NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

25 November 2020

DOCUMENT
AC/35-D/2002-REV5

SECURITY COMMITTEE

DIRECTIVE ON THE SECURITY OF NATO CLASSIFIED INFORMATION

Note by the Acting Chair

1. At Annex is the fifth revision of the Directive on the Security of NATO Classified Information which is published in support of the Security Within the North Atlantic Treaty Organization, C-M(2002)49-REV1. It is binding and mandatory in nature. This document replaces AC/35-D/2002-REV4 which should be destroyed.

2. The revision is a result of the Comprehensive Review of NATO Security Policy (AC/35-N(2015)0025-AS1, dated 21 December 2015).

3. This document has been approved by the Security Committee (AC/35-N(2020)0004-AS1, dated 4 November 2020) and will be subject to periodic review.

(Signed) Marco Criscuolo

Annex 1

Action Officer: M. Rožaj, NOS (Ext. 4084)
Original: English

ANNEX 1
AC/35-D/2002-REV5

DIRECTIVE ON THE SECURITY OF NATO CLASSIFIED INFORMATION
TABLE OF CONTENTS

INTRODUCTION 3
NATO SECURITY CLASSIFICATIONS, SPECIAL DESIGNATORS, MARKINGS AND GENERAL PRINCIPLES 3
The Aggregation Principle 5
Changing NATO Security Classifications or Declassifying NATO Classified Information 5
CONTROL AND HANDLING 6
The Registry System 6
Registry System Handling 6
Information Classified COSMIC TOP SECRET 6
Information Classified NATO SECRET 8
Information Classified NATO CONFIDENTIAL and NATO RESTRICTED 8
STORAGE 8
REPRODUCTIONS, EXTRACTS AND TRANSLATIONS 8
DISSEMINATION AND TRANSFER 10
Dissemination 10
Transfer 10
Hand carriage 11
Couriers / Guards / Escorts 11
Transfer within NATO Nation's or NATO Civil or Military body's Sites or Establishments 11
Transfer outside Sites or Establishments within a NATO Nation 11
Transfer between the territories of NATO Nations 12
Transfer outside the territory of NATO Nations 14
Dissemination and Transmission by means of CIS 14
RECEIPTS AND RECORDS 14
DISPOSAL AND DESTRUCTION 15
Destruction 15
Security Incident 16
Security Breach 16
Compromise 17
Infraction 17
Action Upon Discovery of a Security Breach or Infraction 17

Reporting of Compromises 18

Records of Security Breaches 19

Relief from Continued Accountability for Lost Accountable Documents 19

Action by the Originating NATO Civil or Military body 19

Action by the NATO Office of Security 19

Action by the Secretary General of NATO 19

COURIER CERTIFICATE 20

INSTRUCTIONS FOR THE COURIER 21

The following Appendices to this Directive address the specific procedures, arrangements, and sample documents:

(a) APPENDIX 1 – Courier Certificate

(b) APPENDIX 2 – Instructions for the Courier for the hand carriage of NATO Classified Information

INTRODUCTION

1. This Directive on the Security of NATO Classified Information is published by the Security Committee (AC/35) in support of Enclosure "E" to C-M(2002)49. This Directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This Directive addresses the following aspects in relation to NATO Classified Information:

(a) security classifications and markings;

(b) control and handling;

(c) storage;

(d) reproductions, extracts and translations;

(e) dissemination and transfer;

(f) receipts and records;

(g) disposal and destruction; and

(h) security incidents.

NATO SECURITY CLASSIFICATIONS, SPECIAL DESIGNATORS, MARKINGS AND GENERAL PRINCIPLES

2. NATO security classifications indicate the sensitivity of NATO Classified Information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure. NATO security classifications and their significance are:

(a) COSMIC TOP SECRET (CTS)
unauthorised access or disclosure would result in exceptionally grave damage to NATO;

(b) NATO SECRET (NS)
unauthorised access or disclosure would result in grave damage to NATO;

(c) NATO CONFIDENTIAL (NC)
unauthorised access or disclosure would be damaging to NATO; and

(d) NATO RESTRICTED (NR)
unauthorised access or disclosure would be detrimental to the interests or effectiveness of NATO.

3. Detailed guidance for the originator of NATO Classified Information on how to determine the appropriate NATO security classification based upon the correlation of "impacts of compromise" to NATO security classification levels for various subject areas can be found at Appendix 1 to Annex 1 of the Guidelines on the Security of NATO Classified Information (AC/35-D/1032).

4. NATO UNCLASSIFIED information and Information releasable to the Public shall be protected and handled in accordance with the NATO Information Management Policy (C- M(2007)0118) and The Management of Non-Classified NATO Information (C-M(2002)60).

5. Any national classified information that is received by NATO will be protected in accordance with NATO Security Policy at the appropriate level reflected within the table of national equivalencies that can be found at Annex 1 of the NATO Security Classifications with their National Equivalents (AC/35-D/1002).

6. Special category designators are applicable to specifically identified NATO Classified Information that is deemed to require an additional or enhanced categorization as follows:

(a) "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39) and the supporting Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co- operation Regarding ATOMAL Information (C-M(68)41);

(b) "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO (C-M(71)27(Revised));

(c) “CRYPTO” is a marking and a special category designator identifying all communications security (COMSEC) keying material used to protect or authenticate telecommunications carrying NATO cryptographic security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security policies and directives (SDIP-31/2 and SDIP-293/1);

(d) “BOHEMIA” is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA shall be protected in strict accordance with NATO Signals Intelligence Policy (MC 101) and its companion Allied Joint Publication (AJP) which covers doctrinal and procedural issues.

7. NATO Nations and NATO Civil and Military bodies shall introduce measures to ensure that NATO Classified Information created by, or provided to NATO is assigned the correct NATO security classification. For NATO Civil and Military bodies, these measures shall include:

(a) restricting the authority to decide on a NATO security classification for information at the level of NS and above to a limited number of designated posts;

(b) limiting the information that requires a NATO security classification, and encouraging the placing of more sensitive information into appendices to texts so that the main text can be distributed more widely, with less stringent security measures;

(c) emphasising that documents should be given a NATO security classification based on the information contained therein, which may be different from the classification of the documents to which they are attached, refer or respond; and

(d) emphasizing the need for the review of NATO Classified Information for the purpose of downgrading or declassification, when appropriate.

8. Originators are encouraged to re-assess classification levels at five year intervals with a view to downgrading, declassifying and eventual public disclosure. In all cases, NATO Classified Information will be subject to review for declassification and public disclosure after 30 years (50 years for Intelligence and Nuclear Information) in accordance with the Policy for the Public Disclosure of NATO Information (C-M(2008)0116).

9. Each NATO Civil or Military body shall establish a system to ensure that information classified CTS which it has originated is reviewed no less frequently than once every five years and information classified NS no less frequently than once every 10 years in order to ascertain whether

or not the existing security classification remains valid. Such a review is not necessary in those instances where the originator has predetermined that specific NATO Classified Information shall be automatically downgraded after a predetermined period and the information has been so marked.

10. The overall NATO security classification of a document shall be at least as high as that of its most highly classified component. Covering documents shall be marked with the overall NATO security classification of the information to which they are attached. When covering documents are used they shall contain a statement clearly identifying their NATO security classification or marking when separated from the attachments and shall be protected accordingly.

11. Where possible, component parts like paragraphs, enclosures, annexes etc. of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination.

12. The top and bottom of each page of a document shall be marked with the overall NATO security classification of the document. Individual annexes/appendices/attachments/enclosures may be marked at a level lower than the overall NATO security classification of the document.

13. Cases of apparent over-classification or under-classification shall be brought to the attention of the originator by the recipient. If the originator changes the NATO security classification of the document, they shall inform all recipients in writing.

14. As an additional marking to further limit the dissemination of NATO Classified Information, a Dissemination Limitation Marking may be applied by the originator. Such Administrative or Dissemination Limitation markings are intended to clearly identify the type of information contained therein and the need for limitations to be placed upon access to this information.

The Aggregation Principle

15. When a large amount of NATO Classified Information is collated together, the original security classification markings must be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Changing NATO Security Classifications or Declassifying NATO Classified Information

16. NATO Classified Information may be either upgraded, downgraded or ultimately declassified only by, or with the written consent of, the originator. In cases where the originator cannot be determined, the successor organization or higher authority shall assume the responsibility of the originator. In all such cases, changes in the NATO security classification or any declassification may only occur after the NATO Nations or NATO Civil or Military bodies that have been affected by the subject matter have been consulted.

17. When classified information originating from a NATO Nation(s) or a NATO Civil or Military body(s) is collated into a new product, that information shall not be downgraded or declassified without the written consent of the originator.

18. The originator, or if the originator cannot be determined, the successor organization or higher authority, shall be responsible for ensuring that recipients are promptly notified in writing when

the NATO security classification level of accountable information[1] is changed or the information is declassified.

CONTROL AND HANDLING

The Registry System

19. There shall be a Registry System for the receipt, accounting, handling, distribution and destruction of accountable information[2]. The procedures and requirements of the registry system apply equally across both the physical and electronic domains. Additional details and requirements concerning the electronic domain can be found in Enclosure "F" and its supporting directives, namely: Primary Directive on CIS Security (AC/35-D/2004) and Management Directive on CIS Security (AC/35-D/2005). This requirement may be fulfilled either within a single registry system, in which case strict compartmentalisation of information classified CTS shall be maintained at all times, or by establishing separate registries and control points.

(a) each NATO Nation or NATO Civil or Military body, as appropriate, shall establish a Central Registry for information classified CTS, which acts as the main receiving and dispatching authority for the nation or body within which it has been established. If there is a legitimate reason, a Nation may expand the number of Central Registries (e.g. one for military and one for civilian sphere) however their number shall be kept to a strict minimum. Central Registries may also act as registries for other accountable information;

(b) registries and control points shall act as the responsible organization for the internal distribution of information classified CTS and NS and for keeping records of each document held in that registry's or control point's charge; they may be established at ministry, department, or command levels.

20. Registry personnel handling national classified information in NATO Nations may, if properly cleared and briefed for access to NATO Classified Information, also be responsible for NATO Classified Information.

Registry System Handling

Information Classified COSMIC TOP SECRET

21. Information classified CTS consigned to an addressee in another NATO Nation or NATO Civil or Military body may only be transmitted direct from one registry or control point to another when authorised by the appropriate authority of the NATO Nation or NATO Civil or Military body.

22. Regardless of the type of registry organization, those registries that handle information classified CTS shall ensure that a COSMIC Control Officer (CCO) is appointed and that the CCOs are designated as appropriate to the composition and requirements of the Registry. A Deputy COSMIC Control Officer (DCCO) may perform some of the duties of the CCO and shall assume all authority and responsibility during the latter's absence.

[1] National laws and regulations shall apply where Nations treat NC information as accountable.

[2] Accountable information is defined in the C-M(2002)49 as all information classified CTS and NS and all Special Category Information (such as ATOMAL).

23. The CCO is responsible for the following tasks, which may be delegated to the Head of a COSMIC Registry:

(a) the physical safeguarding of all information classified CTS held by the Central Registry, registry or control point to which they are assigned;

(b) maintaining an up-to-date record of all information classified CTS held or circulating within the registry or control point or passed to other registries or control points;

(c) maintaining records of disclosure and destruction sheets for their registry;

(d) maintaining up-to-date records, by name, of all individuals that have been authorised access to information classified CTS held by their registry or control point;

(e) maintaining up-to-date records of all other registries and control points with which they are authorised to exchange information classified CTS, together with the names of the associated CCOs and their sample signatures;

(f) distribution of information classified CTS to only those addressees authorised to have access to information classified CTS;

(g) transfer of information classified CTS;

(h) obtaining receipts for all information classified CTS distributed or transmitted; and

(i) ensuring that information classified CTS is returned to the responsible registry when no longer required, either for retention or destruction.

24. Heads of COSMIC Central Registries shall notify the NATO Office of Security (NOS) of organisational changes regarding any of the registries or control points for which they are responsible.

25. The registry should be informed one month before a staff member leaves the organization, or 2 weeks before an in-house transfer, in order that an inventory of personal holdings can be carried out. If a replacement has not been appointed, all information classified NS or CTS on charge to the staff member shall be withdrawn and retained by the registry until a transfer of documents can be made.

26. The Registry System shall exercise continuous control of information classified CTS and shall maintain records of each document receipt, distribution and destruction. Records shall identify the COSMIC Central Registry, registry, control point or individual holding the document.

27. At least annually, each registry or control point shall carry out an inventory of all information classified CTS for which it is accountable. Information classified CTS is deemed to have been accounted for, if:

(a) it is physically present, contains the correct number of pages and has the correct copy number; or

(b) a receipt is held from the registry or control point to which it has been transferred; or

(c) a change in NATO security classification or declassification notice or a destruction certificate for the document is held.

28. Registries and control points shall report the results of the annual inventory to the responsible COSMIC Central Registry.

29. Results of annual inventories of all COSMIC Central Registries shall be reported by the responsible security authority to the NOS by March 31st of each year.

30. The dissemination of information classified CTS shall be through COSMIC registry channels. Registries may transfer information classified CTS directly to other registries provided that the transfer and receipt is recorded in the originating and receiving registries. Information classified CTS may be issued outside a registry or control point to an individual who is responsible for its custody, but shall be returned when no longer required. The individual custody of information classified CTS shall not be transferred except through the responsible registry.

Information Classified NATO SECRET

31. The handling requirements for information classified NS are as follows:

(a) up-to-date records of the receipt, distribution and destruction of information classified NS shall be maintained; and

(b) periodic spot-checks shall be conducted of registry and divisional/personal holdings to verify their continued control.

Information Classified NATO CONFIDENTIAL and NATO RESTRICTED

32. Unless specifically required by national laws and regulations, information classified NC and NR is not required to go through the Registry System. Measures shall be in place to prevent unauthorised access to information classified NC and NR.

STORAGE

33. NATO Classified Information shall be stored in accordance with Enclosure "D" to C-M(2002)49 and the supporting Directive on physical security. NATO Classified Information may be collected and stored in any form or medium provided that it is afforded the appropriate degree of protection required for that level of classified information. Any such collections containing more than one NATO security classification shall be afforded the security protection of the highest NATO security classification appearing in the collection.

REPRODUCTIONS, EXTRACTS AND TRANSLATIONS

34. Reproductions, extracts and translations of information classified NS and below may be produced by the addressee under strict observation of the need-to-know principle. Security measures laid down for the original document shall be applied to such extracts, reproductions and/or translations. Reproductions, extracts and translations of information classified NS shall be marked with identifying copy numbers, and the numbers shall be recorded in the responsible registry. Reproductions, extracts, and translations of information classified NC and NR may be produced by the addressee provided they are controlled in a manner to deter unauthorised access. Any extract from a classified document shall bear the NATO security classification of the document or component thereof (if individually classified) from which it was taken. In circumstances where there is uncertainty regarding the appropriate NATO security classification of the extract, the matter shall be referred, in writing, to the originator for determination of the correct NATO security classification.

35. All NATO classified working papers shall be dated and marked with their NATO security classification. Where drafts, working papers and personal print-outs classified NS (and any reproductions thereof) are originated by individuals, sections, or divisions, they do not need to be registered and controlled by the registry unless they are to be passed outside of

their originating division or office, thereby transferring the responsibility for the protection from the originators. However, these documents shall become accountable after a maximum of 5 working days from date of origin. If after this period they are still required for current work, they shall be registered within the registry system and officially charged to the individual.

36. Where necessary, and when originator consent has been obtained, extracts of NATO Classified Information may be included in documents when there is a positive determination of the need-to-know principle regarding the access by individuals in NATO Nations or NATO Civil or Military bodies who have not previously been authorised access to NATO Classified Information. In these circumstances, such individuals must hold, where appropriate, a national Personnel Security Clearance (PSC) up to, at least, the national equivalent of the level of the NATO security classification of the extracted information concerned.

37. If, however, the originator of a NATO classified document wishes to control the further dissemination of information contained therein, the originator shall clearly indicate these special limitations with a note stating, for example: “Reproduction of this document in whole or in part, is prohibited unless authorised by the originator” or “Reproduction of paragraphs ….to….annexes….and….is prohibited unless authorised by the originator”. These special restrictions should be applied with discrimination and as infrequently as possible. More detailed guidance for the use of dissemination markings can be found in the Guidelines on the Security of NATO Classified Information (AC/35-D/1032).

38. Notwithstanding any originator control limitations or caveats, if a document needs to be translated into a language of a NATO Nation the translated document shall retain the original marking, meet all the criteria above regarding reproduction or extraction, and be afforded the same degree of protection as the original. If information classified CTS needs to be translated, the consent of the originator shall be obtained.

39. Information classified CTS shall not be reproduced or extracted, except when required for translation described above. Additionally, in exceptional circumstances, paper reproductions, extracts or translations of information classified CTS, including extracts and reproductions to or from machine readable media[3], may be made for urgent mission purposes, provided that the reproductions, extracts or translations:

(a) are authorised by the CCO of a COSMIC Central Registry or, if authority has been delegated, by the CCO of the responsible registry, sub-registry or control point;

(b) are reported to the COSMIC Central Registry, sub-registry or control point, which shall maintain a record of the number of reproductions made;

(c) bear the reference and copy number of the original information together with the name of the originator and that of the reproducing COSMIC Central Registry, sub-registry or control point;

(d) are marked with an identifying reproduction copy number locally assigned by the body making the reproduction or translation;

(e) display the CTS marking and all other markings of the original information; and

(f) are brought under COSMIC registry control, distributed through COSMIC registry channels and reported in the annual inventory along with other information classified CTS.

[3] Machine Readable Media is a medium that can convey data to a given sensing device.

40. Where, for operational or mission critical reasons, the requirements set out above cannot be immediately met, the officer in charge of a communications centre[4] may authorise the production of those reproductions and translations necessary to make initial distribution of signals/messages classified CTS. A record shall be made of the number of reproductions and translations made together with a list of recipients. Thereafter, the authority for reproduction and translation of the signal/message will be the CCO of the COSMIC Central Registry.

41. Reproductions, extracts and translations of information classified NS, including reproductions to or from machine readable media, may be produced by the addressee when necessary for operational or mission purposes, provided that the reproductions, extracts or translations are marked with identifying copy numbers and the number of reproductions and/or translations, including copy numbers, are recorded by the responsible registry. In circumstances when the registry is not available, a record will be made by the addressee and forwarded to the appropriate registry as soon as possible.

42. Equipment, such as copiers, facsimile equipment and CIS, authorized or accredited for use in the reproduction (or transmission) of NATO Classified Information, shall be physically protected to ensure that only authorised individuals can use or access them.

DISSEMINATION AND TRANSFER

43. The purpose of security during dissemination and physical transfer is to ensure appropriate protection against unauthorised observation, modification or disclosure (deliberate or inadvertent).

Dissemination

44. The dissemination of NATO Classified Information shall be on a need-to-know basis. The dissemination of information classified NC and above shall be restricted to individuals who have the appropriate level of PSC, who have been briefed on their security responsibilities, and who are authorised to have access to such information. In addition to the requirements listed above, the dissemination of information classified CTS shall be in compliance with paragraphs 21 and 30 above. Information classified NR may be disseminated to individuals who have been informed of the prescribed control measures, have been briefed and have a need-to-know for official purposes.

Transfer

45. For the purposes of this Directive the term transfer of information refers to moving NATO Classified Information from one point to one or more other points by physical means. Transportation of NATO Classified Information as Freight is further regulated in the Directive on Classified Project and Industrial Security (AC/35-D/2003).

46. As a general principle, and wherever possible, the use of secure electronic means is preferred over the use of physical transfer of NATO Classified Information. All CIS handling NATO Classified Information shall be subject to a security accreditation process in accordance with Enclosure “F” to C-M(2002)49 and its supporting directives.

[4] Communications Centre is an organization responsible for handling and controlling communications traffic, normally comprising a message centre, a cryptographic centre, and transmitting and receiving stations.

Hand carriage

47. NATO or national staff assigned to hand-carry[5] information classified NC and above shall be appropriately security cleared by their National Security Authority/Designated Security Authority (NSA/DSA) or other competent security authority. Such staff shall be briefed on NATO security procedures and shall be instructed on their duties for protecting the NATO Classified Information entrusted to them.

Couriers / Guards / Escorts

48. When individuals such as guards and escorts are employed for the transfer of NATO Classified Information or in circumstances where they might have inadvertent or unauthorised access to NATO Classified Information, they shall be security cleared to the level deemed appropriate by the relevant security authority.

Transfer within NATO Nation's or NATO Civil or Military body's Sites or Establishments

49. NATO Classified Information carried within the perimeter of a site or establishment shall be covered in order to prevent observation of its contents. Internal procedures defining appropriate security principles should also be adopted when NATO Classified Information is carried outside Class I or Class II areas such as in the Administrative Zones.

Transfer outside Sites or Establishments within a NATO Nation

50. When NATO Classified Information is sent outside the confines of a site or establishment, the packaging requirements of paragraphs 51 and 52 and the receipt requirements of paragraphs 63 to 68 shall be complied with. The physical transfer of NATO Classified Information within a NATO Nation shall be by the following means:

(a) **Military or government courier service**
for information classified up to and including CTS. NOTE: this is the only accepted means for the transfer of information classified CTS.

(b) **National postal services**
If permitted by national laws and regulations, and if approved by the responsible NSA/DSA or other competent security authority, information classified up to and including NS may be transmitted by a national postal service.

(c) **Commercial courier service**
If permitted by national laws and regulations, and if approved by the responsible NSA/DSA or other competent security authority, such services may be used for information classified up to and including NS.

(d) **Hand Carriage**
If permitted by national laws and regulations, information classified up to and including NS may be transmitted by hand carriage by a member of staff or contractor, **acting as a courier,** with an appropriate level of PSC under conditions no less stringent than those prescribed for national information of equivalent NATO security classification, provided that:

(i) a record shall be kept in the appropriate registry, control point or office of all accountable information carried;

[5] Hand Carriage is transfer of information by an individual carrying that information on their person.

(ii) NATO Classified Information shall be packaged in accordance with the requirements of paragraphs 51 and 52, and the locked briefcase or other approved container shall be of such size and weight that it can be retained in the personal possession of the courier;

(iii) NATO Classified Information shall not leave the possession of the courier unless it is stored in accordance with the prescribed security requirements, it shall not be left unattended, and it shall not be opened en route;

(iv) NATO Classified Information shall not be read in public places;

(v) the courier shall be briefed on their security responsibilities and be provided with a formal written authorisation, in accordance with national laws and regulations; and

(vi) for NATO Civil and Military bodies the hand carriage of information classified NC and NS shall be allowed only in exceptional circumstances (e.g. when individuals are required to travel at a short notice, or when time does not permit such information to be sent by approved secure means, and when reproductions cannot be made available locally at the receiving location). Individuals carrying information classified NC and NS shall be provided with a NATO Courier Certificate (Appendix 1 contains an example of a Courier Certificate).

51. Information classified NC and above transferred between sites or establishments shall be packaged so that it is protected from unauthorised or inadvertent disclosure. The following standards shall apply:

(a) it shall be enclosed in two opaque and strong covers. For NS and CTS, a tamper- evident secure envelope, a locked pouch, locked box or a sealed diplomatic pouch may be considered as the outer cover;

(b) the inner cover shall be secured, bear the appropriate NATO security classification, as well as other prescribed markings and warning terms, and bear the full designation and address of the intended recipient;

(c) the outer cover shall bear the designation and address of the intended recipient and a mechanism for proof of delivery for receipting purposes;

(d) the outer cover shall not indicate the NATO security classification of the contents or reveal that it contains NATO Classified Information;

(e) if the NATO Classified Information is hand-carried by courier, the outer cover shall be clearly marked with the notice, “By Courier Only”.

52. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Transfer between the territories of NATO Nations

53. The international transfer of information classified CTS shall be by diplomatic pouch, government courier or military courier.

54. The international transfer of information classified up to and including NS shall be by diplomatic pouch, government courier, military courier or hand carriage.

55. The use of national postal services for international transfer of information classified up to and including NS may be used provided that the NSAs/DSAs of the relevant Nations have a suitable bilateral agreement/arrangement in place in order to support such means of transfer.

56. Commercial services may be used for international transfer of information classified up to and including NC provided that the commercial service provider has been approved for such purpose by its NSA/DSA. The recipient should be notified in advance of such shipment taking place. As a minimum, a commercial service shall provide the possibility to track the shipment from the sender to the recipient and provide the sender with proof of delivery.

57. NATO Classified Information transferred in the context of classified contracts or programmes may be transmitted by other means in accordance with the relevant provisions of Enclosure "G" of the C-M(2002)49 and its supporting directive.

58. In circumstances where other postal or commercial services are used, the packaging requirements shall follow the details as described in paragraphs 51 and 52 above.

59. The following requirements shall be met when information classified NC and above is hand carried by nominated NATO or national staff:

(a) The package shall bear an official seal, or be packaged in a manner to indicate that it is an official consignment, and should not undergo customs or security scrutiny. Official National or NATO Seals shall be handled as accountable documents, and as such, they shall be protected as though they were NS material.

(b) The courier shall carry a Courier Certificate recognised by all NATO Nations (Appendix 1 provides a template of such a Certificate) identifying the package and authorising them to carry the package. As a minimum, the courier shall be briefed in accordance with Appendix 2.

(c) The courier's travel arrangements shall be in accordance with the following restrictions on destinations, routes and means of transportation or, if national regulations are more stringent, in accordance with national regulations:

(i) the courier shall not travel to, through or over non-NATO nations nor use any means of transportation or any transportation carrier registered in a non-NATO nation, to which any of the criteria listed below apply:

(1) the government of the nation:

i. has given evidence by word or deed of an attitude hostile to NATO and/or NATO Nations;

ii. is not able to give a generally agreed level of protection to the life and/or personal belongings of its residents and/or visiting foreigners; or

iii. has given evidence that it does not respect at all times the immunity of a diplomatic seal;

(2) the intelligence services of the nation target NATO and/or NATO Nations; or

(3) the nation is at war, or subject to serious civil strife.

60. In exceptional cases, the restrictions at paragraph 59(c) above may be waived by the NSAs/DSAs or the Heads of NATO Civil or Military bodies, or their designated representatives, if urgent operational requirements cannot be otherwise met.

Transfer outside the territory of NATO Nations

61. The transfer of information classified up to and including NS outside the territory of NATO Nations shall be by diplomatic pouch, government courier, military courier or hand carriage.

Dissemination and Transmission by means of CIS

62. All CIS handling NATO Classified Information shall be subject to a security accreditation process in accordance with Enclosure “F” of NATO Security Policy and its supporting directives.

RECEIPTS AND RECORDS

63. Receipts are required for packages containing NATO accountable information that are transferred between sites / establishments, within national borders or internationally. Receipts shall be obtained against package numbers. Receipts are not required for packages containing information classified NC or NR unless required by the originator or specifically required by national laws and regulations. Receipts shall be unclassified, shall quote the reference number, copy number, and language of the document, and a short title, if it is unclassified.

64. A receipt shall be enclosed in the inner cover of packages containing information classified CTS and NS. The receipt and disposition of information classified CTS and NS shall be recorded as prescribed herein.

65. The receipt, listing the documents, shall be immediately returned to the sender after having been dated and signed by the receiving registry. Documents that contain accountable information shall only be signed for by the appropriately cleared registry personnel.

66. In terms of information classified CTS and special categories only the CCO, DCCO or Alternate DCCO shall sign for this type of accountable information. Additionally, the inner cover of a package containing information classified CTS may contain a marking indicating that it is to be opened only by a specific individual or office. However, the cover shall be opened in the presence of the CCO, DCCO or Alternate DCCO, and a reproduction of the external receipt or other identifying information shall be provided so that the document may be entered into the registry system.

67. A continuous receipt system is required for the distribution of information classified CTS. Users of information classified CTS shall sign and date a disclosure record, which shall remain affixed to the document, or file of documents, until it is destroyed. The record shall be retained for 10 years after destruction of the document.

68. For the distribution of information classified NS within NATO Nations and NATO Civil and Military bodies, each NATO Nation or NATO Civil and Military body concerned shall establish internal procedures, to ensure that information classified NS is controlled and its receipt, disposition and dispatch is recorded.

69. The control records for NATO accountable information shall enable the identification of all individuals who had access to such information in order to facilitate damage assessment or conduct a security investigation into the compromise or loss of accountable information.

DISPOSAL AND DESTRUCTION

70. Proper management of NATO Classified Information extends throughout its life cycle, including those aspects related to its disposal and destruction. At the end of the life cycle, information shall be reviewed for retention, archival storage, downgrading, declassification or destruction.

71. Any such actions need to meet not only security requirements, but also NATO Classified Information management and archival requirements in accordance with the Policy on the Retention and Disposition of NATO Information (C-M(2009)0021) and its supporting directives.

Destruction

72. NATO Classified Information in hard copy which is no longer required for official purposes, including surplus or superseded information and waste, shall be destroyed in such a manner as to ensure that it cannot be reconstructed. It is the responsibility of the NSAs/DSAs or other competent security authority, and the security authorities of NATO Civil or Military bodies (NOS, SHAPE J2, ACT Office of Security) to approve the destruction process, including methods and products utilised for this purpose. The following minimum requirements shall apply:

(a) Shredders

(i) when shredders are used as a final destruction mechanism for NATO accountable information the area of the expelled particle shall not be larger than 5 sq mm. For information classified NR/NC, the area of the expelled particle shall not be larger than 10 sq mm. Shredders shall be cross-cutting in order to enhance confidence that the destroyed information is irretrievable. Shredders are required to have the capacity for manual operation and be constructed so that material cannot be left undestroyed in the machine in the operation.

(ii) when shredders do not meet the requirements of paragraph (i) above there shall be an appropriate onward disposal process where the shredded waste is collected by cleared personnel and destroyed further using an approved method or process ensuring that the classified waste cannot be accessed by unauthorised personnel until it is non-reconstructable.

(iii) any deviation from the requirements described in (i) and (ii) above shall be approved on a case-by-case basis by the relevant NSA/DSA or other competent security authority, subject to a security risk assessment.

(b) Pulpers
the machine is required to masticate classified waste material by breaking down the fibre resistance. The pulp matter is required to be disintegrated and de-fibred so as to be incapable of reconstruction as recognizable information. A locking device capable of being fastened with double padlocks is required to be provided to cover the loading head or any other aperture giving access to the inside of the tank.

(c) Incinerators
incinerators shall be constructed to accept sealed bags of classified waste. Any aperature which permits access to classified waste or ash during or after combustion is required to be sealed or padlocked. The ash residue is not to be recognizable.

73. For the destruction of removable computer storage media, reference shall be made to the guidance document published by the C3 Board as the INFOSEC Technical Implementation

Directive as well as Guidance on Downgrading and Destruction of System Equipment and Storage Media (AC/322-D(2012)0011 and AC/322-D(2012)0012 respectively).

74. It is not necessary to await destruction instructions from the originator for information that is held but no longer required. Registries and other offices[6] that hold such information shall keep it under review to determine whether it is still relevant or whether it can be destroyed.

75. The following are additional requirements for the destruction of accountable information:

(a) all information classified CTS shall be returned to the registry holding it on charge for destruction. Information classified CTS shall be listed on a destruction certificate which shall be signed by the COSMIC Control Officer and by an independent witnessing official, who shall be appropriately cleared and authorised to have access to information classified CTS;

(b) the CCO of the respective COSMIC Central Registry may authorise the responsible Control Officer of any deployed or isolated military unit to destroy information classified CTS which is no longer needed, provided properly executed destruction certificates are furnished to the registry which holds them on charge;

(c) destruction certificates and control records for information classified CTS shall be retained for a minimum period of 10 years in a registry, as they may assist in the conduct of investigations. Reproductions of destruction certificates need not be forwarded to the originator or the appropriate COSMIC Central Registry unless specifically requested;

(d) the destruction of information classified NS shall be recorded and the record shall be signed by the destruction official and independent witness, both of whom shall be appropriately cleared and authorised to have access to information classified NS;

(e) destruction certificates and control records for information classified NS shall be retained in the registry or office performing the destruction for a period specified by individual NATO Nations and NATO Civil and Military bodies, but for not less than five years.

76. The recording of the destruction and the retention of control records of information classified NC and NR is not required unless requested by the originator or specifically required by national laws and regulations. Additional information on retention schedules is provided in the Policy on the Retention and Disposition of NATO Information (C-M(2009)0021) and its supporting directives.

Security Incident

77. A Security Incident is an event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.

Security Breach

78. A Security Breach is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that may result in the actual or possible compromise of NATO Classified Information or supporting services and resources including but not limited to:

(a) NATO Classified Information lost;

[6] This includes sub-registries and the offices of those authorized to hold such information.

(b) NATO Classified Information subject to access by personnel without the correct level of PSC and/or without a need to know;

(c) NATO Classified Information stored in an unsecured cabinet or one not approved for the level of classified information held;

(d) NATO Classified Information left in an unsecured area where uncleared persons have unescorted access;

(e) NATO Classified Information cannot be found at the expected location;

(f) NATO Classified Information transferred by a method not approved by this Directive;

(g) NATO Classified Information handled on a system, which is not appropriately accredited for that level of NATO security classification;

(h) NATO Classified Information has been subjected to unauthorised modification;

(i) NATO Classified information is deliberately under-classified;

(j) NATO Classified Information has been destroyed in an unauthorised manner; or

(k) for CIS, there is a denial of service.

Compromise

79. Compromise denotes a situation when - due to a security breach or adverse activity (such as espionage, acts of terrorism, sabotage or theft) – NATO 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.

80. NATO Classified Information lost, even temporarily, outside a security area is to be presumed compromised. NATO Classified Information lost, even temporarily, inside a security area, including documents which cannot be located at periodic inventories, is to be presumed compromised until investigation proves otherwise.

Infraction

81. An infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO Classified Information (e.g. NATO Classified Information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap NATO Classified Information, etc).

Action Upon Discovery of a Security Breach or Infraction

82. All security breaches or potential security breaches shall be reported immediately to the appropriate security authority. Each reported security breach shall be investigated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the security breach, to determine:

(a) whether NATO Classified Information has been compromised;

(b) whether all the individuals who have or could have had access to the information subject to the breach have at least either a national PSC or authorisation to access NATO Classified Information and are known from existing records to be of such reliability and trustworthiness that no harm to NATO is likely to result from the compromise; and

(c) what remedial, corrective or disciplinary (including legal) action is recommended.

83. Where the investigation yields positive answers to both 82(a) and (b), and where there is reasonable evidence that the access was inadvertent, then the appropriate security authority shall take steps to brief and/or indoctrinate the individuals concerned, as appropriate, to the NATO security classification and special category of the NATO Classified Information to which they have had inadvertent access. The appropriate security authority can close such cases without reporting to the NOS.

84. Where the investigation yields a negative answer to 82 (b) the compromise is reportable to the NOS as described below.

85. The Primary Directive on CIS Security (AC/35-D/2004-REV3) clearly outlines the circumstances in terms of CIS where the NOS is to be immediately informed if a CIS Security Incident has occurred, such as unauthorised major data harvesting.

86. In terms of infractions, the NSA/DSA may investigate, deal with and close such cases without reporting to the NOS. The appropriate security authority of NATO Civil and Military bodies may also investigate, deal with and close such cases without reporting to the NOS unless there are indications of repeat occurences or concerns as to the actions or behaviour of the individual in question.

Reporting of Compromises

87. When a compromise of NATO Classified Information has to be reported under the terms of paragraph 84, the report shall be forwarded through the NSA/DSA or the Head of the NATO Civil or Military bodies concerned to the NOS. Where possible, the reporting authority should inform the originating NATO body at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances. Initial reports shall be forwarded immediately to the NOS in cases where it has been determined that:

(a) there has been a compromise involving information classified NS, CTS or any information with special category designators;

(b) there are indications or suspicions of espionage (provided that the report would not hamper the investigations in hand); or

(c) unauthorised disclosure to the press/media has occurred.

88. Initial reports shall contain the following information:

(a) a description of the information involved, including its NATO security classification and if known, marking reference and copy number, date, originator, subject and scope;

(b) a very brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise and, if known, the number and/or category of unauthorised individuals who have or could have had access; and

(c) whether the originator has been informed.

89. Further reports shall follow as developments warrant. Reports on compromise of information classified NC shall be forwarded when the investigation has been completed and should contain information as requested in paragraph 88(a), (b) and (c). There is no requirement to report compromises involving information classified NR unless they meet the criteria set out

paragraph 87(b) or (c) or specifically required under national laws and regulations. In all cases of reportable compromise the final report, or a progress report, of the investigation shall be with the NOS within 90 days of the initial report.

Records of Security Breaches

90. Heads of NATO Civil and Military bodies shall arrange for records of security breaches, including reports of investigation and remedial and corrective actions, to be kept for 10 years and to be available during security inspections.

Relief from Continued Accountability for Lost Accountable Documents

91. When the final report of investigation shows that accountable information has been irretrievably lost rather than mislaid and a compromise is deemed unlikely, the NSAs/DSAs or the Head of the NATO Civil or Military body may grant relief from continued accountability to the relevant registry or control point.

Action by the Originating NATO Civil or Military body

92. The main purpose of reporting compromises of NATO Classified Information is to enable the originating NATO Civil or Military body to assess the resulting damage to NATO and to take whatever action is necessary to minimise the effects and prevent reccurence. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS.

Action by the NATO Office of Security

93. The NOS shall:

(a) coordinate enquiries where security authorities from more than one NATO Nation are concerned;

(b) coordinate, if necessary, with the originators and the security authorities concerned the final assessment of the damage done to NATO and any minimising action to be taken;

(c) recommend to, and/or conduct in agreement with the security authority concerned, further investigations whenever it considers them necessary; and

(d) inform the Secretary General of NATO, whenever the gravity of damage to the Alliance so warrants.

Action by the Secretary General of NATO

94. The Secretary General of NATO may request the appropriate authorities to make further investigations and to report their findings.

APPENDIX 1
ANNEX 1
AC/35-D/2002-REV5

COURIER CERTIFICATE

(Example)

Valid until ….....

1. This is to certify that the bearer …….*(name and rank where applicable)*.....……, holder of Passport No. ….....……is a member of ……*(parent organization)*…….

2. On the journeys detailed on the overleaf, the bearer is travelling in the execution of their official functions and is designated as an official NATO courier. The person is authorised to carry ……..... (number) of packages of official NATO documents, the seals on which correspond to the specimen seal appearing against the appropriate journey.

3. All Customs and Immigration Officials concerned are, therefore, requested to extend to the official correspondence and documents being carried under official seal by the bearer, the immunity from search or examination conferred by the Agreement on the Status of the North Atlantic Treaty Organization National Representatives and International Staff, and the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces. Should it be deemed absolutely necessary to examine any of the packages carried by the identified courier above, the attention of Customs and Immigration Officials concerned is hereby drawn to the following:

(i) It is requested that the packages will not be inspected by other than properly authorised persons or those having special permission;
(ii) It is requested that the inspection of packages is carried out in an area out of sight of the general public, and in the presence of the courier;
(iii) It is requested that the package, if opened for inspection, is marked after re-closing in order to show evidence of the opening by sealing and signing it and by annotating that the package has been opened;
(iv) Customs, Police, and/or Immigration Officials are requested to give assistance, if necessary, to ensure successful and secure delivery of the documents being carried.

Signature of Authorising Official: Date:

Designation:
(Name and rank in capitals)

Official stamp of NATO Nation or NATO Civil or Military body

DETAILS OF ITINERARY		**SPECIMENS OF SEAL USED**
From	To	See note below
From	To	See note below

NOTE: In addition to an impression of the seal, the officer affixing the seal must print their name, rank and the name and address of their department, command, agency or facility.

INSTRUCTIONS FOR THE COURIER
for the hand carriage of NATO Classified Information

You have been appointed to carry a NATO classified consignment. Your "Courier Certificate" has been provided. Before starting your journey, you will be briefed on the security regulations governing the hand carriage of NATO Classified Information and on your obligations during the specific journey (behavior, itinerary, schedule, etc).

The following general points are brought to your attention:

1. You will be held liable and responsible for the safe custody of the consignment you have been authorised to carry.

2. Throughout the journey, the consignment must stay in your personal possession and must not, under any circumstances, be left unattended.

3. The consignment will not be opened en route except in the circumstances described in paragraph 6 below.

4. In case of emergency, you must take such measures as you consider necessary to protect the consignment, and on no account will you allow the consignment out of your direct personal possession.

5. You are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) is complete, valid and current.

6. IMPORTANT: Should Customs, Police, and/or Immigration Officials inquire into the contents of the consignment, show them your "Courier Certificate" and insist on showing it to the senior Customs, Police, and/or Immigration Official. This action should normally be sufficient to pass the consignment 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 their presence, but this should be done in an area out of sight of the general public.

7. 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 immediatly upon completion of the examination.

8. 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 that the consignment has been opened.

9. Along the route you may contact the following officials to request assistance:

(Name and contact details) .....
.....
(Name and contact details) .....
.....