFIDENTIAL.

How to deal with incidents/scenarios?

Detailed information on previous terrorist attacks and detailed scenarios of potential attack strategies should be classified RESTREINT UE/EU RESTRICTED.

3.7 Organised crime research

What?

'**Organised crime**' means a structured association of more than two persons acting together to commit serious offences to obtain, directly or indirectly, financial or other material benefits.[6]

How to deal with threat assessments?

Assessments of the threat(s) of organised crime should be classified RESTREINT UE/EU RESTRICTED.

How to deal with vulnerability assessments?

Detailed information on gaps in existing systems, tools and methodologies for predicting and detecting organised criminal activities should be classified RESTREINT UE/EU RESTRICTED.

How to deal with specifications?

The following specifications of measures to predict, detect and respond to organised crime should be classified RESTREINT UE/EU RESTRICTED:

- the identification and prioritisation of indicators
- detailed information on factors which influence the development of organised crime
- detailed specifications of technical countermeasures *(e.g. the design, prototypes, characteristics, operation and requirements of key functional tools and systems and information on the software and algorithms employed)*
- detailed information on the operational processes or strategies used by law enforcement personnel to respond to organised criminal acts.

How to deal with capability assessments?

Assessments of the capabilities of law enforcement personnel to predict and detect organised criminal activities including:

- detailed information or test reports on the capabilities of beyond the state-of-the-art detection subsystems *(such as intelligent surveillance systems)*
- demonstrations of systems and evaluations of detection devices, in both simulated and real-life environments
- assessments of the performance of prediction methods and models

should be classified RESTREINT UE/EU RESTRICTED.

Technical, operational and strategic capabilities of law enforcement personnel to respond to organised crime should also be classified RESTREINT UE/EU RESTRICTED

[6] *See Council Framework Decision 2008/841/JHA (OJ L 300, 11.11.2008, p.42-45).*

How to deal with incidents/scenarios

Detailed information on previous incidents or representative scenarios of organised crime should be classified RESTREINT UE/EU RESTRICTED.

3.8 Digital security research

What?

'**Digital security**' covers a wide range of research topics linked to security aspects of ICT components, devices, systems and services, communication protocols and networks (including technological and procedural measures to ensure confidentiality, integrity and availability of information).

How to deal with…

Usually there is no need to classify proposals in the area of digital security research, because In most cases ICT systems (or the measures to ensure their security) do not need any classification.

Particular attention should, however, be paid in the following areas:

- vulnerability assessments — During the research activities, projects may come upon previously unknown vulnerabilities ('zero-day vulnerabilities'); in this case, responsible disclosure is required.
- use-case risk assessment — Depending on the type of use-case and the context *(e.g. critical infrastructure)*, the results of information security risk assessments, (especially if obtained in operational or near operational environments) may include certain threats and/or vulnerabilities that require classification.
- governmental cryptology — Classification might be necessary (but research in this area does not fall within the scope of H2020).

Moreover, classification may be needed if the research extends to security sensitive information that is stored within ICT systems. In this case, the classification must be made in accordance with the rules for that area *(e.g. explosives, CBRN, critical infrastructure and utilities, border security, etc.; see above and below)*.

The need for classification of digital security research will be examined for each proposal on a case-by-case basis.

3.9 Space research

What?

'**Space research**' covers research activities in the field of space (*e.g. satellite navigation, earth observation, satellite communication, space surveillance and tracking and space exploration*).

These activities may use or generate classified information. They will therefore be assessed during the security scrutiny procedure, mainly on the basis of the GNSS classification guide[7].

[7] *This is a RESTREINT UE/EU RESTRICTED document, which will be made available to the national experts during the security scrutiny (in accordance with the applicable security rules).*