PROGRAMME SECURITY INSTRUCTION
for call for proposals
EDF-2024-DA-EUCI:
Countering hypersonic glide vehicles
under the EUROPEAN DEFENCE FUND

(SHORT TITLE: PSI EDF-2024-DA-EUCI*)*

issued by

European Commission

In accordance with COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015

Version 1.1

Dated

23/04/2024

Participants

[PARTICIPANT MEMBER STATES or NORWAY]

EUROPEAN COMMISSION

Version history

VERSION	REFERENCE	DATE	COMMENTS
1.1	Approved	23/04/2024	

Contents

Section 1 - Introduction

1.1 Scope and purpose

1. This Programme Security Instruction (PSI) establishes the security procedures to be applied and the common security procedures and processes including at the **proposal stage**, to be followed for management of the call for proposal **EDF-2024-DA-EUCI**, established under the European Defence Fund (EDF) and assigns the responsibilities for the protection of Classified Information generated or exchanged in connection with the Action.

2. Given the peculiarity of this Call for proposals, it has been established that the information generated in the implementation of the Programme, including the drafting and the submission of proposals, the evaluation process and the implementation of the grant agreements is classified at the level of **SECRET UE/EU SECRET.** The foreground information generated during the implementation of the projects selected for EU funding, including the project deliverables, will be entirely or partly classified at the same level, under Commission's responsibility (Commission Decision (EU, Euratom) 2015/444 and implementing rules).

3. **All the applicants to this Call for proposals (beneficiaries and affiliated entities), MUST be in possession, before they start drafting their proposal, of a valid Facility Security Clearance (FSC) at the above-mentioned level. The CIS used to handle the drafting and the final version of the proposal MUST be accredited by the competent National Security Authority and the personnel involved MUST be cleared at the level of SECRET UE/EU SECRET. The final version of the proposal MUST be submitted in a properly marked CD-ROM or in hard copy, delivered by certified courier in accordance with the provisions of this PSI.**

4. Consortium coordinators established in Norway, applying for this call must contact DG DEFIS at least 21 calendar days in advance, prior the deadline for submission. This in order to establish the correct exchange procedures of the classified proposals in accordance with the provisions of the Security Agreement between the European Union and the Kingdom of Norway.

5. Subcontractors involved in the call **EDF-2024-DA-EUCI** that "need" to access or generate in their premises documents and materials classified at the level of SECRET UE/EU SECRET, MUST be in possession of appropriate FSC and their CIS MUST be accredited at the appropriate level. The personnel with an established "need-to-know" MUST be cleared at the level of **SECRET UE/EU SECRET.**

6. This PSI provides instructions on:

    a. the classification and marking of Action Information;
    b. protective security procedures, including the handling and transfer of EU Classified Information;
    c. visit procedures to be followed when Classified Information is accessed;
    d. measures to be taken in the event of a Security Breach or Compromise involving EU Classified Information;
    e. procedures to be followed for releasing the EU Classified Information;
    f. and procedures to be followed when awarding a grant or sub-contracting.

7. The protection of COMSEC Items with an EU classification is covered by Annex H. This classified annex will be provided to Beneficiaries by the Granting Authority on a need-to-know-basis.

Section 2 - Glossary

For the purpose of this PSI, the following terminology is used:

ACTION means, in the light of Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092, the project selected under the Programme which the Consortium is to carry out.

ACTION CLASSIFIED INFORMATION is any Classified Information provided to, generated in, or used in the Action regardless of form or type; it includes both Classified Foreground Information and Classified Background Information.

BENEFICIARY is a natural person or an entity with legal personality with whom an EDF grant agreement has been signed.

CLASSIFIED BACKGROUND INFORMATION means any Classified Information necessary for, or useful to the implementation of the EDF, generated before or outside the framework of the Action and provided to and used for the purposes of the Action.

CLASSIFIED FOREGROUND INFORMATION is EU Classified Information generated in the performance of the Action.

CLASSIFIED GRANT is an agreement whereby the European Commission (Commission) awards a grant as referred to in Part I, Title VIII, of Regulation (EU, Euratom) No 2018/1046, the performance of which requires or involves access to, storage or creation of Classified Information.

CLASSIFIED INFORMATION means any information or material designated by a security classification, the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or more of the Participants or of the Union as a whole or any other State or international organisation with which the Participants have concluded a security of information agreement. Its classification level, and therefore the level of protection to be afforded to it by the recipient, is indicated by a classification marking.

CLASSIFIED SUB-CONTRACT is a contract entered into by a Beneficiary with a Sub-Contractor for the supply of movable or immovable assets, execution of works or provision of services, the performance of which requires or involves access to, storage or creation of Classified Information.

COMMISSION SECURITY AUTHORITY is a European Commission authority set up within the Directorate-General Human Resources and Security with responsibilities assigned to it

by the Commission Decision on the security rules for protecting EU classified information in the Commission.

COMMUNICATION and INFORMATION SYSTEM (CIS) is any system enabling the handling of information in electronic form. A CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

COMPROMISE of Classified Information denotes a situation when - due to a security breach or adverse activity (such as espionage, acts of terrorism, sabotage or theft) – Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.

COMSEC (Communication Security) means the application of security measures to telecommunications in any form in order to deny unauthorised persons to access information of value derived from the possession and study of such telecommunications or to ensure the confidentiality, availability, authenticity, nonrepudiation and integrity of such telecommunications. Such measures include crypto, transmission and emission (TEMPEST) security, as well as procedural, physical, personnel, document and computer security.

COMSEC ITEM means all material, including keys in all forms, such as documents, devices or equipment, that describe, contain or relate to cryptographic products and is essential to the encryption, decryption or authentication of telecommunications and any other item that performs critical COMSEC functions.

CONSORTIUM, with reference to Part I, Title VIII of Regulation (EU, Euratom) No 2018/1046, means a collaborative grouping of ***Undertakings*** constituted to carry out an action under this Programme.

COURIER is an appropriately cleared and authorised government employee from a Participant State or staff member of a Participant organisation, or a Beneficiary or Sub-Contractor employee who is appropriately approved by the Security Authorities to hand-carry Classified material to its destination.

DESIGNATED SECURITY AUTHORITY (DSA) is a state authority responsible to the National Security Authority (NSA) of a Participant which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority in that Participant State.

DOCUMENT means any recorded information regardless of its physical form or characteristics.

ELECTRONIC TRANSMISSION means the sending of Action Information from one place to another by electronic means.

EU 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.

EU COMSEC INSTRUCTIONS is the document that establishes the security instructions and assigns the responsibilities for the implementation of security policy concerning EU Classified COMSEC Items generated and exchanged under the Action. This document also provides common security procedures for the marking, handling, storage, destruction and electronic transmission of COMSEC and CRYPTO Items. The COMSEC Instructions are at Annex G to this PSI.

FACILITY SECURITY CLEARANCE (FSC) means an administrative determination by an NSA, DSA or competent Security Authority that a facility can afford an adequate level of protection to Classified Information to a specified security classification level.

GOVERNMENT-TO-GOVERNMENT CHANNELS are transfers of Classified Information via diplomatic pouch or through other channels approved by the Security Authorities involved.

GRANTING AUTHORITY is the Commission department responsible for the implementation of the budget of the Programme.

NATIONAL SECURITY AUTHORITY (NSA) is a Government authority with ultimate responsibility for the security of Classified Information in that country.

NEED-TO-KNOW is the principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to accomplish a designated and approved function relating to the Action.

ORIGINATOR of Classified Background Information means a State or an international organisation under whose authority Classified Information has been created and/or introduced into the EDF.

ORIGINATOR of Classified Foreground Information is the European Commission. *(Whilst Beneficiaries or Sub-Contractors can create EU Classified Information for the Action, they are not considered Originators for the purposes of this PSI).*

PARTICIPANTS are the European Commission , EU Member States or Norway that are listed in this PSI, which are responsible for co-ordinating the implementation of this PSI. In the meaning of this definition, Beneficiaries and Sub-Contractors are not considered Participants.

PERSONNEL SECURITY CLEARANCE (PSC) means a statement by a competent authority of a Participant State made following completion of a security investigation conducted by a competent authority of a Participant State and which certifies that an individual is cleared to have access to Classified Information up to the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above or of an equivalent national level until a specific date.

PROPOSAL STAGE means the period from the publication of a call for proposals to the signature of a grant agreement.

PSI CUSTODIAN is appointed by the European Commission and is responsible for the control of this PSI, including annexes, and for ensuring the correct issuing and version control.

RELEASE is the passing of Action Information, by any means of communication, to the State or international organisation that is not a Participant to the Action.

SECURED AREA is a physically protected area with a visibly defined and protected perimeter through which all entry and exit is controlled by means of a pass or personal recognition system, where unescorted access is granted only to individuals who are security cleared and are specifically authorised to enter the area on the basis of their need-to-know, and where all other individuals are escorted at all times or are subject to equivalent controls.

SECURITY ASPECTS LETTER (SAL) is a set of special contractual conditions, issued by the granting authority, which forms an integral part of a classified contract, classified grant agreement or classified sub-contract involving access to or generation of Classified Information, that identifies the security requirements or those elements of the contract, grant agreement or sub-contract that require security protection.

SECURITY AUTHORITY is the NSA or DSA or other authority responsible for the maintenance of standards for the security of Classified Information within a State or an international organisation.

SECURITY BREACH occurs as result of an act or omission which is contrary to the security provisions set out in this PSI or in any other applicable laws, rules or regulations.

SECURITY CLASSIFICATION GUIDE (SCG) is a document which describes the elements of a programme, project, contract, grant agreement or sub-contract which are classified, specifying the applicable security classification levels. The SCG issued to Beneficiaries or

Sub-Contractors may be modified throughout the life of the programme, grant agreement or sub-contract, and the classified elements may be re-classified or downgraded**.**

SECURITY OFFICER is a person, having the appropriate security expertise, designated by the management to be responsible for the proper implementation of security-related decisions and for the co-ordination of available security resources and measures within a facility involved in the classified parts of the Action, as well as to be the technical advisor to management on security matters related to the Action.

SUB-CONTRACTOR is legal entity awarded a sub-contract under the Action.

Section 3 - PSI applicability and the security responsibilities of Participants

3.1 Applicability

1. This PSI applies to any Beneficiary or Sub-Contractor that will access or create Classified Information under the preparation stage and implementation of **call EDF-2024-DA-EUCI.** The latest approved version of this PSI and its annexes will be referenced to in the Security Aspects Letter of a grant agreement or sub-contract, and as such, is applicable to Beneficiaries or Sub-Contractors on a contractual basis.

2. The provisions of this PSI do not put any legal obligations either on the Security Authorities of the Participant States.

3. Questions concerning the content and interpretation of this PSI, and any proposed changes, shall be addressed to the Commission Security Authority, which will consult with the Granting Authority and the Participants' Security Authorities, if required.

4. The text of this PSI and its further amendments will be submitted to Commission Security Expert Group for advice.

3.2 Responsibilities

3.2.1 Security Authorities

1. In accordance with national rules, the Security Authorities of Beneficiaries or Sub-Contractors under their jurisdiction are responsible for:

    g. Monitoring the implementation of the provisions of this PSI within their establishments, and by Beneficiaries or Sub-Contractors under their jurisdiction;

    h. Conducting the Facility Security Clearance (FSC) process for Beneficiaries or Sub-Contractors that are required to handle and/or store Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above at their facility;

    i. Upon request, and where Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above is involved, responding to FSC Information Sheet (FIS) requests from another Security Authority or Granting Authority;

    j. Conducting the Personnel Security Clearance (PSC) process on the personnel handling Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above.

2. The Security Authorities of all Participants are responsible for:

    a. Upon request, and where Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above is involved, responding to PSC Information Sheet (PSCIS) queries submitted by another Security Authority;

    b. Submitting and/or approving Transportation Plans, Courier Certificates, international visit requests (i.e. request for visit), etc. in accordance with the provisions of this PSI;

c. Informing the Originator's competent Security Authority and, where EU Classified Information is concerned, the Commission Security Authority, identified in Annex A, about any security breach, which may have led to a loss or Compromise of Classified Information;

d. Investigating all cases in which it is known, or where there are grounds for suspecting a Compromise of Classified Information provided or generated pursuant to the Action has occurred;

e. Ensuring, in liaison with the PSI custodian, that their details in Annex A are up to date;

f. Reviewing and updating this PSI, upon request from the Commission in accordance with Commission Decision (EU, Euratom) 2015/444.

3.2.2 Granting Authorities

1. The Granting Authority for the EDF shall notify, through the Commission Security Authority, the relevant Security Authority of the Beneficiary or Sub-Contractor of any classified grant or sub-contract awarded together with its end-date, the level of classified information to be used, and whether and at what level a capability to store and/or handle EUCI on a CIS is necessary. The Granting Authority shall also provide a copy of the relevant parts of the classified grant or sub-contract (e.g. the Security Aspects Letter) to the Security Authority of the Participant in order to facilitate their security monitoring of the grant or sub-contract.

2. The Commission shall distribute the latest issue of this PSI to their Beneficiaries and the NSAs/DSAs involved.

3. The Granting Authority is responsible for providing, through the Commission Security Authority, to the NSAs/DSAs involved the updated details of their Beneficiaries or of the Sub-Contractors under sub-contracts with their Beneficiaries.

3.2.3 Beneficiaries or Sub-Contractors

1. Beneficiaries or Sub-Contractors are responsible for the implementation of this PSI within their facilities, in particular for ensuring that:

   a. The provisions of the latest version of this PSI are implemented;

   b. Classified Information and COMSEC Items generated by the Beneficiary or Sub-Contractor, or entrusted to them, are appropriately safeguarded;

   c. A Security Officer is appointed who is responsible for supervising and directing security measures in relation to the Action. This individual shall be responsible for limiting access to Classified Information involved in the classified grant or sub-contract to those employees who have been briefed, authorised for access, have a Need-to-Know and (for access to Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above) have been granted a PSC at the appropriate level;

   d. Any Classified Foreground Information generated by the Beneficiary or Sub-Contractor is classified in accordance with this PSI and the relevant Security Classification Guide (SCG);

e. The security classifications of Classified Background Information are retained and not changed without the prior written consent of the Originator;

f. Classified Information is only provided to individuals who have a Need-to-Know and an appropriate PSC, if required;

g. Classified Information (at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) is provided only to Beneficiary or Sub-Contractor facilities that have been granted an FSC. Prior to providing Classified Action Information to another Beneficiary or Sub-Contractor, the FSC status of that Beneficiary or Sub-Contractor shall be established;

h. Classified Information is not released to Third Parties to the Action without the appropriate release procedures of this PSI having been followed;

i. Classified Foreground Information is not used for purposes other than the Action, unless the prior written consent of the Originator has been obtained through their Granting Authority;

j. The relevant security provisions of this PSI, as referred to in the Security Aspects Letter, or parts thereof, are included as part of any contractual arrangement with Sub-Contractors;

k. Appropriate action is taken in the event of any actual or suspected Security Breach, Compromise or loss involving Classified Information; and

l. Their Security Authority is informed about any suspected or actual Security Compromises or losses of Classified Information as soon as is possible.

m. The latest version of this PSI is forwarded to their Sub-Contractors.

Section 4 - Security instructions

4.1 Handling and protection of Action related Classified Information

1. EU Classified Information, both Foreground and Background, that is provided to or generated by Beneficiaries or Sub-Contractors in connection with the proposal stage and the implentation of call EDF-2024-DA-EUCI shall be handled and protected in accordance with Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information and the Commission Decision (EU, Euratom) 2021/259 laying down implementing rules on industrial security with regard to classified grants, taking into account the supplementary provisions set out in this PSI.

2. Classified Background Information with a national classification marking or a classification marking of international organisation provided to or exchanged among Beneficiaries or Sub-Contractors in connection with the Action shall be handled and protected in accordance, respectively, with their applicable national laws and regulations or with the rules and regulations applicable to the international organisation under whose authority the classified information has been generated, in accordance with existing security agreements or arrangements. Annex B provides for a table of equivalent security classification markings, for reference.

3. Classified Information shall be upgraded, downgraded or declassified only with the consent of the Originator.

4. For compilations of information (i.e. aggregation) a higher level of classification may be required. Classification on this basis shall be clearly documented by the Originator of the Classified Information.

5. Equipment and system components or parts thereof revealing Classified Information (e.g. during assembly or testing works) shall be handled and protected in accordance with the Classification level of the information revealed.

4.2 Marking of Classified Foreground Information generated by Participants

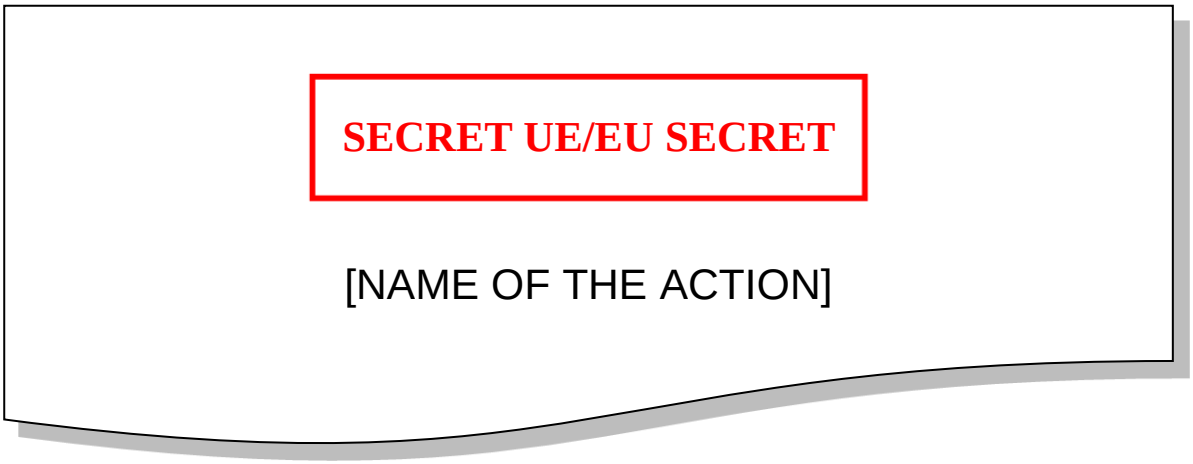
4.2.1 Security classification markings

1. Classified Foreground Information shall be classified in accordance with the Security Aspects Letter. For grants or sub-contracts, the relevant parts of the SCG shall be extracted or specific classification guidance shall be given by the Granting entity in the respective SAL to the Grant Agreement or Sub-Contract.

2. Such Classified Foreground Information shall be marked with the appropriate EU classification marking: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET. For documents the EU classification marking will be applied on the top and bottom of each page, centred, and in capital letters.

3. A statement will be added underneath the classification marking, at latter's every occurrence, identifying that the EU Classified Foreground Information is relating to a given Action under EDF. This indicates that this information can be shared with the Participants, Beneficiaries and Sub-Contractors to the Action only, and that the information must not be used for purposes other than those of the given Action.

Example:



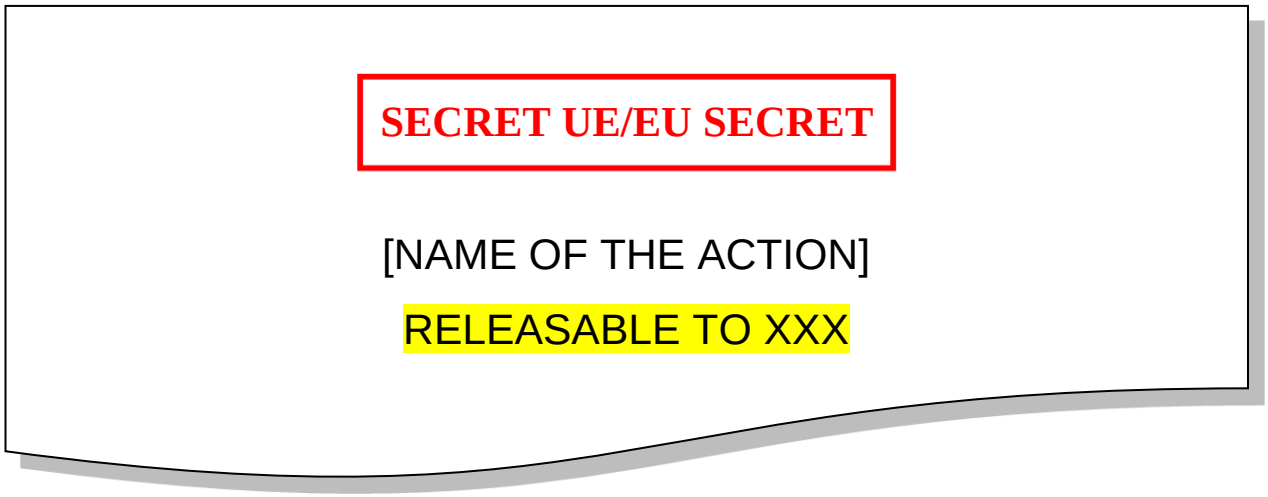
4. For Classified Foreground Information not in the form of documents (e.g. electronic files and physical equipment/material), the EU classification marking shall be applied in such a way as to clearly identify the level of classification.

4.2.2 Declassification and downgrading markings

1. If Classified Foreground Information needs to maintain its classification only for a defined period, it may be downgraded/declassified at that point by or on behalf of the Originator.

4.2.3 Releasability markings

1. Where the Originator has agreed to release Classified Information to the State or international organisation that is not a Participant to the Action or to another EU Action or Programme, a releasability statement, in compliance, if necessary, with the EU-Third Party Security of Information Agreement, shall be added underneath the classification marking, at latter's every occurrence, as shown in this example:

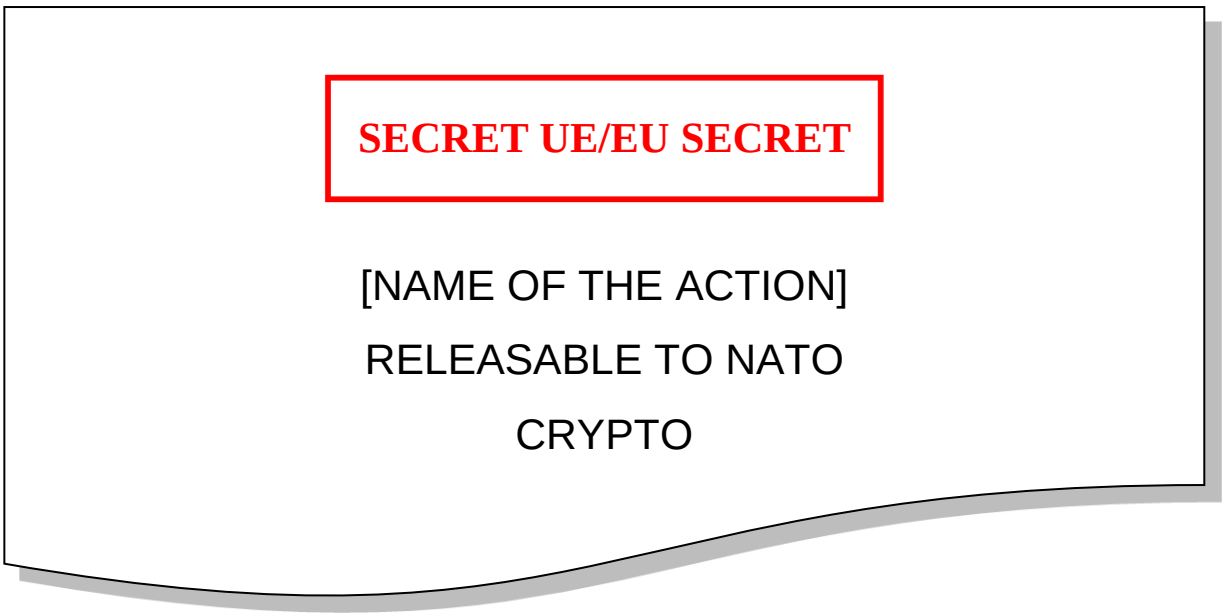


4.2.4 Crypto and CCI markings

1. In addition to EDF Action identifier markings or to releasability markings, it is allowed to add the special category designators 'CRYPTO' or 'CCI'. These identify that Classified Information is,

respectively, a cryptographic item or controlled cryptographic item. These designators should be added at every occurrence of the EU security classification marking.

Example:



4.3 Security Classification Guide (SCG)

1. The SCG provides guidance on the items requiring a security classification as Classified Foreground Information generated in the course of the Action. The SCG may also identify items requiring no classification or requiring their identification as relating to a special category (e.g. crypto or CCI).

2. It will be prepared in close coordination with experts of Participant States in the projects and will form an annex to the Security Aspects Letter (SAL), which will be integral part of the classified grant agreement or classified sub-contract.

3. The classification levels assigned in the SCG are those anticipated for each item of listed information or equipment. Changes or questions concerning the interpretation of the SCG shall be addressed to the Commission, who may consult with the Participants' Security Authorities.

4.4 Specific procedures for the protection of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET Classified Information

4.4.1 Access

1. Access to and handling of Classified Information at these levels for the purposes of the Action shall be limited to individuals having the appropriate level of PSC and a Need-to-Know.

2. When individuals are first granted access to Classified Information at these levels generated under the Action they must have been briefed by their Security Officer on the security requirements in this PSI. They shall acknowledge their responsibilities for protecting this information in writing, and a record of this acknowledgement shall be retained by the Security

Officer. Individuals required to access to Classified Information at these levels shall be briefed at regular intervals by their Security Officer.

3. Security debriefings shall be given to personnel when they no longer require access to Classified Information at these levels. The debriefing shall consist of a reminder of the continuing responsibility to protect the Classified Information and the possible penalties for failure to do so. Debriefing certificates may be used to record the debriefings and shall be retained by Security Officers.

4.4.2 Handling and storage

1. Classified Information at these levels shall only be handled and stored in Participants' establishments if they are authorised to handle and store that level of Classified Information in accordance with the applicable laws, rules or regulations of the Participant, and in the facilities of Beneficiaries or Sub-Contractors that have been granted an appropriate FSC or other appropriate approval to handle and store classified information up to such level.

2. When created or received, documents or material classified at these levels shall be registered for purposes of accountability in dedicated registry or logbooks. For such purposes a classified registry shall be established which shall be responsible for recording the life cycle of the Classified Information at these levels at the facility, including its dissemination and destruction. Registering of classified documents or material by electronic means shall be subject to the prior approval of the Security Authority.

3. Classified Information at these levels shall only be worked on in a Secured Area approved in accordance with the applicable laws, rules and regulations of the Participant in a manner that prevents unauthorised access to the information, shall not be discussed or worked on in public (e.g. on public transport) and shall not be left unattended or handled in a manner that could result in unauthorised access.

4. Secured Areas that have been designated as 'Technically Secured Areas' by Security Authorities shall be equipped with Intruder Detection Systems (IDS), be locked when not occupied and be guarded when occupied. Any keys shall be controlled, all persons and material entering such areas shall be controlled. Such areas shall be regularly physically and/or technically inspected as required by the competent Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry. Technically secured areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

5. When not in use, documents or other small items classified at these levels shall be stored in a secured container approved in accordance with the applicable laws, rules or regulations of the Participant. If the material is of such a size or format that it cannot be stored in a secured container, advice shall be sought from the relevant Security Authority as to how it should be protected.

6. The physical reproduction of Classified Information at these levels shall be limited to the minimum necessary to fulfil a particular action or function. Copies shall be made in a Secured Area using equipment approved in accordance with the applicable laws, rules or regulations of the Participant. The security measures applicable to the original document shall also apply to any copies made. Copies shall be managed appropriately and securely destroyed when no longer required.

7. Translations of Classified Information at these levels shall only be undertaken by personnel holding an appropriate level of PSC. If a translation is created it shall be marked as the original,

be afforded the same level of protection as the original, and be securely destroyed when no longer required.

8. When no longer required by the holder, Classified Information at these levels shall be destroyed in such a manner to ensure that it cannot be reconstructed. The destruction shall be by a method that is in accordance with the applicable laws, rules or regulations of the Participant. Such destruction shall be carried out by an individual, and witnessed by another individual, both holding a PSC of an appropriate level. A destruction certificate shall be created and shall be recorded and filed in the registry/logbook. Destruction certificates are to be retained for five years by the establishment or facility where the destruction took place.

4.4.3 Information Assurance

1. Classified Information at these levels shall be processed and stored electronically in CIS which have been appropriately accredited for the level of classification to be handled. The accreditation to be applied shall be in accordance with the applicable laws, rules or regulations of the Participant.

2. Classified Information at these levels may be stored on removable or portable data storage media or devices. It shall be handled and protected to the same standards as documents containing the same level of classified information, if not encrypted with an approved encryption. Sub-section 4.7.4 provides further information on the procedures and considerations that apply for removable storage media.

3. CIS used within facilities located on the territory of one Member State and handling Action-related Classified Information will be accredited by the relevant Security Authority or competent Security Accreditation Authority (SAA), as appropriate, in accordance with the applicable laws, rules or regulations of the hosting Participant.

4. For security accreditation of such CIS handling EDF-related Classified Information, whose components are under different jurisdictional domains (e.g. different SAAs), all concerned SAAs shall take part in the security accreditation process. In such case the system-specific information assurance requirements and the accreditation process will be identified in dedicated security requirements documentation, which will be jointly approved by the SAAs involved.

5. Accredited portable computing devices not using approved encryption shall only be used or stored in an accredited Secured Area.

6. EUCI at this level that is transmitted electronically shall be protected by cryptographic products approved by the Council.

7. Interconnection of Beneficiary or Sub-Contractor's CIS handling Action related Classified Information to other Participants' CIS will be jointly accredited by the respective Security Accreditation Authorities (SAAs). Appropriate security arrangements should be in place to ensure that the SAAs and the different CIS providers of the interconnected CIS are bound by relevant security requirements on the protection of Action-related Classified Information handled or exchanged via such CIS.

8. Areas in which CIS are installed or operated to display, store, process or transmit Action related Classified Information will be established as Secure Areas. CIS areas housing servers, network management systems, network or communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to specifically authorised persons.

4.4.4 Tempest

1. Facilities that house CIS handling Classified Information at these levels shall be assessed by their Security Authority on the threat of Compromise by unintentional electromagnetic emanations. TEMPEST security measures shall be commensurate with the risk of exploitation and the level of classification of information.

4.5 Specific procedures for the protection of RESTREINT UE/EU RESTRICTED Classified Information

4.5.1 Access

1. Access to Classified Information at this level shall be limited to individuals who have an established Need-to-Know for the purposes of the Action.

2. When individuals are first granted access to Classified Information of RESTREINT UE/EU RESTRICTED level generated under the Action they must have been briefed by their Security Officer on the security requirements in this PSI. They shall acknowledge their responsibilities for protecting this information in writing, and a record of this acknowledgement shall be retained by the Security Officer.

3. In principle, PSCs are not required for access to Classified Information at this level. Where Participant States require a PSC for grant agreements or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, those national requirements shall not place any additional obligations on other Participant States or exclude applicants, Beneficiaries or Sub-Contractors from Participants that have no such PSC requirements for access to RESTREINT UE/EU RESTRICTED information from related grant agreements or subcontracts.

4.5.2 Handling and storage

1. In principle, FSCs are not required for Beneficiaries or Sub-Contractors handling and storing Classified Information at this level at their facility. Where Participant States require an FSC for grant agreements or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, those national requirements shall not place any additional obligations on other Participant States or require an FSC from a Beneficiary or Sub-Contractor of another Participant that does not require an FSC at that level according to its applicable laws, rules or regulations.

2. There is no requirement to register Classified Information at this level in the dedicated classified registry or logbooks unless required by a Participant State's applicable laws, rules or regulations.

3. Classified Information at this level shall not be discussed or worked on in public (e.g. on public transport).

4. Classified Information at this level shall not be left unattended or handled in a manner that could result in unauthorised access. As a general rule, when not in use, such information should be stored in locked desks, cabinets, or similar containers to which access is limited to persons having the required Need-to-Know. Classified Information at this level may also be stored in the open in locked rooms, provided access to the room is restricted to persons who have a Need-to-Know.

5. The physical reproduction of Classified Information at this level shall be limited to the minimum necessary to fulfil a particular action or function. Copies shall be managed appropriately by the facility and securely destroyed when no longer required.

6. Translations of Classified Information at this level shall be marked as the original, be afforded the same level of protection as the original, and be securely destroyed when no longer required.

7. When no longer required by the holder, Classified Information at this level shall be destroyed in such a manner that ensures it cannot be reconstructed. The destruction shall be by a method that is in accordance with the applicable laws, rules or regulations of the Participant.

4.5.3 Information Assurance

1. Classified Information at this level shall be processed and stored in CIS which have been accredited for this level of classification by the appropriate Security Authority.

2. The security accreditation of CIS handling Classified Information at this level and of any interconnection thereof may be delegated to the Security Officer of a Beneficiary or Sub-Contractor if this is permitted by national laws, rules or regulations. Where that task is delegated, the Beneficiary or Sub-Contractor shall be responsible for implementing the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant Security Authorities or SAAs retain the responsibility for the protection of Classified Information at this level handled by the Beneficiary or Sub-Contractor and the right to inspect the security measures taken by the Beneficiary or Sub-Contractor. In addition, the Beneficiary or Sub-Contractor shall provide to the Granting Authority and, where required, to its NSA/DSA a statement of compliance certifying that the CIS handling Classified Information at this level have been accredited. The accreditation to be applied shall be in accordance with the applicable laws, rules or regulations of the Participant. Minimum requirements for Beneficiary or Sub-Contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level are described in Annex D.

3. Classified Information at this level that is transmitted shall be protected by cryptographic products approved by the EU or the relevant Security Authority. For interconnected systems this needs to be approved by the relevant Security Authorities (or SAAs).

4. Portable computing devices not using approved encryption shall only be used or stored in areas with appropriate access control. Data storage media and computing devices containing Classified Information at this level, which are not encrypted with an approved encryption system shall not be carried outside premises unless they can be held under personal custody.

5. Classified Information at this level may be stored on removable data storage media or devices. Section 4.7.4 provides further information on the procedures and considerations that apply.

4.6 Access to Classified Information at meetings

1. Access to Classified Information at meetings, which include conferences, symposia and seminars, shall be subject to the provisions of this PSI.

4.7 Procedures for sending Classified Information

1. For the purposes of this document the following terminology is used to denote the 'sending' of Classified Information:

    a. **Transport:** for the physical movement of Classified Information (e.g. by hand carriage, postal service, commercial courier, transport by road, rail, air or sea).

    b. **Electronic Transmission:** for the electronic transfer of Classified Information (e.g. via email).

2. For the purposes of this PSI, electronic transmission does not include the transport of removable storage media and devices. This aspect is addressed in Section 4.7.4.

4.7.1 Transport within a single Participant State

1. The transport of Programme Classified Information within the territory of a Participant State will be in accordance with the applicable laws, rules or regulations.

4.7.2 Procedures for sending CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET Classified Information between the Participants, Beneficiaries and/or Sub-Contractors

1. As a general principle, the preferred means for sensing Classified Information at these levels under the Action is electronic transmission using approved encryption methods or products.

2. The following means are permitted for sending CONFIDENTIEL UE/EU CONFIDENTIAL Classified information:

    a. Electronic transmission using approved encryption systems, cryptographic products or methods;

    b. Government-to-Government Channels;

    c. Hand carriage by authorised personnel holding the appropriate level of PSC;

    d. Approved transport by road, rail, ship or air by security cleared transport companies or escorting personnel;

    e. Carriage by non-security cleared approved postal services or commercial courier companies, in accordance with national laws and regulations.

3. The following means are permitted for sending of SECRET UE/EU SECRET Classified Information:

    a. Electronic transmission using approved cryptographic products or methods;

    b. Government-to-Government Channels;

    c. Hand carriage by authorised personnel holding the appropriate level of PSC; or

    d. Approved transport by road, rail, ship or air by security cleared transport companies or escorting personnel.

4. Entities will transport Classified Information on the condition that the sender first obtains confirmation from its relevant Security Authority that the receiving site holds a valid FSC at the appropriate level or has been approved otherwise for handling of classified information up to the appropriate classification level, and that the entity is entitled to receive Action-related Classified Information at that level.

International electronic transmission

5. Electronic transmission of Classified Information at these levels between Participants shall be protected by cryptographic methods or products approved by the EU.

Government-to-Government channels

6. Government-to-Government Channels (e.g. diplomatic bag services) to be used for the transport of Classified Information at these levels shall be in compliance with the regulations of the sending Participant. (Note: this is not to be confused with the hand carriage of Classified Information, which is covered in the next sub-section.)

Hand carriage

7. Classified Information at these levels may be hand carried by an individual holding the appropriate level of PSC.

8. An individual hand carrying the Classified Information shall be briefed on his/her responsibilities by the Security Officer before the carriage occurs.

9. An individual hand carrying the Classified Information from one Participant State to another will be issued with a Courier Certificate, a template of which is provided in Annex D, or the national equivalent. Senders can use this template in that Annex or an equivalent national document approved by their Security Authority. The individual hand-carrying the information shall carry the Courier certificate during the carriage, and be able to present this upon arrival at the receiving facility.

10. During the hand carriage the consignment shall remain in the personal custody of the individual or be appropriately secured as described in this PSI. It shall not be left unattended and shall not be opened en route.

International carriage by approved postal services or commercial courier services

11. SECRET UE/EU SECRET Classified Information shall not be sent internationally by postal service or commercial courier service.

12. The sending of Classified Information by approved postal services or commercial courier services is only permitted for consignments up to and including the classification level CONFIDENTIEL UE/EU CONFIDENTIAL, provided such means of exchange are permitted by the applicable laws, rules or regulations of the sending Participant.

13. For consignments up to and including the classification level CONFIDENTIEL UE/EU CONFIDENTIAL, postal services or commercial courier services shall only be used if the following criteria have been met:

    a. The Security Authority of the sender permits the use of postal services or commercial courier services according to its applicable laws, rules or regulations;

b. The Security Authority of the sender may, according to its applicable laws, rules or regulations, require the postal service or commercial courier service to hold an FSC;

c. The postal service or commercial courier service to be used is located within the Participant State's territory, has a security programme for handling valuable items, including a signature service, a continuous record of accountability on custody and a tally record or electronic track and trace system;

d. The postal service or commercial courier service to be used shall ensure that the consignment is delivered to the recipient prior to a specified time and date within a 24-hour period under regular circumstances, or within a clearly defined time frame for consignments over distances that cannot reasonably be covered within a 24 hour period; and

e. The postal service or commercial courier service shall provide to the sender proof of receipt and delivery of the consignment.

14. When CONFIDENTIEL UE/EU CONFIDENTIAL Classified Information is sent by postal service or approved commercial courier service the consignment shall be prepared and packaged as follows:

    a. The consignment shall be sent using double envelopes (the inner envelope being a tamper-evident envelope) or other suitably secure packing material;

    b. The classification level shall be clearly visible on the inner envelope/package;

    c. The classification shall not be indicated on the outer envelope/package;

    d. Both the inner and outer envelope/package shall usually be addressed to the recipient's classified registry or the Security Officer, as indicated on the FSC confirmation, and shall include a return address;

    e. A registration receipt form shall be placed inside the inner envelope/packaging for the recipient to complete and return. The registration receipt, which itself shall not be classified, shall quote the reference number, date and copy number of the document, but not the subject;

    f. Delivery receipts are required in the outer envelope/packaging. The delivery receipt, which itself shall not be classified, should quote the reference number, date and copy number of the document, but not the subject; and

    g. The courier service must first obtain and provide the consignor with proof of delivery of the consignment on the signature and tally record, or the courier must obtain receipts/package numbers.

15. The sender shall liaise with the named recipient before the consignment is sent to agree a suitable date/time for delivery.

16. The sender is solely responsible for the consignment that is sent by postal service or commercial courier service. In the event that the consignment is lost or not delivered on time, the sender shall follow up with the postal service or commercial courier service to ascertain the circumstances of the security incident, and inform its NSA/DSA and the Granting Authority.

Transport by freight – general requirements

17. Classified Information at these levels which is of such size or shape that it cannot be transported by one of the methods listed above, or large volumes of Classified Information, may be transported as freight by a commercial transport company. (Note: this is not to be confused with a commercial courier service as covered in the previous sub-section.)

18. The transport company shall hold an FSC at the appropriate level and/or shall be capable of deploying security cleared couriers or escorts for the transport, if permitted under the sender's applicable laws, rules or regulations.

19. Where Classified Information at these levels requires overnight storage at the transport company's facilities, an FSC with storage capabilities shall be required. Senders shall check with their Security Authority before selecting a commercial transport company whether an FSC will be required for the transport.

20. The sender shall prepare a Transportation Plan using Annex E (or an equivalent national document approved by their Security Authority). When the sender has completed the Plan, it shall submit it to its Security Authority for consideration. Once reviewed, the sender's Security Authority will submit the Transportation Plan to the Security Authority of the recipient for its consideration. Transport by freight cannot take place until both the sending and recipient Security Authorities have agreed the Transportation Plan.

21. The degree of protection and measures required for the transport shall be determined by the highest classification level of the contents of the consignment.

22. Containers used for the transport shall not bear any visible indication that they contain Classified Information. These containers shall be sealed with seals/locks in such a way that any tampering will be evident. Any evidence of tampering shall be considered a Security Breach and be reported as soon as possible.

23. Journeys will be point-to-point to the extent possible, and will be completed with the shortest possible delays and stops. Appropriate security measures shall be in place at all stages during the transport.

24. If possible, routes to be used for road and rail will be limited to the territory of Participant States. If not possible, routes through non-Participant States will be planned in close cooperation with the Security Authorities of the sender and recipient.

Security escorts or security guards

25. Any security escort/guard team shall be composed of an adequate number of personnel to ensure regular tours of duty and rest. Their number shall depend on the highest classification level of the consignment, the method of transport to be used, the estimated time in transit and at designated stops, and the quantity and level of the Classified Information to be protected.

26. It is the responsibility of the sender and, where applicable, the recipient to instruct security escorts and security guards on how the consignment shall be protected.

Transport by road

27. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC, who may be the driver, co-driver or another individual escorting the transport. One of these individuals shall be issued with and carry a Courier Certificate, as shown in Annex D, or

the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect Classified Information.

28. Classified Information shall be secured in containers by a lock or padlock, or in a closed or locked vehicle. If this is not possible because of the size or nature of the contents, the consignment shall be suitably sealed using a tamper-evident method to protect the classified aspects.

29. Where stops are required during transport, attempts should be made by the sender to arrange for stops to be at suitably cleared government establishments or Beneficiary's or Sub-Contractor's facilities holding an FSC. In the event such arrangements cannot be made, or an emergency situation arises due to accident or breakdown of the vehicle, at least one of the individuals with a PSC accompanying the consignment shall be responsible for monitoring and keeping it under constant control.

30. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding an appropriate level of PSC.

31. Where appropriate and permissible, the sending and receiving Security Authorities, plus any Participant States the transport will pass through, shall advise their customs or other relevant authorities of impending consignments.

Transport by rail

32. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC. One of these individuals shall be issued with and carry a Courier Certificate, as shown in Annex D, or the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect Classified Information.

33. Passenger accommodation shall be made available for security escorts and/or security guards. During stops the security escorts and/or guards shall remain with the consignment.

34. Where possible, loading and unloading of the consignment shall be under the security control of at least one individual holding the appropriate level of PSC.

35. Deliveries and collection shall be so timed as to prevent, to the extent possible, a consignment being held in warehouses without an appropriate level of FSC.

Transport by sea

36. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC. One of these individuals shall be issued with and carry a Courier Certificate, as shown in Annex D, or the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect Classified Information.

37. Preference shall be given to using ships that sail under the flag of a Participant State.

38. The consignment shall be stowed in locked stowage space approved by the Security Authority of the sender. Where practicable, at least one security escort or security guard holding an appropriate PSC shall accompany the consignment.

39. Except in case of emergency, stops at a port of a non-Participant State are not permitted unless the prior approval of the sender's Security Authority has been obtained. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding the appropriate level of PSC.

40. Deliveries to the port of embarkation and collection from the port of disembarkation shall be timed to prevent, as far as possible, a consignment being held in port warehouses, unless the warehouse has an appropriate level of FSC.

Transport by air as freight

41. Unless there are clear reasons why this is not possible, the consignment shall be accompanied by at least two individuals with the appropriate level of PSC. If this requirement cannot be met the sender should consult its Security Authority to seek its approval. One of these individuals shall be issued with and carry a Courier Certificate, as shown in Annex D, or the national equivalent. Before the transport occurs, these individuals shall be briefed on their responsibilities to protect Classified Information.

42. Where possible, the consignment will be delivered straight to the aircraft rather than being stored in warehouses at airports or airfields (unless a warehouse has an approved storage capability for classified items at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above). A sufficient number of security escorts and/or security guards shall be provided to keep the consignment under adequate supervision.

43. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding the appropriate level of PSC.

44. Direct flights will be used whenever possible.

45. Intermediate routine stops of short duration may be permitted, provided the consignment remains in the aircraft. If the cargo compartment is to be opened at a stop, every effort shall be made to ensure that a security escort or security guard accompanying the consignment is present.

46. In the event that the aircraft is delayed at an intermediate stop for a significant period of time or is forced to make an unscheduled or emergency landing, the individual holding the courier certificate will take all reasonable measures possible for the protection of the consignment. That individual shall inform his/her Security Authority of the delay as soon as possible. If necessary, that individual will seek the assistance of his/her Diplomatic mission in the country concerned.

47. At its final destination, every effort will be made for the aircraft to be met on landing and the consignment to be placed under the security control of at least one individual holding an appropriate level of PSC.

4.7.3 Procedures for sending RESTREINT UE/EU RESTRICTED Classified Information

1. As a general principle the preferred means for sending Classified Information at this level under the Action is by electronic transmission. Such transmission shall be protected by approved cryptographic methods or products.

2. When electronic transmission is not possible, the following physical means are permitted for transporting Classified Information at this level without additional requirements, unless required by the sender's Security Authority:

    a. Hand carriage;

b. Transport by postal services or commercial courier services;

c. Government-to-Government channels;

d. By freight.

3. The transport shall be in accordance with the sender's applicable laws, rules or regulations. The envelope or wrapping shall not reveal the classification level of the information contained.

4.7.4 Procedures for transporting Classified Information using removable storage media

1. The use of removable storage media to transfer Classified Information in the Action is generally encouraged over sending physical documents for both cost and practical reasons, but using removable storage media also carries additional risks that must be mitigated by the sender. The compromise of removable storage media containing a number of classified documents will usually be more damaging than the compromise of a consignment of physical documents given the volume of information which can be stored on such media.

2. When considering using removable storage media, only the necessary classified documents to perform a particular task/activity should be stored on the media. It is not permitted to store classified documents that are not relevant or no longer associated with a task/activity. Sender should bear in mind that large amounts of Classified Information stored on such devices may warrant a higher classification level.

3. Personal USB sticks and those given freely at conferences, seminars, etc. are not to be used for storing or transferring Classified Information.

4. Removable storage media containing Classified Information are required to be labelled with the appropriate classification marking. Measures shall be in place to prevent unauthorised access to such storage media and to maintain the Need-to-Know principle.

5. If CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET Classified Information is stored on removable storage media it must be logged and registered as stipulated by this PSI.

6. The use of removable storage media in a facility must be strictly controlled and accounted for.

7. Only CIS that has been appropriately accredited and/or approved shall be used to transfer Classified Information from the removable storage media.

8. When transporting Classified Information on removable storage media particular care should be taken to ensure that the media does not contain malware prior to the transfer of the data onto the media.

9. All CIS used for processing EUCI shall use appropriate system configuration to preserve integrity, functionality and to enforce access control. For example, AutoRun and AutoPlay (or similar functions) shall be disabled on all CIS to prevent unauthorised applications or malware from running automatically from removable media. In the event that an application attempts to run automatically from removable media, the user must cancel it and take steps to ensure that it does not run again.

10. Unless the removable storage media is encrypted with an EU approved cryptographic product for that level of classification it must be prepared, packaged and transported in exactly the same manner as Classified Information in physical form. If suitably encrypted, the removable

storage media shall be handled in accordance with security operating procedures pertinent to the encryption system used.

11. Removable storage media that is used to transport Classified Information shall be accompanied by a dispatch note, detailing the removable storage media containing the Classified Information, as well as all files contained on it, to allow the recipient to make the necessary verifications and to confirm receipt.

12. As a general rule, documents on the removable storage media that are either no longer required, or have been transferred onto an appropriate CIS are to be securely removed or deleted using approved products or methods. Unless stored in an appropriate security cabinet or facility, CDs/DVDs without rewriting capability should be destroyed when no longer needed. Any destruction/deletion shall be by use of a method that is in accordance with the applicable laws, rules or regulations of the Participant holding the removable storage media.

Section 5 - Release of Classified Information

1. The release of Classified Foreground Information to entities other than to Participants to the Action and their Beneficiaries or Sub-Contractors is not permitted without the specific written approval of the Commission, as Originator. This decision has to be taken after consultation with Member States whose national Classified Background Information has been used for generating Classified Foreground Information.

2. Requests for release of Classified Foreground Information will be submitted through the Granting Authority to the competent European Commission officer representing the Originator (as identified in Annex A2) for approval. Any such requests by Beneficiaries or Sub-Contractors shall be made through the contractual chain.

3. If Classified Background Information is being considered for release, the prior written approval of the Originator is required before such information is released.

Section 6 - International Visits among Participants, Beneficiaries and Sub-Contractors

1. Each Participant and their Beneficiaries or their Sub-Contractors will permit visits involving access to Classified Information to their establishments, or to Beneficiary or Sub-Contractor facilities located on their territory or under their jurisdiction, by Government representatives of another Participating State, staff of Participants, and by Beneficiary or Sub-Contractor employees. Such visits are subject to the provisions of this Section.

6.1 Procedures for International Visits at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET

1. The arrangements described hereafter apply to representatives of the Action Participants, the external experts contracted by the Granting Authority and to the personnel of Beneficiaries or Sub-Contractors under Action who need to undertake visits to another Participant or to facilities of Beneficiaries or Sub-Contractors, and where such visits require or may require access to Action Information classified at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET.

2. Each Participant and Beneficiary or Sub-Contractor will permit visits involving access to classified Action information on a case-by-case basis to its facilities, by civilian or military representatives of other Action Participants or by personnel of Beneficiaries or Sub-Contractors, provided that the visitor holds the appropriate PSC (for CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET) and has a Need-to-Know.

3. Such visits will be arranged directly between the security officials of the visitor and the establishment/facility to be visited without involving the NSAs/DSAs concerned, however, by respecting additional national requirements for notification of such visits to their NSAs/DSAs[1].

4. Visitors shall comply with all security regulations and other relevant regulations of the host establishment to be visited. Any Action Information disclosed or made available to visitors shall be treated as if supplied via official channels to the entity sponsoring the visit.

5. Prior to arrival at the facility to be visited, a Request for Visit, as shown in Annex F, or the national equivalent, including confirmation of the visitor's PSC, shall be provided at least 24 hours before arrival directly by the Security Officer of the sending facility/establishment to the Security Officer of the facility to be visited.

6. Both the sending and receiving facilities are to confirm that there is a need for the visit and both must hold an FSC.

   (a) Responsibilities of the sending Security Officer:

   • The sending Security Officer must ensure with the parent NSA/DSA that the receiving facility is in possession of an appropriate FSC;

   • Confirm that the visitor holds a valid PSC.

   (b) Responsibilities of the receiving Security Officer:

   • The receiving Security Officer must ensure with the parent NSA/DSA that the sending facility is in possession of an appropriate FSC;

[1] NSAs/DSAs will retain the right to request facilities under their jurisdiction to be visited or conducting such international visits to inform their NSA/DSA about any such visits.

• The receiving Security Officer must ensure that records are kept of all visitors, including the name, the organisation they represent, date of expiry of the PSC, the date(s) of the visit(s) and the name(s) of the person(s) visited.

Such records are to be retained for a period no less than three years.

(c) Responsibilities of the Visitor:

• To confirm identity, the visitor must be in possession of a valid ID card or passport for presentation to the Security Officer or other authorised official at the receiving facility/establishment/command/headquarters.

6.2 Procedures for International Visits at the level of RESTREINT UE/EU RESTRICTED

1. Visits relating to Classified Information at the level of RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending facility and the receiving facility without formal requirements.

Section 7 - Awarding of grants agreements and sub-contracting (security aspects)

1. An FSC is granted by an NSA/DSA to indicate, in accordance with its applicable laws, rules or regulations, that a Beneficiary or Sub-Contractor under its jurisdiction is capable of protecting Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET at that facility. FSCs are confirmed by the Security Authority responding to a Facility Security Clearance Information Sheet (FSCIS) request submitted by another Security Authority. Some Participant States may, in accordance with their applicable laws, rules or regulations, also issue FSC certificates for their Beneficiaries or Sub-Contractors.

2. In case where the Beneficiary or Sub-Contractor is a Government or a Government controlled entity, the responsible NSA of that entity shall confirm to the Granting Authority that the entity is capable in handling EU classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, as appropriate.

3. NSAs/DSAs will notify the appropriate authority of the Participants if an FSC that it has issued to one of its Beneficiaries or Sub-Contractors has been suspended or withdrawn.

7.1 Proposal submission stage and awarding of classified grants within EDF

1. Prior to launching an invitation to submit a proposal or awarding a classified grant, the Granting Authority will determine the security classification of any information that may be provided to applicants.

2. All Beneficiaries or their Sub-Contractors who are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either during the performance of the classified grant agreement itself or during the proposal stage, must hold a Facility Security Clearance (hereinafter 'FSC') at the required level. The following identifies the three scenarios that may arise during the proposal stage for a classified grant agreement involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

a) No access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the proposal stage:

Where the invitation to submit a proposal or the call for proposals concerns a grant agreement that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the applicant to handle such information at the tender stage, an applicant not holding an FSC at the required level shall not be excluded from the bidding process.

b) Access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the Granting Authority during the proposal stage:

Access will be granted to applicant personnel who are in possession of a Personnel Security Clearance (hereinafter 'PSC') at the required level and who have a need-to-know. The Granting Authority will verify whether an FSC is also required under national laws and regulations at this stage before such access is granted.

Where EUCI is provided to an applicant at the proposal stage, a non-disclosure agreement shall be signed, obliging the tenderer or applicant to handle and protect

EUCI provided to him in accordance with Commission Decision (EU, Euratom) 2015/444.

c) Handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the applicant during the proposal stage:

Where the invitation to submit a proposal or the call for proposals requires applicants to handle or store EUCI at their premises, the applicant shall hold an FSC at the required level or shall be granted other appropriate approval to handle and store classified information at these levels. In such circumstances, the Granting Authority will obtain an assurance from the relevant NSA/DSA that the applicant has been granted an appropriate FSC or other approval. Access will be granted to the applicant personnel who are in possession of a PSC at the required level and who have a need-to-know.

Where EUCI is provided to an applicant at the proposal stage, a non-disclosure agreement shall be signed, obliging the applicant to handle and protect EUCI provided to it in accordance with Commission Decision (EU, Euratom) 2015/444.

3. An FSC is not required for access to classified information at RESTREINT UE/EU RESTRICTED level, either at the proposal stage or for the performance of the grant agreement. However, some EU Member States require an FSC for grant agreements or sub-contracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations. Such national requirements shall not put additional obligations on other Member States or exclude Beneficiaries/Sub-Contractors from Member States not having such FSC requirements for access to RESTREINT UE/EU RESTRICTED information for related grant agreements or sub-contracts or a competition for such, while these grant agreements or sub-contracts shall be performed in Member States according to their national laws and regulations.

4. Where an FSC is required for the performance of a classified grant agreement, the Granting Authority will submit a request to the Beneficiary's NSA/DSA using a Facility Security Clearance Information Sheet (hereinafter 'FSCIS'). The classified grant agreement will not be signed until the Beneficiary's NSA/DSA has confirmed the applicant's FSC or has otherwise approved its capability to handle and store classified information up to required level; or, in case the classified grant agreement is awarded to a consortium, until the NSA/DSA of at least one applicant within the consortium, or more if necessary, has confirmed that applicant’s FSC or has otherwise approved its capability to handle and store classified information up to required level.

7.2 Sub-contracting to Sub-Contractors of Participant States or non-Participant EU Member States to the Action

1. Sub-contracting to entities other than already permitted under the grant agreement shall be subject to prior written consent from the Granting Authority.

2. Before a Beneficiary enters into negotiations for a sub-contract involving Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to a Sub-Contractor based in another Participant State or in a non-Participant EU Member State, the Security Officer of the Beneficiary proposing the sub-contract shall first obtain confirmation from its NSA/DSA that the potential Sub-Contractor has a valid FSC (if required). FSCs will be queried and confirmed as described at the start of this Section.

3. No Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be provided to the facility of the Sub-Contractor before an FSC confirmation has been obtained from the relevant NSA/DSA.

4. The Granting Authority shall notify, through the Commission Security Authority, the NSA/DSA of a Sub-Contractor when a classified sub-contract is awarded, and shall provide a copy of the sub-contract-specific security provisions.

7.3 Sub-contracting to Sub-Contractors located in a non-EU State or established by an international organisation

1. Where the classified grant agreement permits sub-contracting, such sub-contracting to entities located in a non-EU State or established by an international organisation shall be subject to prior written consent from the Granting Authority.

2. Before a Beneficiary enters into negotiations for a sub-contract involving Classified Information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to a Sub-Contractor based in a non-EU State or established by an international organisation, the Security Officer of the Beneficiary proposing the sub-contract shall first obtain confirmation from its NSA/DSA through the Commission Security Authority that the potential Sub-Contractor has a valid FSC. FSCs will be queried and confirmed as described at the start of this Section.

3. Any sub-contracting to an entity, which is located in a non-EU State or established by an international organisation constitutes a release of EUCI to that non-EU State or international organisation.

4. Prior to authorising the placement of a sub-contract with a Sub-Contractor located in a non-EU State or established by an international organisation, the Granting Authority shall verify whether a Security of Information Agreement is in place with that State or international organisation, and, if applicable, ensure, following the consultation with Member States whose national Classified Background Information has been used for generating Classified Foreground Information, that the awarding of such sub-contract does not contravene the security and defence interests of the Union and its Member States.

5. Sub-contracts placed with a Sub-Contractor located in a non-EU State or established by an international organisation will include a security clause requiring the Sub-Contractor to protect EUCI in accordance with the Security of Information Agreement in place between the EU and that non-EU State or international organisation.

6. The Granting Authority shall notify, through the Commission Security Authority, the Security Authority of a Sub-Contractor when a classified sub-contract is awarded, and shall provide a copy of the sub-contract-specific security provisions.

7.4 List of approved Beneficiaries and Sub-Contractors

In order to allow for tracing the flow of classified information relating to EDF, and to allow NSAs/DSAs to monitor the implementation of the provisions of this PSI at facilities of Beneficiaries or Sub-Contractors under their jurisdiction, the Commission will maintain a list of Beneficiaries and Sub-Contractors that are involved in grant agreements classified at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET in the EDF.

The list shall be provided to the Participants' NSAs/DSAs at least twice a year.

7.5 Security plan in the event of non-selection of an applicant, or termination or expiry of a classified grant agreement

1. This sub-section describes the procedures which the Participants and Beneficiaries or Sub-Contractors shall follow in the event of the following:

    a. A Granting Authority, or Beneficiary terminates, respectively, a classified grant agreement or sub-contract;

    b. A classified grant agreement or sub-contract expires;

    c. An applicant receives or generates Classified Information in the proposal stage but is not selected; or

    d. A Beneficiary receives and generates Classified Information during an early phase of the Action but is not selected for funding or work on a future phase of the Action.

7.5.1 Participant-held information

1. In the event of termination or expiry of a classified grant, the Participants' respective rights and responsibilities with regard to Classified Background and Classified Foreground Information relating to the Programme shall be determined by the Granting Authority, taking into account the rights of the Originator.

2. A Participant that retains Classified Information shall continue to safeguard it in accordance with this PSI and its applicable laws, rules or regulations, and shall not use that information for other purposes without the prior written consent of the Originator.

7.5.2 Beneficiary-held information

1. A Beneficiary or Sub-Contractor that is authorised by the Commission (or the Originator for Classified Background Information) to retain Classified Information shall safeguard it in accordance with this PSI and the applicable laws, rules or regulations.

2. Without the prior written consent of the Commission (or the Originator for Classified Background Information), a Beneficiary or Sub-Contractor shall not use Classified Information for any other purpose than for which it was provided.

3. All Classified Information released within the context of a classified grant, sub-contract, proposal or tender, will be retained, returned, or destroyed according the following provisions:

    a. An applicant for a grant or tenderer for a sub-contract receives or generates information during, respectively, the proposal or tendering stage, and is not selected:

        i. All invitations to submit a proposal or tender shall contain a clause requiring an applicant or tenderer who does not eventually submit a proposal or tender to return all classified documents which were provided to enable the applicant or tenderer to submit a proposal or tender to the Granting Authority by the date set for the submission of proposals or opening of tenders.

        ii. An unsuccessful applicant or tenderer shall be required to return all classified documents after a stipulated period of time (normally within 15 working days after notification that a proposal or tender was not accepted).

b. When a Beneficiary or Sub-Contractor has held a classified grant or sub-contract, but the classified grant or sub-contract is terminated, expires or if the Beneficiary or Sub-Contractor is not selected for further funding or work on the next phase of an Action, the Beneficiary or Sub-Contractor:

i. Shall return all Classified Information unless approval for retention or destruction has been given, as provided for in paragraphs ii. and iii. below.

ii. If the Commission Security Authority (or Originator) approves that a Beneficiary or Sub-Contractor can destroy the Classified Information, the Beneficiary or Sub-Contractor shall ensure that the destruction is undertaken in accordance with the relevant security rules and regulations.

iii. If the Commission (or Originator) approves that a Beneficiary or Sub-Contractor can retain the Classified Information, the Beneficiary or Sub-Contractor shall continue to protect the information in accordance with its applicable laws, rules or regulations and this PSI.

4. In the event that an FSC is withdrawn, the Beneficiary or Sub-Contractor shall return all Classified Information to, respectively, their Granting Authority or Beneficiary, or dispose of such information in accordance with instructions from their Security Authority.

7.6 Procedures related to breaches, compromises or loss of Classified Information

1. The personnel shall report suspected or actual Security Breaches, Compromises and losses of Classified Information to their Security Officer or Local Security Officer as soon as possible, and no later than 24 hours after the discovery.

2. Where applicable, the Security Officer concerned will initiate damage limitation or mitigation measures promptly.

3. The Security Officer of the facility concerned shall investigate the circumstances of the security incident and report it to its Security Authority in accordance with the following:

a. If it is suspected that Classified Information has been compromised, lost, or a Security Breach that represents a significant risk of future Compromise has occurred, this shall be reported to the competent Security Authority as soon as possible, and no later than 48 hours after the discovery.

b. If Classified Information is known to have been compromised this shall be reported immediately in order for the Security Authority to mitigate the potential damage that may be caused.

4. Once informed of a security incident, the Security Authority concerned shall take the appropriate action in accordance with its applicable laws, rules or regulations.

5. For suspected or actual Compromise, or loss of Classified Information, or serious security breaches that may represent a significant risk of future Compromise, the Security Authority shall submit a report to the Commission Security Authority and the relevant NSA/DSAs, as identified in Annex A including the following details as a minimum:

a. A description of the circumstances of the security incident;

b. The date or period when the security incident occurred;

c. The location of the security incident;

d. The security classification and markings of the information involved in the security incident;

e. A list of the Classified Information that has been or may have been compromised or that is unaccounted for;

f. Specific identification of the Classified Information, to include Originator, subject, reference, date, copy number, and language;

g. Actions taken to locate and recover the Classified Information;

h. The responsible person(s) and reasons for Compromise or possible Compromise;

i. Assessments of the likelihood of Compromise (i.e. "certain", "probable", "possible", or "unlikely") including an explanation;

j. A statement on whether the Originator has been informed of the security incident; and

k. Actions taken to secure the Classified Information and limit further damage.

6. Such reports should be classified, at least, at RESTRICTED level.

7. The Security Officer where the security incident occurred shall provide all necessary assistance to its Security Authority in preparing the report.

8. Any additional measures related to the reporting of Security Breaches, Compromise or loss of COMSEC Items are addressed in the Action COMSEC Instructions (Annex G).

ANNEX A – SECURITY AUTHORITIES OF PARTICIPANTS OF THE EDF ACTION

A1 - SECURITY AUTHORITIES OF THE PARTICIPANT STATES[2]

A2 – OTHER SECURITY AUTHORITIES

European Commission Security Authority

European Commission Security Directorate

DG HR Security Directorate (DS)

Rue de la Loi 200

B-1049 Brussels

Belgium

Telephone: +32 2 2958716 (Industrial Security Advice)

Point of Contact for standard Requests for Visits (RfV)

Telephone: +32 2 2991551

Email: EC-SECURITY-CLEARANCE@ec.europa.eu

Please send a copy to the LSO:

DG DEFIS LSO

BREY 09/110

Telephone: +32 2 2950261

Email: DEFIS-LSO@ec.europa.eu

For matters related to the release of Action-related information:

DG DEFIS - Director "A" Defence Industry

Email: DEFIS-A@ec.europa.eu

[2] To be completed for a given specific Action PSI.

ANNEX B - TABLE OF EQUIVALENT SECURITY CLASSIFICATION MARKINGS[3]

[3] This table is provided for reference to help compare classification markings of Classified Foreground Information (EUCI) with those of Classified Background Information. Please note that the main principles for handling and protecting Classified Foreground Information (EUCI) and Classified Background Information are set out, respectively, in paragraphs 4.1.1 and 4.1.2 of this PSI.

Participant	Secret	Confidential	Restricted
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	*(Note 1, see below)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG
France	SECRET SECRET DÉFENSE *(Note 2, see below)*	CONFIDENTIEL DÉFENSE *(Notes 2 and 3, see below)*	*(Note 4, see below)*
Germany *(Note 5, see below)*	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)

Participant	Secret	Confidential	Restricted
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!
Ireland	SECRET	CONFIDENTIAL	RESTRICTED
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET SECRET *(Note 6, see below)*	KUNFIDENZJALI CONFIDENTIAL *(Note 6, see below)*	RISTRETT RESTRICTED *(Note 6, see below)*
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
Norway	HEMMELIG	KONFIDENSIELT	BEGRENSET

Note 1. Belgium: 'Diffusion Restreinte/Beperkte Verspreiding' is not a security classification in Belgium. Belgium handles and protects RESTREINT UE/EU RESTRICTED information and classified information bearing the national classification markings of RESTRICTED level in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

Note 2. France: Information generated by France before 1 July 2021 and classified SECRET DÉFENSE and CONFIDENTIEL DÉFENSE continues to be handled and protected at the equivalent level of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL respectively.

Note 3. France: France handles and protects CONFIDENTIEL UE/EU CONFIDENTIAL information in accordance with the French security measures for protecting SECRET information.

Note 4. France: France does not use the classification 'RESTREINT' in its national system. France handles and protects RESTREINT UE/EU RESTRICTED information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union. France will handle classified information bearing the national classification markings of RESTRICTED level in accordance with its national rules and regulations in force for 'DIFFUSION RESTREINTE'. The other Participants will handle and protect information marked 'DIFFUSION RESTREINTE' according to their national laws and regulations in force for the level RESTRICTED or equivalent or according to the standards defined in the present document whichever is higher.

Note 5. Germany: VS = Verschlusssache.

Note 6. Malta: The Maltese and English markings for Malta can be used interchangeably.

Note 7. Portugal and Spain: Attention is drawn to the fact that the markings RESERVADO and SECRETO used by Portugal and Spain refer to different classifications. Creators of documents with RESERVADO or SECRETO markings are advised to put below these classification markings an annotation indicating the country of origin – either "(ORIGINATOR: PORTUGAL)" or "(ORIGINATOR: SPAIN)".

ANNEX C – FACILITY AND PERSONNEL SECURITY CLEARANCE FOR BENEFICIARIES AND SUB-CONTRACTORS INVOLVING RESTREINT UE/EU RESTRICTED INFORMATION[4]

Member States and associated countries.	FSC		PSC	
	YES	NO	YES	NO
Belgium		X		X
Bulgaria		X		X
Czechia		X		X
Denmark	X		X	
Germany		X		X
Estonia	X			X
Ireland		X		X
Greece		X		X
Spain		X		X
France		X		X
Croatia		X		X
Italy		X		X
Cyprus		X		X
Latvia		X		X
Lithuania		X		X
Luxembourg	X		X	
Hungary		X		X
Malta		X		X

[4] These national requirements for FSC/PSC must not place any additional obligations on other Member States or beneficiaries, contractors and sub-contractors under their jurisdiction.

Netherlands	X (only for defence- related grant agreements and subcontracts)			X
Austria		X		X
Poland		X		X
Portugal		X		X
Romania		X		X
Slovenia	X			X
Slovakia	X			X
Finland		X		X
Sweden		X		X
Norway		X		X

ANNEX D – MINIMUM REQUIREMENTS FOR PROTECTION OF EUCI IN ELECTRONIC FORM AT RESTREINT UE/EU RESTRICTED LEVEL HANDLED IN THE BENEFICIARY'S (SUB-CONTRACTOR'S) COMMUNICATION AND INFORMATION SYSTEMS

General

1. The Beneficiary (Sub-Contractor) must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED classified information is in compliance with the minimum security requirements as stated within this security clause and any other additional requirements advised by the Granting Authority or, if applicable, with the National Security Authority (NSA) or Designated Security Authority (DSA).

2. It is the responsibility of the Beneficiary (Sub-Contractor) to implement the security requirements identified in this document.

3. For the purpose of this document a Communication and Information System (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax, servers, network management system, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.

4. Special equipment such as cryptographic products must be protected in accordance with its dedicated Security Operating Procedures (SecOPs).

5. Beneficiaries (Sub-Contractors) must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a responsible Security Officer of the facility.

6. The use of privately-owned equipment of Beneficiary's (Sub-Contractor's) personnel (hardware and software) for processing RESTREINT UE/EU RESTRICTED classified information is not permitted.

7. Accreditation of the Beneficiary's (Sub-Contractor's) CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the Participant's Security Accreditation Authority (SAA) or delegated to the Security Officer of the Beneficiary (Sub-Contractor) as permitted by national laws and regulations.

8. Only information classified RESTREINT UE/EU RESTRICTED encrypted using approved cryptographic products may be handled, stored or transmitted (wired or wireless) as any other unclassified information under the grant agreement (sub-contract). These cryptographic products must be approved by the EU or a Member State.

9. External facilities involved in the maintenance/repair work must be obliged, on a contractual basis, to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED as set out in this document.

10. At the request of the Granting Authority or relevant NSA/DSA/SAA, the Beneficiary (Sub-Contractor) must provide evidence of compliance with the grant agreement (sub-contract) Security Clause. If also requested, the Beneficiaries (Sub-Contractors) will permit an audit and inspection of the Beneficiary's (Sub-Contractor's) processes and facilities by representatives of the Granting Authority, the NSA/DSA/SAA, or the relevant EU security authority in order to ensure compliance with these requirements.

Physical Security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management system, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be limited to only specifically authorised persons. Without prejudice to paragraph 8 equipment as described in paragraph 3 has to be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (for example, USB, mass storage devices, CD-RWs) to components on the CIS.

Access to CIS

13. Access to Beneficiary's (Sub-Contractor's) CIS handling EUCI is based on a strict need to know principle and authorisation of personnel.

14. All CIS must have up to date lists of authorised users and an authentication of all users at the start of each processing session.

15. Passwords, which are part of most identification and authentication security measures, must be a minimum of 9 characters long and must include numeric and "special" characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. Passwords must be changed as soon as possible if they have or are suspected of having been compromised or disclosed to an unauthorised person.

16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or CIS must activate a password protected screen saver after 15 minutes of inactivity.

17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked after at most 5 successive incorrect login attempts.

18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.

19. SecOPs must be available for the Users and Administrators and must include security roles descriptions and associated list of tasks, instructions and plans.

Accounting, Audit and Incident Response

20. Any access to the CIS must be logged.

21. The following events must be recorded:

    a) all log on attempts whether successful or failed;
    b) log off (including time out where applicable);
    c) creation, deletion or alteration of access rights and privileges; and
    d) creation, deletion or alteration of passwords.

22. For all of the events listed above at least the following information must be communicated:

    a) type of event;
    b) user ID;
    c) date and time; and
    d) device ID.

23. The accounting records should support the capability to be examined by a Security Officer for potential security incidents and that they can be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.

24. The Beneficiary (Sub-Contractor) must have an established response strategy to deal with security incidents. Users and Administrators must be instructed on how to react to incidents, how to report incidents and what to do in case of emergencies.

25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the Granting Authority. The report must contain a description of the information involved and a description of the circumstances of the (suspected) compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the Security Officer.

Networking & Interconnection

26. When a Beneficiary (Sub-Contractor) CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this leads to a significant increase in threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED classified information handled by that CIS. This includes the internet, other public or private CIS such as other CIS owned by the Beneficiary (Sub-Contractor). In this case, the Beneficiary (Sub-Contractor) must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The Beneficiary (Sub-Contractor) will provide to the Granting Authority and where nationally required, the competent SAA a statement of compliance certifying that the Beneficiary (Sub-Contractor) CIS and respective interconnection have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED.

27. Remote access from others systems to LAN services (e.g., remote access to e-mail and remote SYSTEM support) are prohibited unless special security measures are implemented and agreed by the Granting Authority and where nationally required, approved by the competent SAA.

Configuration Management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams) must be available and regularly maintained.

29. Configuration checks must be carried out by the Security Officer of the Beneficiary (Sub-Contractor) on hardware and software to ensure that unauthorised hardware and software has not been introduced.

30. Changes to the Beneficiary (Sub-Contractor) CIS configuration must be assessed for their security implications and must be approved by the Security Officer and where nationally required, the SAA.

31. The system must be scanned for the presence of security vulnerabilities at least quarterly. Software must be implemented allowing detection of malware. Such software must be kept up-to-date. If possible, the software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.

32. The Beneficiary (Sub-Contractor) must develop a Business Continuity Plan. Back-up procedures are established addressing the following:

    a) frequency of back-ups;
    b) storage requirements on-site (fireproof containers) or off-site;
    c) control of authorised access to back-up copies.

Sanitisation and Destruction

33. For CIS or data storage media that has at any time held RESTREINT UE/EU RESTRICTED classified information the following sanitisation must be performed to the entire system or storage media prior to its disposal:

    a) Flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
    b) Magnetic media (e.g. hard disks) must be overwritten or degaussed;
    c) Optical media (e.g. CDs and DVDs) must be shredded or disintegrated; and
    d) For any other storage media, the Granting Authority or, if appropriate, the NSA/DSA/SAA, should be consulted on the security requirements to be met.

34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to an entity not authorised to access RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).

ANNEX E - PROCEDURE FOR HAND CARRIAGE OF CLASSIFIED INFORMATION

C.1. When hand carriage of classified material is permitted, the following procedures will apply:

a. The Courier will carry a courier certificate recognised by all Participants, authorising him to carry the package as identified (see the courier certificate example below) stamped and signed by the Security Authority and the consignor's officer;

b. A copy of the "Notes for the Courier" (shown below) will be attached to the certificate; and,

c. The courier certificate will be returned to the issuing Security Authority through the consignor's security officer immediately after completion of the journey.

C.2. The consignor's security officer is responsible for instructing the bearer in all of his duties and of the provisions of the "Notes for the Courier".

C.3. The courier will be responsible for the safe custody of the classified material until such time that it has been handed over to the consignee's security officer. In the event of a breach of security, the consignor's Security Authority may request the authorities in the country in which the breach occurred to carry out an investigation, report their findings, and take legal action, as appropriate.

(LETTERHEAD)

COURIER CERTIFICATE

EU EDF ACTION TITLE (optional)

COURIER CERTIFICATE NO. …… (*)

FOR THE INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer:

Mr./Ms. **(name/title)**

Born on**: (day/month/year)** in **(country)**

A national of **(country)**

Holder of passport/identity card no.: **(number)**

Issued by: **(issuing authority)**

On: **(day/month/year)**

Employed with: **(company or organisation)**

Is authorised to carry on the journey detailed below the following consignment:

(Number and particulars of the consignment in detail, i.e. No. of packages, weight and dimensions of each package and other identification data as in shipping documents)

……..

……..

(*) May also be used by security guards.

- The material comprising this consignment is classified in the interests of the security of:

(Indicate the countries having interest. At least the country of origin of the shipment and that of the destination should be indicated. The country (or countries) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly authorised persons of those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police and/or Immigration officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

(LETTERHEAD)

Annex to the "Courier Certificate" No…….

for the International Hand Carriage of

Classified Material

NOTES FOR THE COURIER(*)

1. You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE" has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behaviour, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security obligations.

2. The following general points are brought to your attention:

(*) May also be used by security guards.

(a) You will be held liable and responsible for the consignment described in the Courier Certificate;
(b) Throughout the journey, the classified consignment must stay under your personal control;
(c) The consignment will not be opened en route except in the circumstances described in sub-paragraph (j) below;
(d) The classified consignment is not to be discussed or disclosed in any public place;
(e) The classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance and storage facilities may be utilised. You are to be instructed on this matter by your company Security Officer;
(f) While hand carrying a classified consignment, you are forbidden to deviate from the travel schedule provided, unless unforeseen circumstances require a change of schedule;
(g) In cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (l) below. If you have not received these details, ask for them from your company Security Officer;
(h) You and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current;
(i) If unforeseen circumstances make it necessary to transfer the consignment to an individual other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (l);
(j) There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials inquire into the contents of the consignment, show them your "Courier Certificate" and this note and insist on showing them to the senior Customs, Police and/or Immigration Official; this action should normally suffice to allow the consignment to pass through unopened. However, if the senior Customs, Police and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public.

You should take precautions to show officials the minimum content necessary to them that the consignment does not contain any other item and ask the official to repack or assist in re-packing it immediately upon completion of the examination.

You should request the senior Customs, Police and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the DSA's of their respective governments.

(k) Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a DSA of the receiving government.

(l) Along the route you may contact the following officials to request assistance:

……

……

From:

(Originating country)

To:

(Country of destination)

Through:

(List intervening countries)

Authorised stops:

(List locations)

Date of beginning of journey:

(Day/month/year)

Signature of company's Security officer	Signature of the Security Authority
(Name)	(Name)
Company's stamp	Official stamp or NSA/DSA's seal

N O T E: To be signed on completion of journey

I declare in good faith that, during the journey covered by the "Courier Certificate", I am not aware of any occurrence or action, by myself or by others that could have resulted in the compromise of the consignment, except the events listed below *(if needed)*:

…….

…….

Courier's Signature:

Witnessed by:

(Company Security Officer's signature)

Date of return of the "Courier Certificate":

(Day/month/year)

MULTI-TRAVEL COURIER CERTIFICATE N° …….

for international hand carriage of classified DOCUMENTS, EQUIPMENTS AND/OR COMPONENTS

This is to certify that the bearer Mr/Ms (name and title) …… born on (day, month, year) …… in (country) ……..……, a national of (country) …….. holder of passport or identity card n° …… issued by (issuing authority) : ……. on (day, month, year) :…… employed by (company or organization) : ……..……... is authorized to carry classified documents, equipment and/or components between the following countries: ……..……..……

The bearer above is authorized to use this certificate as many times as necessary, for classified shipments between the countries here above until (date): ……..

The shipment description should be attached to each consignment.

The attention of customs authorities, police and immigration services is drawn to the following points:

- The material forming each consignment is classified in the interest of national security of the countries here above.
- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a Need-to-Know and in the presence of the courier.
- It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.
- Customs, Police and/or Immigration officials of countries to be transited, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Signature of Security Officer

Signature of the Security Authority

NOTES FOR THE COURIER

You have been appointed to carry/escort classified consignments. Your "Courier certificate" has been provided. Before starting your journeys, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your obligations during the specific journey (behaviour, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security obligations.

The following general points are brought to your attention:

1. You will be held liable and responsible for the consignments described in the "descriptions of shipments".
2. Throughout the journey, the classified consignments must stay in your personal possession, unless you are accompanying a classified consignment under NSA/DSA approved transportation plan.
3. The consignments will not be opened en route except in the circumstances described in paragraph 10 below.
4. The classified consignments are not to be discussed or disclosed in any public place.
5. The classified consignments are not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilized. You are to be instructed on this matter by your company security officer.
6. While hand carrying or accompanying a classified consignment, you are forbidden to deviate from the schedule provided.
7. In case of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal possession except under circumstances described in paragraph 2 above; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as stated in paragraph 11 below. If you have not received these details, ask for them from your company security officer.
8. You and the company security officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current.
9. If unforeseen circumstances make it necessary to transfer a consignment to other than the designated representative of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in the description of shipment.
10. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your "courier certificate" the description of shipment and this note and insist on showing them to the senior Customs, Police, and/or Immigration Official; This action should normally suffice to allow the consignment to pass through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignment you may open it in his presence, but this should be done in area out of sight of the general public.

    You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination.

You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the consignment by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the NSA/DSA of their respective governments.

11. Along the route you may contact the officials whose details will be provided to you before each journey and request assistance from them.
12. Upon return from each journey, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a NSA/DSA of the receiving government.

ANNEX to multi-travel certificate

Multi-travels courier certificate No:.....

Description of shipment nr : ……..

Transport from (date) : …… to (date) : ……

Bearer (name) : ……

Itinerary : from (originating country) …… to (destination country) …… through (crossed countries) …… authorized stops (list of locations) : ……

References of receipt or inventory list: ……

Description of the shipment (number of package, dimensions and, if needed, weight of each package)

Officials you may contact to request assistance

Signature of company's Security Officer

Note to be signed on completion of each shipment:

I declare in good faith that, during the journey covered by this "shipment description", I am not aware of any occurrence or action, by myself or by other, that could have resulted in the compromise of the consignment, except the events listed below *(if needed)*:

……..

……..

Place and date of declaration: ……

Courier’s signature:……..

Witnessed by (name and signature of company Security Officer): …….

ANNEX F - TRANSPORTATION PLAN

(LETTERHEAD)

TRANSPORTATION PLAN -

FOR THE TRANSPORT OF CLASSIFIED CONSIGNMENTS

(INSERT NAME OF EDF ACTION)

1. INTRODUCTION

This transportation plan lists the procedures for the transport of classified **(insert EDF Grant or Contract name)** consignments between **(insert EDF Action Participants)**.

2. DESCRIPTION OF CLASSIFIED CONSIGNMENT

Provide a general description of the consignment to be moved. If necessary, a detailed, descriptive listing of items to be moved under this plan, including nomenclature, may be appended to this plan as an annex. Include in this section a brief description as to where and under what circumstances transfers of custody will occur.

3. IDENTIFICATION OF AUTHORISED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organisation, the authorised representatives of each EDF **Action** Participant who will authorise receipt for and assume security responsibilities for the classified consignment. Mailing addresses, telephone numbers, telefax numbers, and/or telex address, network addresses should be listed for each Participant's representatives.

4. DELIVERY POINTS

(a) Identify the delivery points for each Participant (e.g. ports, railheads, airports, etc.) and how transfer is to be effected.

(b) Describe the security arrangements that are required while the consignment is located at the delivery points.

(c) Specify any additional security arrangements, which may be required due to the unique nature of the transport or of a delivery point (e.g. an airport freight terminal or port receiving station).

5. IDENTIFICATION OF CARRIERS

Identify the commercial carriers, freight forwarders and transport agents, where appropriate, that might be involved to include the level of security clearance and storage capability.

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

(a) List, by participant, the storage or processing facilities and transfer points that will be used.

(b) Describe specific security arrangements necessary to ensure the protection of the classified consignment while it is located at the storage/processing facility or transfer point.

7. ROUTES

Specify in this section the routes for transport of the classified consignments under the plan. This should include each segment of the route from the initial dispatch point to the ultimate destination including all border crossings, in particular travel through non-Participant States. Routes should be detailed for each Participant in the logical sequence of the shipment from point to point. If overnight stops are required, security arrangements for each stopping point should be specified. Contingency stop over locations should also be identified as necessary.

8. PORT SECURITY AND CUSTOMS OFFICIALS

In this Section, identify arrangements for dealing with customs and port security officials of each Participant. The facility must verify that the courier has been provided with the necessary documentation and is aware of the rules necessary to comply with customs and security requirements. Prior co-ordination with customs and port security agencies may be required so that the Project/Programme transport will be recognised. Procedures for handling custom searches and points of contact for verification of transport at the initial dispatch points should also be included here.

9. COURIERS

When couriers are to be used, provisions for the international hand carriage of classified materials specified in Section II and Annex D will apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to carry out an inventory of transport and to examine all documentation upon receipt of the transport and:

(a) Notify the dispatcher of any deviation in routes or methods prescribed by this plan;

(b) Notify the dispatcher of any discrepancies in the documentation or shortages in the shipment.

(c) Clearly state the requirement for recipients to promptly advise the Security Authority of the dispatcher of any known or suspected compromise of classified consignment or any other exigencies which may place the transport in jeopardy.

11. DETAILS OF CLASSIFIED TRANSPORT

This section should contain the following items:

(a) Identification of dispatch assembly points.

(b) Packaging requirements that conform to the security rules of the EDF Action Participants. The requirements for dispatch documents seals, receipts, storage and security containers should be explained. Any unique requirement of the EDF Action Participants should also be stated.

(c) Documentation required for the dispatch points.

(d) Courier authorisation documentation and travel arrangements.

(e) Procedures for locking, sealing, verifying and loading consignments. Describe procedures at the loading points, to include tally records, surveillance responsibilities and witnessing of the counting and loading arrangements.

(f) Procedures for accessibility by courier to the shipment en route.

(g) Procedures for unloading at destination, to include identification or recipients and procedures for change of custody, and receipt arrangements.

(h) Emergency communications procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency.

(i) Procedures for identifying each consignment and for providing details of each consignment; the notification should be transmitted no less than six working days prior to the transport of the classified consignment.

12. RETURN OF CLASSIFIED MATERIAL

This section should identify requirements for return of classified material to the manufacturer or sending participant (e.g. warranty, repair, test and evaluation, etc.).

NOTE: Samples of these forms should be included, as appropriate, as enclosures to the plan as necessary.

(1) Packing list

(2) Classified material receipts

(3) Bills of lading

(4) Export declaration

(5) Waybills

(6) Other Participant-required forms

ANNEX G - REQUEST FOR VISIT[5]

Note: The completed form must be submitted directly to the Security Officer of the establishment to be visited. Fields of the form related to NSAs/DSAs should be left empty.

<table>
<tr><td colspan="3">REQUEST FOR VISIT

TO: _____

(Country/international organisation name)</td></tr>
<tr><td>1. TYPE OF VISIT REQUEST</td><td>2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS</td><td>3. SUMMARY</td></tr>
<tr><td>☐ One-time
☐ Recurring
☐ Emergency
☐ Amendment
☐ Dates
☐ Visitors
☐ Agency/Facility

For an amendment, insert the NSA/DSA original RFV Reference No._____</td><td>☐ CONFIDENTIAL or above</td><td>No. of sites: _____

No. of visitors: _____</td></tr>
<tr><td colspan="3">4. ADMINISTRATIVE DATA:</td></tr>
<tr><td colspan="2">Requestor:

To:</td><td>NSA/DSA RFV Reference No._____

Date (dd/mm/yyyy): _____/_____/_____</td></tr>
</table>

[5] This annex contains standard forms used by the Member States. The term 'contract' in this annex should be understood as also meaning 'grant agreement' or 'sub-contract'. The term 'company' should be understood as also meaning 'entity'.

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Government ☐ Industry ☐ European Commission ☐ Other

If other, specify: _____

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - ***(Annex 1 to be completed)***

7. DATE OF VISIT ***(dd/mm/yyyy)***: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE ***(Select one from each column)*****:**

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

9. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE ***(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*****:**

10. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:

Only if required by the laws/regulations of the countries involved	
☐ Unclassified ☐ RESTRICTED	☐ CONFIDENTIAL ☐ SECRET If other, specify: _____

11. PARTICULARS OF VISITOR(S) - *(Annex 2 to this form to be completed)*

12. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

13. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

14. REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REMARKS *(Mandatory justification required in case of an emergency visit)*:

ANNEX 1 to RFV FORM

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. ☐ Government ☐ Industry ☐ EC ☐ EDA ☐ Other If other, specify: _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

2. ☐ Government ☐ Industry ☐ EC ☐ EDA ☐ Other

If other, specify: _____

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

3. ☐ Government ☐ Industry ☐ EC ☐ EDA ☐ Other

If other, specify: _____

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

4. ☐ Government ☐ Industry ☐ EC ☐ EDA ☐ Other

If other, specify: _____

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

5. ☐ Government ☐ Industry ☐ EC ☐ EDA ☐ Other

If other, specify: _____

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

PARTICULARS OF VISITOR(S)
1 ☐ Government ☐ Industry ☐ EC Employee ☐ EDA Employee ☐ Other (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
2 ☐ Government ☐ Industry ☐ EC Employee ☐ EDA Employee ☐ Other (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/AGENCY:

3 ☐ Government ☐ Industry ☐ EC Employee ☐ EDA Employee

☐ Other (Specify: _____)

SURNAME:

FORENAMES *(as per passport)*:

RANK *(if applicable)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/AGENCY:

4 ☐ Government ☐ Industry ☐ EC Employee ☐ EDA Employee

☐ Other (Specify: _____)

SURNAME:

FORENAMES *(as per passport)*:

RANK *(if applicable)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/AGENCY:

5 ☐ Government ☐ Industry ☐ EC Employee ☐ EDA Employee

☐ Other (Specify: _____)

SURNAME:

FORENAMES *(as per passport)*:

RANK *(if applicable)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/AGENCY:

(Continue as required)

ANNEX H – COMSEC INSTRUCTIONS FOR COMSEC ITEMS WITH AN EU SECURITY CLASSIFICATION EXCHANGED UNDER EDF ACTION XX

This annex is classified at the level of RESTREINT UE/EU RESTRICTED

Should you be entitled access this annex please address your motivated request to

DEFIS-DEFENCE-SECURITY@ec.europa.eu