COUNCIL OF THE EUROPEAN UNION

Brussels, 17 February 2012

7368/12

LIMITE

CSC 13

NOTE

From :	The General Secretariat of the Council
To :	Council Security Committee and its Information Assurance sub-area
Subject :	Security inspection checklist

Following the adoption of the Council's security rules for protecting EU classified information on 31 March 2011[1], delegations will find attached the security inspection checklist updated by the GSC Security Office and the Information Assurance office.

The checklist details the items to be verified in the course of an inspection of a Member State or EU agency. It will be used for any visit pursuant to Article 12 (5) of the Council's Security Rules to ascertain effectiveness of the security measures in place in a third State or international organisation for protecting EUCI provided or exchanged.

---

[1] Council Decision 2011/292/EU, OJ L 141, 27.5.2011, p.17

SECURITY INSPECTION CHECKLIST

TABLE OF CONTENTS

1.1 GENERAL INTRODUCTION

This checklist contains guidelines for evaluating the measures implemented or planned for protecting EU classified information.

Basic principles for such evaluations are laid down in the Council's security rules for protecting EU classified information (Council Decision 2011/292/EU of 31 March 2011). These are supplemented by the Council's guidelines on the conduct of security inspections set out in doc. 16567/06.

1.2 RELEASE OF EU CLASSIFIED INFORMATION TO THIRD STATES OR INTERNATIONAL ORGANISATIONS

The Council's security rules provide for the possibility of releasing EU classified information to third States or international organisations. Release of EU classified information to third States or international organisations requires an assurance that they will provide the protection required by the Council. The decision to release EUCI originating in the Council to a third State or international organisation is taken by the Council on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the EU.

For the Council, the procedures governing the release of EU classified information to third States and international organisations are laid down in the Council's security rules. EU classified information may normally be released only on the basis of a security of information agreement or an administrative arrangement.

In certain cases when no framework is in place, EU classified information may exceptionally be released by autonomous decision[2], following a recommendation by the Council Security Committee, depending on the confidence that can be placed in the security regulations, structures and procedures in the third State or international organisation to which the EUCI is to be released.

[2] This decision has been sub delegated to COREPER (see doc. 14125/02).

1.3 INSPECTION CHECKLIST

This checklist may be used for four different kinds of inspections or assessment visits:

- Periodic inspections of the security arrangements for protecting EU classified information in the GSC, Member States and their Permanent Representations, as well as Member States' premises in Council buildings.
- Periodic inspections of the security arrangements for the protection of EU classified information in EU agencies.
- Assessment visits to a third State or international organisation in order to assess the level of preparedness and the effectiveness of measures taken by that State or international organisation for the protection of EU classified information which may be released to it under the terms of a security agreement with the third State or international organisation concerned.
- Assessment visits in a third State or international organisation in order to determine the level of EUCI to be exchanged with that State or international organisation.

1.4 CONDUCT OF AN INSPECTION OR ASSESSMENT VISIT

Security inspections and assessment visits are conducted in accordance with the guidelines on the conduct of security inspections approved by the Council (doc. 16567/06).

Member States, third States or international organisations with which an inspection or assessment visit is agreed will provide the inspection or assessment team with an up-to-date record of its legal and regulatory framework for protecting classified information as well as documentation on the security organisation mandated to implement this legal and regulatory framework.

This checklist should allow the inspection or assessment team to evaluate the security and the organisation in the field of physical security, personnel security, classified document security, industrial security and SCIS security.

After evaluation, the inspection or assessment team will present a formal technical report highlighting strengths, weaknesses and areas requiring improvement and, where possible, recommendations to address any of the weaknesses or areas of improvement established.

PART I PROTECTIVE SECURITY

SECTION 1 BASIC PRINCIPLES, MINIMUM STANDARDS AND SECURITY ORGANISATION

1.1 INTRODUCTION

In order to implement the Council decision on security rules for protecting EUCI, Member States should designate a National Security Authority responsible for protecting EUCI (Article 15(3) of the Council Decision).

1.2 PURPOSE, DEFINITION, RESPONSABILITY

	COUNCIL DECISION	ITEMS TO CHECK
1.2.1 PURPOSE, SCOPE AND DEFINITIONS	Article 1	- Is there any legislation on the protection of classified information? - To what is this legislation applicable? - What security measures are provided for by this legislation? - Are there approved national security procedures and/or directives on the protection of classified information? - Are the nature and scope of the instructions/directives appropriate for the task? - Are there security officers in the different departments of the organisation to supervise implementation of the security instructions/directives? - Organisation of all administrative and/or governmental departments to which EU classified information

	COUNCIL DECISION	ITEMS TO CHECK
		maybe sent. - What security standards are in place? - Do they meet the EU minimum security standards?
1.2.2 DEFINITION OF EUCI, SECURITY CLASSIFICATIONS AND MARKINGS	Article 2	
1.2.3 RESPONSIBILITY FOR IMPLEMENTATION	Articles 14 - 15(3)(a)(i-vi)	- Is there a National Security Authority (main tasks and responsibilities) or are there any security organisations in charge of intelligence activities, risk assessment and threat analysis? - Are common standards applied? - Is there national or international cooperation? - Who is responsible for security organisation? - How is the NSA organised? - Are the following responsibilities specified? o Management of classified information? o Establishment of TRÈS SECRET UE/ EU TOP SECRET registries and sub registries? o Existence of a formally-appointed classified information control officer and alternates? o How frequently are inspections conducted by the NSA?

	COUNCIL DECISION	ITEMS TO CHECK
		○ How is the security clearance process managed? ○ Do security plans to protect EU classified information exist?

SECTION 2 PERSONNEL SECURITY

2.1 INTRODUCTION

Personnel security is the basis of the security organisation especially if we consider that an ever increasing amount of information is exchanged and made available to ever greater numbers of people.

2.2 PRACTICAL GUIDELINES FOR INSPECTING PERSONNEL SECURITY

	COUNCIL DECISION	ITEMS TO CHECK
2.2.1 AUTHORISING ACCESS TO EUCI	Annex I para. 3-4	- What are the procedures or rules to determine the "need-to-know"? - Who is responsible for determining the need-to-know? - Is the need-to-know principle understood and applied to access to classified information? - What levels of security clearance are foreseen? - What are the procedures for controls to ensure that access is not granted to EUCI without appropriate valid clearance and need-to-know? - Does the national process for clearance security requests comply with the Council's security rules? - Are the positions which require access to classified information identified?

	COUNCIL DECISION	ITEMS TO CHECK
2.2.2 PERSONNEL SECURITY CLEARANCE REQUIREMENTS	Annex I para. 5-7	- What are the procedures for the security clearance of personnel who require access to classified information? - Is there a difference between the procedures applied to civilian and military personnel? - What is the national administrative procedure for a National Security Authority / National Administration to grant clearance? - If the individual concerned resides in another state, is the competent national authority allowed/obliged to seek assistance from the competent authority of the state of residence? - Is there an inter-departmental administration that centralises requests (military and non-military personnel)? - Which department is responsible for delivering the request? - What are the procedures for an individual to apply for clearance, and what are the subsequent phases, from the applicant's point of view, in obtaining security clearance? - What are the controls and types of validation during the process (submission of application, transmission…)?

	COUNCIL DECISION	ITEMS TO CHECK
	Annex I para. 8-16	- What are the national procedures for security screening? - Are there any restrictions as to what kind of information can be obtained /looked for? - Are the following typical searches undertaken o Loyalty o Discretion o Integrity o Etc… - Is the outcome of the investigation classified? - What are the procedures in the case of adverse information coming to light? Feedback to the service or institution that made the request? - What are the procedures in the case of an appeal? With whom can the person lodge an appeal? - Can the appeal body change the decision of NSA on personnel security clearance? - Is there a difference in the length of period to be investigated for CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET?

	COUNCIL DECISION	ITEMS TO CHECK
	Annex I para. 26-28	- What are the rules on the length of validity of security clearance? - What are the procedures for managing personnel security clearance certificates? - Is an interview part of the screening process? - How are requests for clearance extensions/renewals managed? - Is clearance extended under simplified procedures? - Is security clearance extended by up to 5 years as of the date of the last investigation on which it was based? - Do the vetting authorities provide the extension/renewal certificates in time? - Could the PSC be extended even if the security investigation has not been completed? If so, for what period? - How are records concerning security clearance managed? - Who is responsible for the central record? - Where is the central record located? - Are the records protected? - What are the procedures when the data subject has left the service: retirement,

	COUNCIL DECISION	ITEMS TO CHECK
		transfer, etc.? - Are there any exemptions from the PSC requirement? - Are exempt individuals briefed?
2.2.3 SECURITY EDUCATION AND AWARENESS	Annex I para. 29-31	- Is there a Security training programme on managing classified information and follow up of training courses (frequency, content)? - Are cleared personnel briefed on initial assignment and on departure from locations processing classified information? Are individual records kept of the security training attended by staff and is some form of 'certificate' issued? - Are cleared personnel briefed regularly at intervals not exceeding 12 months on the obligations regarding the protection of classified information? - Are personnel obliged to acknowledge their obligations in writing? - Is there a security education / awareness programme (films, posters, security warnings, advertising about the risk of loss or compromise of classified information)?

	COUNCIL DECISION	ITEMS TO CHECK
		- Does the security programme specifically address intelligence-related and other threats? - Is there an obligation to report potential foreign intelligence approaches? - Are there procedures to inform persons with access to RESTREINT UE/EU RESTRICTED information about appropriate security regulations and the consequences of negligence? - Is there an active training programme including general regulations and their specific application to local conditions - Are there specific rules concerning private travel?
2.2.4 EXCEPTIONAL CIRCUMSTANCES	Annex I para. 32-40	- Is there a procedure for temporary access to classified information without a PSC? - Is it one-time access or it can be repeated? - What is the period and the level of classified information that can be accessed? - Are the individuals briefed on their obligations? Do they acknowledge it in writing? - Is there a procedure for temporary access to information classified at a higher level than the level of the PSC?

	COUNCIL DECISION	ITEMS TO CHECK
		Which level?
2.2.5 POTENTIAL ACCESS TO EUCI	Annex I para. 43-44	- Are guards, couriers, escorts cleared or screened? - Are they briefed on security procedures for protecting EUCI?
2.2.6 WITHDRAWAL OF A PSC	Annex I para. 22-24	- If there is a break between the beginning of the service and notification of the security investigation outcome, or in individual's service, is the NSA contacted to confirm the validity of the outcome? - What are the procedures to withdraw clearance in the case of security problems? - Can the individual concerned appeal against the withdrawal?
2.2.7 ATTENDANCE AT MEETINGS IN THE COUNCIL	Annex I para. 41-42	- Is there a procedure on participating in classified meetings?

SECTION 3 PHYSICAL SECURITY

3.1 INTRODUCTION

The main objective of physical security measures is to prevent an unauthorised person from gaining access to EU classified information and/or material. Physical security measures must be designed to protect all premises, areas, buildings, offices, rooms, communication and information systems, etc. in which EU classified information and material is stored, handled and discussed.
The Council's security rules (Council Decision 2011/292/EU of 31 March 2011) define physically protected areas and contain general requirements for security approved equipment and intrusion detection devices as well as for the control of keys and combinations.
Guidelines on technical specifications of equipment to be used for the physical protection of EUCI contain specifications for security containers, locks, approved equipment and intrusion detection devices as well as for the control of keys and combinations.

3.2 PHYSICALLY PROTECTED AREAS

3.2.1. SECURED AREAS (INCLUDING TECHNICALLY SECURED AREAS)

A Secured Area is an area where a visibly defined and protected perimeter is established through which all entry and exit are controlled by means of a pass or personal recognition system. Unescorted access is granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know; all other individuals must be escorted at all times or be subject to equivalent controls.

Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, additional requirements must apply, such as the level of highest security classification of the information normally held in the area must be clearly indicated and all visitors are required to have specific authorisation to enter the area, will be escorted at all times and will be appropriately security cleared.

Secured Areas protected against eavesdropping will be designated as technically Secured Areas. Additional requirements must apply: such areas must be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys must be controlled in accordance with section VI of Annex II to the Council's security rules; all persons and material entering such areas must be controlled; such areas must be regularly physically and/or technically inspected as required by the competent security authority. Such inspections must also be conducted following any unauthorised entry or suspicion of such entry; and such areas must be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

3.2.2 ADMINISTRATIVE AREAS

An Administrative Area is an area where a visibly defined perimeter is established which allows individuals and, where possible, vehicles to be checked. Unescorted access may be granted only to individuals who are duly authorised by the competent authority, and all other individuals must be escorted at all times or be subject to equivalent controls.

3.3 PRACTICAL GUIDELINES FOR PHYSICAL SECURITY INSPECTIONS

	COUNCIL DECISION	ITEMS TO CHECK
3.3.1 PHYSICAL SECURITY REQUIREMENTS AND MEASURES	Annex II para. 3-7	- Is the documentation provided on the protection of the facilities in accordance with the layout of the facilities and the procedures in place? - Are all these measures applied? - Identify specific areas that require further investigation. - Check for the existence of comprehensive threat assessments and procedures and check whether they are updated regularly. - What are the specifications of the secure storage facilities. - Are the national storage requirements for classified information complied with? - Is there a certification system?

	COUNCIL DECISION	ITEMS TO CHECK
		- Give construction details for o Walls o Floor o Ceilings o large openings. - Is there a special form or logbook to record each technical intervention on strong rooms? - Are physical security measures at perimeters satisfactory? - Is there a PIDS or IDS used to assist security staff? - What is the security level of the automated access control system (**EN50133** norm)? Security of the card? Quality of the reader? Power back-up? - Is there a guard patrol? - To what level are security guards cleared? - Do the guards have written instructions? - How are they supervised and controlled? - CCTV installation (**EN50132** norm)? - Is an alarm system used? - Is there a norm for the alarm system? - What is the security level of the alarm system (**EN50131** norm)? Make? Type

	COUNCIL DECISION	ITEMS TO CHECK
		of detectors? Access to keypad? Power backup? Fault checks? Alarm transmission? Alarm reaction? - What are the means of communication in the event of an emergency? - Is there a rapid reaction force in the event of an alarm? - What is its response time? - What are the procedures to activate and deactivate the security devices? - Are there zones without lighting? - Are the lights in the building in the event of an emergency - Are there standards for physical barriers? - Surrounding walls (what are they made of?) - What are the characteristics of doors (**EN1627** norm for burglary resistance)? - Windows (**EN356** norm for burglary resistance)? - Are the physical measures implemented in accordance with the nature and the location of the premises?

	COUNCIL DECISION	ITEMS TO CHECK
3.3.2 PHYSICALLY PROTECTED AREAS	Annex II para. 12-22	Separation between outside open zone and administrative zone. - Are there norms and/or criteria to establish different levels of access to areas? - What is the quality of the materials used and their state? - Will fences, doors, windows and walls adequately resist unauthorised intrusion? For how long? - Is there a zoning system consistent with that defined in the Council's security rules? - Do the types of security zone correspond to the type of information to be protected? - Are there any provisions for technically Secured Areas? - Are the perimeters of the security zones clearly defined? - Are documents in the personal possession of cleared staff stored and managed in accordance with established regulations?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are there security checks at the end of the working day for areas where classified documents are stored or processed? - Is there a special security form for this? - Are there access controls for secured areas where classified information is stored? - Check the access procedures relating to personnel not permanently working in the Secured Area. - Check the access procedures relating to visitors. - Is there an access control system for visitors? - Check the access procedures relating to cleaning and maintenance personnel - Is there a system for controlling and/or supervising cleaning and maintenance personnel? - Are checks carried out on security containers, safes and rooms during off-duty hours, including holidays and weekends? - What are the alert procedures? - Are there regular exercises? - Are there provisions for protection from overlooking and eavesdropping?

	COUNCIL DECISION	ITEMS TO CHECK
		- What are the types of area and protection? - When was the last inspection? - How is the area controlled (access – alarm)? - Have telecom lines been installed? - Are there special rooms for copiers and telefax machines?
3.3.3 PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI	Annex II para. 23-29	
3.3.4 CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI	Annex II para. 30-31	- What is the quality of locks? (EN1300 norm for High security locks – EN 1303 for standard cylinders) - Is there a key and combination management system? - Will combinations be changed at least every 12 months or when there is a change in personnel knowing the combination? - Are keys and combinations adequately protected from unauthorised appropriation/disclosure? - What type of cabinet/protection? - How are locks managed? - What is the procedure for handling spare keys and combination backups?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are there spare keys and combinations and are they kept in appropriately secure locations? - Are there approved construction specifications for containers? - Do safes conform with the EN1143 norm? - Is there a special form or logbook to record each technical intervention on a safe or container?

SECTION 4 MANAGEMENT OF CLASSIFIED INFORMATION

4.1 INTRODUCTION

The Council's security rules lay down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter, detect and recover from deliberate or accidental compromise or loss of such information.

4.2 PRACTICAL GUIDELINES FOR DOCUMENT SECURITY INSPECTION

	COUNCIL DECISION	ITEMS TO CHECK
4.2.1 CLASSIFICATION MANAGEMENT	Annex III para. 2-16	- What are the criteria for classifying information? - Are the markings/classifications comparable to those used in the EU? - Is there a table of equivalence with other countries? - Are all classified documents appropriately marked with a security classification? - Are security classifications correctly assigned? - What are the rules for producing classified documents? - What details must figure on classified documents? - What are the procedures for downgrading classified documents? - What are the procedures for declassifying classified documents?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are classified documents reclassified only with the consent of the originator or a releasing authority?
4.2.2 REGISTRATION OF EUCI FOR SECURITY PURPOSES	Annex III para. 17-24	- Is there a registry for classified documents? - Who is in charge of receiving and handling EU classified documents? - What are the registry procedures? - Is there a TRÈS SECRET UE/EU TOP SECRET registry? - Are all incoming EU classified documents centrally registered and immediately brought under registry control? - Does the Central Registry control all TRÈS SECRET UE/EU TOP SECRET documents that enter the organisation? - Can organisations receive such information from other sources? - What are the procedures for releasing EUCI to third States or international organisations? - Are records kept of any such release?

	COUNCIL DECISION	ITEMS TO CHECK
		- Is the Central Registry notified of all TRÈS SECRET UE/EU TOP SECRET information received from other sources? o Chronological number attributed to the document o Date of receipt o Originator's number o Identification of sender o Short title o Language o Level of classification o Number of pages of the document o Date of transmission o Number and distribution of the copies o Physical location of the document o Number of the receipt - What is the classification of the logbooks and/or index cards: CONFIDENTIEL EU/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET? - What are the procedures to prevent alteration of logbooks or index cards (entries in pencil unauthorised and illegible cancellations, etc.)? Do similar procedures also exist for classified documents registered electronically?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are logbooks properly protected (classification, storage,…)? - Are the pages of logbooks numbered and are the cards/hard copy controlled? - Which administration is in charge of storing classified documents (amount of EU classified documents, physical location,…)? - How is the storage of classified documents organised? - Is EUCI stored separately from national or other country's /organisation's classified information? - How many EU classified documents are held? - Are classified documents which are removed from storage kept under the constant control of duly authorised individuals? - What are the responsibilities of the Control Officer? - Does the Control Officer keep or have lists kept of individuals in the unit/organisation who are authorised access to TRÈS SECRET UE/EU TOP SECRET information? - Are the security clearances of all the authorised persons checked?

	COUNCIL DECISION	ITEMS TO CHECK
		- Is there a record of TRÈS SECRET UE/EU TOP SECRET documents that are handled and distributed? - Do disclosure sheets exist for TRÈS SECRET UE/EU TOP SECRET documents? Are they attached? - Are control numbers assigned to each TRÈS SECRET UE/EU TOP SECRET document? - Are there signed receipts for all movements of TRÈS SECRET UE/EU TOP SECRET documents? - Are the procedures for the initial receipt of TRÈS SECRET UE/EU TOP SECRET documents carried out only by the Control Officer or a duly authorised alternate? - Is the distribution and storage of TRÈS SECRET UE/EU TOP SECRET information kept to a minimum? - Are classified computer media included in the annual muster? - Are reports of annual musters of TRÈS SECRET UE/EU TOP SECRET documents submitted received correctly and on time? - Is TRÈS SECRET UE/EU TOP SECRET information transmitted exclusively via the TRÈS SECRET

	COUNCIL DECISION	ITEMS TO CHECK
		UE/EU TOP SECRET registry system? - Are TRÈS SECRET UE/EU TOP SECRET documents disseminated in accordance with listings of authorised recipients?
4.2.3 COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS	Annex III para. 25-27	- Is all reproduction equipment under appropriate control and is use restricted? - Is there a copy marking system on documents? - Are the regulations for producing copies, translations and extracts, microfilming, or scanning of documents correctly applied? - Are there lists of the classified documents which are reproduced? - Are the copies recorded? - Are there records of TRÈS SECRET UE/EU TOP SECRET documents which are reproduced? - Is the prior consent of the originator always sought for each reproduction of TRÈS SECRET UE/EU TOP SECRET documents?

	COUNCIL DECISION	ITEMS TO CHECK
4.2.4 CARRIAGE OF EUCI	Annex III 28-40	- Are packaging, integrity of the package,… inspected? - Is the contents, including markings/classifications examined? - Is the page count checked? - Who is authorised to sign receipts? - Is a disclosure record inserted when required? Records of this control - Are written acknowledgements of receipt up to date? - Are there lists of signature specimen of authorised individuals? Are the signatures on the receipts compared with them? - Are documents on receipts and destruction certificates properly identified? - What are the procedures to prevent alteration of or additions to receipts and destruction certificates? - Do you chase up any outstanding recipients? - Are lists and specimens kept of signatures of authorised individuals? - What are the distribution procedures? - Are records of documents distributed by the central registry? - What is the system for transporting

	COUNCIL DECISION	ITEMS TO CHECK
		classified documents inside and outside Secured Areas? - Are EU classified documents always distributed through the registry system? - Is there a classified courier system? - Are pouches and parcels for couriers properly prepared (double-cover, sealed, etc.)? - Are there instructions for the personal hand carriage of classified documents? - What are the procedures and rules for personal carriage of classified documents inside and outside Secured Areas? - Are the rules concerning the national and international transmission of classified documents known and complied with? - What are the procedures for organising meetings involving highly sensitivity issues (with regard to distribution)?

	COUNCIL DECISION	ITEMS TO CHECK
4.2.5 DESTRUCTION OF EUCI	Annex III para. 41-46	- What is the approved destruction method for: o Paper? o Microfilm? o Tapes? o CD-ROM? o HDD? o Electronic devices (e.g. crypto modules)? - Is there a systematic programme for the destruction of classified documents that are no longer required? - Are there norms for the destruction of classified documents? - Are there lists of destroyed documents? - Is the destruction of TRÈS SECRET UE/EU TOP SECRET documents carried out only by the Central Registry and in the presence of a witness cleared to the level TRÈS SECRET UE/EU TOP SECRET? - Are the destruction certificates of TOP SECRET documents duly signed?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are TRÈS SECRET UE/EU TOP SECRET destruction certificates, control records, external transfer receipts and disclosure records maintained for a minimum of ten years from the date of destruction or permanent external transfer? - Are classified working papers and drafts properly controlled? - Are TRÈS SECRET UE/EU TOP SECRET documents always returned to the Central Registry that holds them on charge for destruction? - Are documents classified SECRET UE/EU SECRET destroyed by the responsible registry in the presence of a witness cleared to at least the level SECRET UE/EU SECRET? - Are classified documents CONFIDENTIEL UE/EU CONFIDENTIAL destroyed by the responsible registry? - Are SECRET UE/EU SECRET and ONFIDENTIEL UE/EU CONFIDENTIAL destruction certificates kept for a minimum of 5 years?

	COUNCIL DECISION	ITEMS TO CHECK
4.2.6 CONTINGENCY PLANS	Article 5(3)	- Are there contingency plans? - Are there physical security measures for the protection of classified information during a local or national emergency? - Are users confident to follow the procedures in the case of fire, natural disaster or civil disturbance? - Do the instructions include anti-terrorist measures? - Are there instructions for the destruction, evacuation or special protection of national classified documents in the case of an emergency? - What are the procedures for emergency destruction? Are they exercised? - Are the instructions displayed? - Are there provisions for priority to be given to the destruction of crypto equipment in the case of an emergency? - What is the method for emergency physical destruction? - Is there emergency planning or similar procedures? - Are there contingency plans?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are there physical security measures for the protection of classified information during a local or national emergency? - Are users confident to follow the procedures in the case of fire, natural disaster or civil disturbance? - Do the instructions include anti-terrorist measures?
4.2.7 INSPECTIONS AND ASSESSMENT VISITS	Annex III para. 47-60	- Are there procedures for the internal control of information? - Is there an effective system for spot-checking TRÈS SECRET UE/EU TOP SECRET documents to ensure that they are accounted for? - Are the spot-checks conducted by independent officials? - Are records kept? - Are there national guidelines on how to make an inventory and check classified documents below TRÈS SECRET UE/EU TOP SECRET level? - How frequently are these inventories made? - Is an inventory planned every 12 months?

	COUNCIL DECISION	ITEMS TO CHECK
		- How and when are the annual findings transmitted to the Secretary-General of the Council? - Are there procedures to report breaches and/or compromise(s) of security? - What action is foreseen when a compromise of information is detected (investigation, penalties)? - Give the number of breaches during last year reported to NSA handled internally - Has there been any follow-up and/or corrective action? - Are records kept? If so, review the records. - What is the procedure for reporting security breaches (when applicable) to the Security Office of the General Secretariat of the Council? - What are the legal procedures for personnel involved in compromising classified information? - What are the procedures for organising inspections? - On what legal basis? - Who is responsible for the inspections?

	COUNCIL DECISION	ITEMS TO CHECK
		- When was the last inspection conducted? - Has corrective action been taken or initiated as required by previous reports?

SECTION 5 INDUSTRIAL SECURITY

5.1 INTRODUCTION

This chapter lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the GSC. Such contracts should not involve access to information classified "TRÈS SECRET UE/EU TOP SECRET".

5.2 PRACTICAL GUIDELINES FOR INDUSTRIAL SECURITY INSPECTION

	COUNCIL DECISION	ITEMS TO CHECK
5.2.1 SECURITY ELEMENTS IN A CLASSIFIED CONTRACT	Annex V para. 3-7	- Who is in charge of industrial security - the NSA, a DSA or another competent security authority? - Is there a SCG to help determine the classification of any information provided to bidders and contractors? - What principles are applied in order to determine the security classification of the various elements of a classified contract?
5.2.2 FACILITY SECURITY CLEARANCE (FSC)	Annex V para. 8-13	- What elements are evaluated and verified in order to issue an FSC? - How is the integrity of the entity evaluated? - How are ownership, control or the potential for undue influence evaluated?

	COUNCIL DECISION	ITEMS TO CHECK
		- Has the entity established a security system covering all appropriate measures necessary for the protection of information or material classified C-UE /EU-C or S-UE/EU-S? - Has the personnel security status of management, owners and employees been established? How? - Is there a Facility Security Officer responsible for enforcing the security obligations within the entity?
5.2.3 CLASSIFIED CONTRACTS AND SUB-CONTRACTS	Annex V para. 14-23	- If EUCI is provided to a bidder at the pre-contractual stage, is the bidder obliged to hold an FSC at that time? - Are bidders which fail to submit a bid or are not selected obliged to return all classified documents within a specific period of time? - Is all EUCI returned to the contracting party upon termination of the classified contract, or can the contractors/sub-contractors can retain it? - Does the contractor seek the prior written consent of the contracting authority before sub-contracting a part of the classified contract and providing EUCI?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are sub-contracts awarded to entities registered in a non-MS which has not concluded a security of information agreement with the EU? What about administrative arrangements? - How do contractors ensure that sub-contracting activities are undertaken in accordance wit the minimum standards laid down in CSR?
5.2.4 VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS	Annex V para. 24-26	- Are the visits arranged directly or in liaison with NSA/DSA? - Are records of all visitors kept? - What are the requirements for a visitor to access EUCI? - Does the visitor have access to all EUCI?
5.2.5 TRANSMISSION AND CARRIAGE OF EUCI	Annex V para. 27-28	- What are the procedures for carrying EUCI within and outside the entity?
5.2.6 TRANSPORT OF CLASSIFIED MATERIAL AS FREIGHT	Annex V para. 29	- What are the procedures for the transport of classified material as freight? - If a commercial courier for freight or a transport company is used for freight, are the companies obliged to provide a FSC, are their personnel cleared?

	COUNCIL DECISION	ITEMS TO CHECK
		- Are transportation plans drawn up by the consignor and approved by the NSA/DSA/ or another competent security authority?
5.2.7 TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES	Annex V para. 30	- What are the security measures for transferring EUCI to contractors/subcontractors located in third States? R-UE/EU-R, C-UE/EU-C, S-UE/EU-S?
5.2.8 HANDLING AND STORAGE OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED	Annex V para. 31-36	- What are security measures required for the handling and storage of EUCI at the level of "RESTREINT UE/EU RESTRICTED"? - Are there any measures to check the trustworthiness of the entity for a contract involving "RESTREINT UE-EU RESTRICTED"?

PART II INFORMATION ASSURANCE (IA)

SECTION 1 INTRODUCTION TO INFORMATION ASSURANCE INSPECTION PROCEDURES

The Information Assurance security inspection or review process is carried out to support a number of objectives, mainly to ensure that minimum standards exist and are consistent with Council Decision 2011/292/EU;
in particular:

- To verify that the authorities responsible in the field of IA are well defined and implemented;
- To identify the national IA risk management rules and procedures;
- To verify IA education and awareness programmes;
- To identify and inspect the points of presence of EU communication and information systems (CIS);
- To identify national CIS handling EUCI and inspect their accreditation status; and
- If necessary, to recommend changes.

The inspection checklist includes the following sections:

- General aspects, legal basis and organisation of IA;
- Security accreditation procedures;
- Network defence capabilities;
- CIS handling EUCI;
- CIS physical and personnel security;
- Security of electronic media;
- Emergency and Contingency Planning.

This document may only be regarded as being indicative. Every inspection/assessment visit requires prior tailoring.

0. REFERENCE TO PREVIOUS INSPECTION

	COUNCIL DECISION	ITEMS TO CHECK
		- Is the inspection a follow-up visit? - What are the major changes in the area of Information Assurance since the last inspection? - Have the recommendations made by the GSC during the last visit been taken up (if any, see inspection report)?

1. GENERAL

	COUNCIL DECISION	ITEMS TO CHECK
1.1 LEGAL BACKGROUND FOR EUCI PROTECTION		- What is the legal basis for protecting national CI in electronic form? - Are there specific rules for protecting EUCI in electronic form (such as regulations, directives, by-laws)? - Is there a supportive layer of IA policies and guidelines? - Which IA policies and guidelines from other sources (e.g. EU, NATO) have been adopted?

	COUNCIL DECISION	ITEMS TO CHECK
1.2 SECURITY AUTHORITIES	Article 10(8-9)	- Are the following authorities defined and designated? o Information Assurance Authority (IAA) o TEMPEST Authority (TA) o Crypto Approval Authority (CAA) o Crypto Distribution Authority (CDA) o Security Accreditation Authority (SAA, CIS-related) o Information Assurance Operational Authority (IAOpsA, CIS-related) - To whom do they report?
1.3 RISK MANAGEMENT/ACCREDITATION	Annex IV para. 47	- Is the security accreditation process defined and implemented for all CIS handling EUCI? - Have the latest versions of the SSRSs been approved by the SAA? - Are security accreditation strategies defined or any equivalent document setting out the degree of detail for the accreditation process commensurate with the required level of assurance? - Are the approval conditions for accreditation clearly defined? - Have the results of the risk assessment been reviewed by and

	COUNCIL DECISION	ITEMS TO CHECK
		agreed with the SAA? - Has the residual risk been clearly identified and documented, and agreed by both the Head of the organisation and the SAA?
	Article 5(1-2)	- Is a recognised risk methodology / tool used to assess the CIS risks?
	Annex IV para. 51	- Have System-specific Security Requirement Statements (SSRSs) (or national equivalent(s)) been drawn up for systems handling EUCI? - Are Security Operating Procedures (SecOPs) accessible by users, and security / system administrators?
		- Does the administration follow international standards? o ISO 2700x o Common Criteria o Others - Is an Information Security Management System (ISMS) defined and implemented? - Is the role of the risk owner defined and fulfilled?

	COUNCIL DECISION	ITEMS TO CHECK
		- Have users signed an acknowledgement of compliance with the SecOPs? - Are SecOPs up-to-date?
1.4 INFORMATION ASSURANCE AWARENESS	Annex IV para. 22	- Is there an education and awareness programme for o new entrants o improving the Information Assurance awareness of existing staff?
1.5 SECURITY INCIDENTS	Annex IV para. 47(d) Annex IV para. 16	- Do the SecOPs clearly state the procedures to be followed by the users on detection of an incident? - Do the SecOPs clearly state the procedures to be followed by the CIS IA Operational Authority, including reporting the incident to the relevant Authority?
1.6 NETWORK DEFENCE	Annex IV para. 16-17	- Does the country or international organisation have organisational entities responsible for network defence (cyber defence) issues? - Is there a governmental Computer Emergency Response Team (CERT) operational? - Does the CERT (or another entity) cooperate with the GSC?

2. EU CIS

	COUNCIL DECISION	ITEMS TO CHECK
2.1 EU CIS POINTS OF PRESENCE (POPS)		- Which EU CIS have PoPs in the country or in the international organisation? (MS: Capital and PermRep) o CORTESY? o EXTRANET-R? o FADO? - Are there additional means for exchanging EUCI with the GSC (Chiasmus, ACID, …)? - For each PoP: o Physical and personnel security? o Accreditation status (statement of compliance)? - Interconnections? Accreditation status (statement of compliance)?
2.2 NATIONAL CIS HANDLING EUCI		- Are there CIS handling EUCI in the country/organisation? If yes, specify the following: o classification level of EUCI o security mode of operation o need-to-know separation o interconnections

	COUNCIL DECISION	ITEMS TO CHECK
	Article 10(6-7)	- Do the cryptographic products that protect EUCI in national CIS have national approval and/or EU approval? - How is EUCI transmitted between the capital and the PermRep/Mission in Brussels? - Are all CIS handling EUCI accredited? - Is there a security policy on interconnection? - Are all interconnections with CIS handling EUCI accredited? Specify the accreditation strategies.
2.3 CRYPTOGRAPHIC SECURITY		(TECH-I-01) - Is cryptographic equipment and cryptographic keying material used in the organisation? - Is the key material handled and/or controlled by the organisation or by a third party? - Has the Crypto Custodian been appointed? - Is an inventory kept of all classified (crypto) items? - Are crypto devices properly secured (physical environment, anti-tampering measures, etc.)?

	COUNCIL DECISION	ITEMS TO CHECK
		- Have appropriate measures been put in place to separate EU from non-EU crypto devices?
2.4 BUSINESS CONTINUITY MANAGEMENT	Article 5(3-4)	- Has a Business Continuity Plan (BCP) been drawn up (based upon a risk assessment) and tested? - Has the BCP been reviewed and approved by senior management and the SAA? - Is the BCP implemented?
2.5 USE OF PORTABLE COMPUTING DEVICES		- Are there any restrictions/procedures regulating the use of portable devices? - Is the use of portable devices for processing EUCI on mission allowed in the relevant SSRS and SecOPs? - Are the users given "instructions for the use of portable devices on mission"? - May portable devices be used by visitors/contractors/staff of the organisation?
2.6 USE OF CELLULAR/MOBIL TELEPHONES IN THE ORGANISATION		- Are procedures in place for controlling the use of mobile phones in the organisation?
2.7 WORKING AT HOME AND REMOTE ACCESS		- Does the organisation require/allow staff to work at home or elsewhere using PCs / laptops with access to

	COUNCIL DECISION	ITEMS TO CHECK
		EUCI? - Are only the organisation's computers and the organisation's media provided for this purpose? - Can you provide details of the organisation's remote access policy?

3. CIS SECURITY ASPECTS (TO BE CHECKED FOR EVERY CIS HANDLING EUCI, AS APPROPRIATE)

	COUNCIL DECISION	ITEMS TO CHECK
3.1 PHYSICAL SECURITY		- Are there procedures for the physical security of CIS assets? - Is the physical perimeter containing the CIS well defined? - Is this perimeter entirely contained within a secured area? - If not, are the components/segments crossing uncontrolled areas appropriately protected?
3.2 MAIN COMPUTER ROOMS		- Are the servers, network management system, network controllers communications controllers contained within a separate computer room or in a separate secured rack?

	COUNCIL DECISION	ITEMS TO CHECK
	Annex II para. 12	- Are servers and communication infrastructures processing EU information physically separated from those processing non-EU information? - If required, is the Computer Room established as a Technically Secured Area? - Is access to the room controlled by an approved device (e.g. combination lock or other access control device such as a proximity badge)? - Is access to the Computer Room limited to only authorised persons (including outside normal working hours)? - Have intrusion detection alarms been installed?
3.3 EMISSION SECURITY		
	Article 10(5)	- Is the CIS (or any part of it) located outside the EU? - Does the CIS (or any part of it) consist of transportable equipment? (Transportable equipment more than 60 days at one location is considered to be a fixed and must be treated accordingly)

	COUNCIL DECISION	ITEMS TO CHECK
		(IASG 4-02) - Has TEMPEST Zoning according to the Information Assurance security guidelines IASG 4-02 (TEMPEST Zoning Procedures) been undertaken in the organisation? - Was the facility zoning done by measurement or based on the shortest distance between the facility where the classified information is processed and the Inspectable Space perimeter? (IASG 4-01) - Do the zone levels of equipment installed in the CIS match the facility zone levels according to IASG 4-01 (Selection and Installation of TEMPEST Equipment, details are classified)? - Was all equipment installed in the CIS certified and zoned by the TA? - Is the TEMPEST equipment serviced and maintained by a TA approved method and/or by a TA certified company? - Is a Faraday Cage used? If yes, was it accredited by the TA? - Do the procedures for the installation of CIS equipment refer to IASG-04-

	COUNCIL DECISION	ITEMS TO CHECK
		01?
3.4 INTERNAL ENVIRONMENTAL CONTROLS		- Has a smoke / fire detection system been installed? - Has an air conditioning system been installed? - Have temperature / humidity controls been installed? - Have water sensors been installed?
3.5 EXTERNAL ENVIRONMENTAL CONTROLS		- Is the CIS operated in a building shared with other organisations/entities? If yes, specify? - Distance from nearest building
3.6 OFFICE AREAS		- If required, are any office areas established as secured areas? - Are procedures in place for access control?
3.7 CIS EQUIPMENT		- Is there an updated inventory of CIS equipment? - Are seals used to detect tampering attempts? - How are security seals managed? - Are any physical checks for tampering carried out on equipment? - How frequently are such checks performed?

	COUNCIL DECISION	ITEMS TO CHECK
3.8 INTRUDER AND ENVIRONMENTAL ALARMS		- Do intrusion and environmental alarms exist? - Do the security instructions clearly state the regime for testing alarms (the frequency of tests, the procedures for setting alarms, and the procedures for reacting to an alarm)? - Are the alarms tested regularly? - If the local security environment of the CIS is shared with other organisations/entities, which controls are in place to ensure separation?
3.9 CIS PERSONAL SECURITY		- Are there procedures on personnel security aspects of the CIS (e.g. clearances required for users/administrators)? - Are there procedures for handling visitors? - Are all personnel with authorised access to the Computer Room and associated areas cleared to (at least) the highest classification level of EU information handled? - Are security and system administrators appropriately cleared? - Is all staff (including contract staff) associated with hardware and software maintenance cleared to (at least) the highest classification level

	COUNCIL DECISION	ITEMS TO CHECK
		of EU information handled? - Is there an up-to-date list of personnel with authorised access to the Computer Room and associated areas? - Does an appropriate member of the senior management of the organisation sign off this list? - Is a list kept of personnel with authorised access to the CIS? - Are procedures clearly established for controlling ancillary staff (cleaners / maintenance staff) requiring access to the Computer Room and associated areas?
3.10 MEDIA SECURITY		- Are backup magnetic tape cartridges / cassettes / diskettes / CDs / USB keys correctly labelled with the highest classification they (may) carry? - Are backups stored in appropriate containers according to the highest classification they (may) carry? - Are server(s) labelled to indicate the highest classification of EU information handled? - Are workstations labelled to indicate the highest classification of EU information that may be processed?

	COUNCIL DECISION	ITEMS TO CHECK
		- Do security registration procedures apply to media storing EUCI? - Are the procedures for the off-line (air gap) transfer of information to/from the CIS documented? (IASG BP-09) - Are there procedures on the reuse, downgrading and declassification of media?
3.11 IDENTIFICATION AND AUTHENTICATION		- What identification and authentication mechanism is used for the CIS? - Are user-IDs individually assigned and the procedures for their assignment clearly documented? - Are procedures for deleting accounts (on departure of personnel from posts) clearly documented? - For CIS processing information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above: Do the identification and authentication services rely on stronger means like SMARTCARDS with cryptographic coprocessors?

	COUNCIL DECISION	ITEMS TO CHECK
3.12 ACCESS CONTROL		- Are access control mechanisms implemented to apply the "need-to-know" principle for controlling access to EU information? - Are the mechanisms for establishing user rights and permissions clearly documented in the SecOPs? - Do the access control mechanisms permit discretionary access to directories and files?
3.13 OBJECT REUSE		- Could the workstations retain sensitive data (e.g. temporary files on hard disk)? - Do the printers retain the images of the last printed files? - Do the printers have a "reprint" facility?
3.14 REGISTRATION OF CLASSIFIED INFORMATION		- Does the CIS allow classified information to be printed? - How it is ensured that any classified data is printed in compliance with the security registration rules?
3.15 AUDIT AND ACCOUNTABILITY		- Are audit logs kept for at least the following events: o successful / failed logon and logoff, o failed attempts to access files, o successful / failed changes to

	COUNCIL DECISION	ITEMS TO CHECK
		user / system privileges, o successful / failed system and security management activities? - Are failed activities investigated by the security administrator?
3.16 USE OF SECURITY MANAGEMENT TOOLS		- If Security Management Tools such as a Security Information and Event Manager (SIEM) or Intrusion Detection System (IDS) are used, describe which and for what purpose, e.g.: o audit analysis, o intrusion detection.
3.17 COMPUTER VIRUS/MALICIOUS CODE PROTECTION		- Have procedures been clearly documented for checking installed operating system software, software packages and utility programs for the presence of computer viruses and other malicious software? - Is virus / malicious code detection software installed on all boundary protection devices, servers and workstations? - Is it configured to automatically check on start-up of the system? - Is virus / malicious code detection software installed on a stand-alone (quarantine) PC?

	COUNCIL DECISION	ITEMS TO CHECK
		- Is the software regularly updated (e.g. with the latest available software engine and latest known virus patterns downloaded from the software vendor's web site)?
3.18 HARDWARE AND SOFTWARE MAINTENANCE		- What are the protective measures against unauthorised modifications of software and hardware? - Is there any need to monitor software/hardware utilisation level or any procedures preventing saturation? - Have procedures for the identification, storage and control of security-related spare parts been documented?