DOCUMENT XVIII:

GUIDANCE ON THE HAND CARRIAGE OF PORTABLE CIS FOR THE TRANSPORTATION OF CLASSIFIED INFORMATION AT RESTRICTED LEVEL

Further advice on this document may be obtained from the respective NSA/DSA

CLASSIFICATION LEVEL

RECORD OF CHANGES		
Date	*Issue*	*Changes*
03.10.2011	V 2.0	Approved version
15.06.2011	V 1.2	
01.03.2011	V 1.1	

DISTRIBUTION RECORD		
Organization / Company	*Name*	*Via*

INDEX

1. DEFINITIONS AND ACRONYMS 3
2. REFERENCES 3
3. INTRODUCTION 3
4. SCOPE 4
5. PRINCIPLES 5
6. CARRIAGE OF PORTABLE CIS CONTAINING INFORMATION AT RESTRICTED LEVEL 6
ANNEX A: AUTHORIZATION FOR CARRIAGE OF PORTABLE CIS 7

1. DEFINITIONS AND ACRONYMS

CIS: Communication and Information Systems.

Cryptographic algorithm: A mathematical function and its associated set of relevant security parameters.

Cryptographic equipment: A product that embodies a cryptographic mechanism that is specifically required to enhance security.

Cryptographic key: A sequence of random or pseudo-random bits used initially to set up and periodically change the operations performed in cryptographic equipment. Examples of cryptographic key are key for the purpose of encrypting or decrypting electronic signals, or for determining transmission security patterns, or for producing other key.

Cryptographic material: Material, including key, publications, devices, or equipment, which contains crypto information and is essential to the encryption, decryption or authentication of telecommunications.

Cyber security: Measures taken to protect a computer or computer system against unauthorized access or attack.

NCSA: National Communication Security Authority

Portable CIS: For the purpose of this guidance, portable CIS are any handheld devices, generally laptops, but also other devices such as pen-drives, CDs/DVDs, memory cards, etc. Portable CIS may be distinguished based on their nature as proper CIS (laptops, PDAs, smart-phones) or as storage devices (either magnetic or optical).

2. REFERENCES

1. **CE 428/2009 Regulation** (5 May 2009)**,** setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

3. INTRODUCTION

The availability of information between participants in a classified programme or contract is a key objective with critical implications not only for security but also for the development plan and cost-effectiveness of the classified programme or contract.

For the above-mentioned reasons, availability requires a continuous improvement on the flow/distribution channels and means of transport with the aim of reducing the time the people with a need-to-know should wait to be able to access the information they need.

From a security point of view, both the flow/distribution channels and the transport of information are every day issues which pose a challenge for those whose responsibility is to, as far as possible, ensure a reasonable level of protection of classified information.

Experience has shown that the flow/transport/transfer of information using portable CIS is not only part of the future but also of the present and it is therefore urgent and necessary to provide some guidance to ensure that such means of communication is secure.

To obtain a reasonable level of protection of classified information stored or carried in portable CIS, it is necessary to consider the following statements:

- Portable CIS are extremely vulnerable to theft during carriage and this constitutes a considerable risk to the classified information stored in them.

- Hand carriage of portable CIS permits the information to be available in a reasonable timeframe, thus avoiding delays and extra costs caused by the use of government-to-government channels.

From a risk analysis viewpoint, in order to decrease the residual risk produced as a consequence of the above statements, it is necessary to define precisely the safeguards and conditions under which this method of transport can be used.

This document provides:

a. Principles for the transport and the use of portable CIS containing classified information at RESTRICTED level, outside the regular security areas.

b. Guidance for the employee/courier if stopped by custom officials or any other persons in authority who may request access to the data contained in the portable CIS.

This guidance may be incorporated into national security laws and regulations which, if required, may be more stringent.

4. SCOPE

The following guidance applies only to transport of CIS containing information at RESTRICTED level. For the CONFIDENTIAL and SECRET levels another LOI SC3 document will apply.

5. PRINCIPLES

To avoid potential security incidents and possible compromise where ever possible classified information at the level of RESTRICTED should be sent in advance through appropriate secure channels

However, where advance transmission is not possible and hand carriage of the RESTRICTED information on portable CIS is necessary, national rules and regulations should reflect that the carriage of portable CIS is only to be undertaken in exceptionally urgent circumstances when the classified information contained on the portable device is essential to be accessed away from the parent facility.

Prior to transporting portable CIS containing information at RESTRICTED level across international borders, the existence of a signed Bilateral Security Agreement and the relevant provisions of the security regulations of the country to be visited should be taken into account.

The classified information contained should be limited to what is necessary to accomplish the mission.

Portable CIS containing information at RESTRICTED level, to be transported across international borders should be encrypted with an encryption product approved by the relevant NSA/DSA. It can only be stored in locked rooms or containers (cabinets, desks etc.). During travel, such material should not be handled in a manner that could result in unauthorised access or an insight into the information at RESTRICTED level such as in trains, planes or in other public areas.

Such portable CIS should be retained at all times under the control of the employee/ courier and should never at any time be left unattended in any public location, or in a hotel room. The risk of opportunistic theft from vehicles, even from locked boots, requires that portable CIS, simply as attractive items, should never be left unattended in such places.

Those portable CIS used to carry RESTRICTED information should:

- have a configuration so as to withstand hacking tentative and data thief
- have their data link disabled (Bluetooth, Wifi…)
- have a firewall
- use an account with limited privilege
- have the latest version of software (with all security patch.)
- not allow automatic execution of removable media (CD-ROM, USB keys..)

In addition, the portable CIS should provide a means to erase data in a secure manner.

6. CARRIAGE OF PORTABLE CIS CONTAINING INFORMATION AT RESTRICTED LEVEL

The Carriage of portable CIS containing RESTRICTED information will be submitted to authorization by the competent Authority. The template to issue such an Authorisation is at ANNEX A. This authorisation when signed by the relevant competent Authority will replace a courier certificate.

Personnel should be aware that during the international transport of portable CIS, the device or media is liable to be technically scanned by Customs personnel to assure that no illicit material is being transported. Therefore, a minimalist solution should always be preferred (e.g. CD/DVD instead of laptop). In the event that a Customs official requests access to the data contained in the portable CIS the bearer is to provide the Authorisation for the Carriage of Portable CIS at ANNEX A, and request, that should further inspection be required, that the matter be first referred to an appropriately security cleared Investigation Officer.

Every effort should be made to ensure that the CIS device is not removed from the bearer's personal possession whilst it is in an operational state and they should not allow a full examination of the contents of the portable CIS device. If the official takes the device from the bearer whilst it is in an operational state or wishes to impound the device, the bearer should request that they be permitted to immediately contact their Embassy for advice and seek their assistance. The bearer should also inform the Departmental/Company Security Officer of the incident as soon as possible.

All personnel transporting portable CIS containing classified information at RESTRICTED level should be informed of, and acknowledge their understanding of their responsibilities for protecting the information.

ANNEX A: AUTHORIZATION FOR CARRIAGE OF PORTABLE CIS

INSERT APPROPRIATE EMBLEM

[INSERT COUNTRY]

FOR THE ATTENTION OF: Customs Authorities, Border Police etc.

References:

A. CE regulation Nr 428/2009

It is hereby certified that the following officer ("The Bearer") is an employee of <insert name of company/government> and is authorized by the NSA/DSA of [Insert country] to carry Official portable CIS equipments and associated media.

Name		Title		Appointment	
Passport Number		Visa Number			

AUTHORISED EQUIPMENTS

This authorization applies to the following equipments, which are declared to be containing information which is the property of [Insert Country]

Unit Type	Make	Model	Serial Number
Portable Computer			
Removable Hard Disc			
Portable Printer			
CD/DVD - Memory Stick - Memory Card			
Other Peripherals and removable media			

SECURITY APPROVAL

This authorization permits the transport and the use of the equipments at up to RESTRICTED level, in accordance with the national Policy of [Insert Country].

In accordance with Reference A, it is declared that any encryption technology used within these equipments is intended for the personal use of the Bearer. Exemption from any Government control is therefore claimed.

.Return of Equipment to [Insert country]

It has been agreed with the Customs authority in [Insert country] that should a Customs Officer at port of entry declare a requirement to scan the media associated with these Portable CIS, the Bearer is to direct that the matter must be referred to an appropriately cleared Investigation Officer, who should be contacted through:

[Insert POC details of home Customs authority]

Should you require any further information, please contact the undersigned:

AUTHORISING SECURITY OFFICER (to be completed by the security officer of the courier)

Signature:			
Name:		Tel:	
Name of company:		Fax:	

AUTHORISING NSA (to be completed by the security officer of the courier if required by the laws and regulations of the country of departure)

Name/position/signature

Stamp

Date : the xx