NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

17 January 2012

DOCUMENT
AC/35-D/2002-REV4

SECURITY COMMITTEE

DIRECTIVE on the SECURITY of INFORMATION

Note by the Chairman

1. At Annex is the fourth revision of the Directive on the Security of Information which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies.

2. This revision reflects approved changes to the following areas :

   (a) Deletion of Appendix 5 - Security Arrangements for the Release of NATO Classified Information to the Western European Union (WEU);

   (b) Appendix 8 - Security Assurance;

   (c) Appendix 9 - Personnel Security Certificate (for non-NATO national); and

   (d) Appendix10 - Attestation of Personnel Security Clearance (for non-NATO national)

3. This document has been approved by the Security Committee (AC/35-WP(2010)0001, AC/35-WP(2011)0009 and AC/35-WP(2011)0011 refer) and will be subject to periodic review.

(Signed) Stephen F. Smith

Annex: 1

Action officer: Robert Keil, NOS/IA/IF, ext. 4084
Original: English
DMS 1889086

ANNEX 1
AC/35-D/2002-REV4

DIRECTIVE ON THE SECURITY OF INFORMATION

INTRODUCTION

1. This Security of Information directive is published by the NATO Security Committee (AC/35) in support of Enclosure "E" to the NATO Security Policy (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 :

(a) classification and markings of information;

(b) control and handling of information;

(c) reproductions, translations and extracts of information;

(d) dissemination and transmission of information by physical means ;

(e) receipts and records;

(f) disposal and destruction;

(g) security infractions, breaches and compromises; and

(h) security arrangements for the release of NATO classified information to non-NATO nations and international organisations.

CLASSIFICATION and MARKINGS

2. Security classifications indicate the sensitivity of NATO 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 disclosure would result in exceptionally grave damage to NATO;

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

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

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

3. NATO nations and NATO civil and military bodies shall introduce measures to ensure that information created by, or provided to NATO is assigned the correct security classification. For NATO civil and military bodies, these measures shall include:

(a) restricting the authority to decide on a security classification for information to a limited number of designated positions;

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

(c) emphasising that documents shall not necessarily be given the same security classification as those to which they are attached, refer or respond.

4. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

5. The top and bottom of each page of a document shall be marked with the overall security classification of the document, noting that individual annexes / appendices / attachments / enclosures may be marked with a classification level lower than the overall security classification of the document.

6. The overall security classification of a document shall be at least as high as that of its most highly classified component. Component parts of documents classified NC and above shall, where possible, be classified (including by paragraph) by the originator to facilitate decisions on further dissemination of appropriate sections. Covering documents shall be marked with the security classification of the information contained therein when they are separated from the information they accompany.

7. When information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts. Original security classification caveats must be retained when information is used to prepare composite documents.

8. 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 classification of the document, he shall inform all addressees.

9. An originator of classified information that is collated into a new product by a NATO civil or military body who, when consulted in the course of a review for the declassification of NATO classified information, objects to the declassification of specific information, will indicate the earliest date or event on or around which he shall either agree to its declassification or review it again for declassification.

Changing Classifications

10. The classification level of NATO classified information may be changed only by, or with the consent of, the originator. However, if the originator cannot be determined, the successor organisation or higher authority shall assume the responsibility of the originator. In such cases, changes in classification may occur only after the NATO nations or NATO civil or military bodies that have an interest in the subject matter have been consulted.

11. The originator, or if the originator cannot be determined, the successor organisation or higher authority, is responsible for ensuring that recipients are promptly notified when the classification level of information is changed.

Dissemination Limitation Markings

12. As an additional marking to further limit the dissemination of NATO classified information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

The Registry System

13. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single registry system, in which case strict compartmentalisation of CTS information shall be maintained at all times, or by establishing separate registries and control points:

(a) each NATO member nation may establish up to two Central Registries for CTS, which act as the main receiving and dispatching authority for the nation or body within which it has been established. Central Registries may also act as registries for other accountable information; and

(b) registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information 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.

14. 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.

15. Regardless of the type of registry organisation, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO). CCOs shall be designated as necessary. A Deputy COSMIC Control Officer (DCCO) may perform some of the duties of the COSMIC Control Officer on a permanent basis and shall assume all authority and responsibility during the latter's absence.

16. 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 he is 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, and maintaining records of disclosure and destruction sheets for his registry;

(c) maintaining up-to-date records, by name, of all individuals authorised access to information classified CTS held by his registry or control point;

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

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

(f) transmission of information classified CTS;

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

(h) ensuring that documents classified CTS are returned to the responsible registry when no longer required, either for retention or destruction; and

(i) in the case of Heads of COSMIC Central Registries, notifying NOS of organisational changes regarding any of the registries or control points for which he is responsible.

Registry System Handling

Information Classified COSMIC TOP SECRET (CTS)

17. Documents classified CTS consigned to an addressee in another member nation or NATO civil or military body may be transmitted direct from one registry or control point to another when authorised by the appropriate authority of the member nation or NATO civil or military body.

18. The Registry System shall exercise continuous control of individual documents classified CTS, which includes such items as microfiche and computer storage media, and shall maintain records of document receipt, distribution and destruction. Records shall identify the COSMIC Central Registry, registry, control point or individual holding the document.

19. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable. A document classified CTS is deemed to have been accounted for, if:

(a) it is physically accounted for and contains the correct number of pages;

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

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

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

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

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

Information Classified NATO SECRET (NS)

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

(a) up-to-date records of the receipt, disposition, and dispatch 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 (NC) and NATO RESTRICTED (NR)

24. Unless specifically required by national security rules and regulations, NC and NR material is not required to go through the Registry System. Measures shall be in place to prevent unauthorised access to NC and NR material.

STORAGE

25. NATO classified information shall be stored in accordance with NATO Security Policy (Enclosure “D”) and the supporting physical security directive requirements. NATO classified information may be stored as microfilm, on computer storage media, provided the collections or media are afforded the same security protection as the original information and any collections or media containing more than one classification shall be afforded the security protection of the highest classification appearing in the collection or on the microfilm, or computer storage media. Information classified NR shall be stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled.

REPRODUCTIONS, TRANSLATIONS, AND EXTRACTS

26. Reproductions and translations of documents 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 reproductions and/or translations. If classified NS, they shall be marked with identifying copy numbers. The number of reproductions and/or translations of NS documents and their copy numbers shall be recorded.

27. Extracts of NATO classified documents may be included, if necessary, in documents which need to be seen by individuals in member nations or NATO civil or military bodies who have not been authorised access to NATO classified information, provided they hold a national personnel security clearance to the level of the classification of the extracted information. In order to ensure that the extracts are properly protected, such papers shall be given an appropriate security classification and shall be distributed on a need-to-know basis. An extract from a classified document shall bear the classification of the document or component thereof (if individually classified) from which it is taken unless it is obvious that it justifies another classification. If so**,** it shall be referred to the original or higher classification authority for determination of the correct classification.

28. If, however, in exceptional circumstances, the originator of a classified document desires to control the further dissemination of information contained therein, the originator shall indicate these special limitations with a prominent and suitable note to the effect, 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.

29. Notwithstanding originator control prohibitions, addressees whose national language is not that of a document may translate the document, provided the requirements for copying have been met and the translation includes all classifications markings and caveats of the original document. In addition, translations of documents classified CTS shall be reported to the originator.

30. Information classified CTS shall not, except in exceptional cases, be copied. Extra paper copies of information classified CTS shall normally be obtained from the originating NATO nation or NATO civil or military body. In exceptional cases, paper copies or translations of information CTS, including extracts and copies to or from machine readable media may be made for urgent mission purposes, provided that the copies or translations :

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

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

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

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

(e) display the CTS marking and classification 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 CTS information.

31. As an exception to the above, the officer in charge of a communications centre may authorise the production of those copies and translations necessary to make initial distribution of signals/messages classified CTS. A record shall be made of the number of copies made. Thereafter, the authority for reproduction and translation of the signal/message will be the CCO of the COSMIC Central Registry.

32. Reproductions, extracts and translations of information classified NS, including copies to or from machine readable media, may be reproduced by the addressee when necessary for mission purposes, provided that the reproductions and/or translations are marked with identifying reproduction copy numbers and the number of reproductions and/or translations, including reproduction copy numbers, are recorded.

33. Reproductions, extracts, and translations of information classified NC and NR may be reproduced by the addressee provided they are controlled in a manner to deter unauthorised access.

34. Equipment, such as copiers, facsimile equipment and IT systems, used to reproduce classified information, shall be physically protected to ensure that only authorised individuals can use them.

DISSEMINATION AND TRANSMISSION BY PHYSICAL MEANS

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

Dissemination

36. 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 personnel security clearance, who have been briefed on their security responsibilities, and who are authorised to have access to such information. The dissemination of information classified CTS shall be in compliance with paragraph 22 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.

Transmission

Transmission within Sites or Establishments

37. Classified information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

Transmission outside Sites/Establishments within a NATO Nation

38. Whenever a courier service is used for the transmission of NATO classified information outside the confines of a site or establishment, the packaging requirements of paragraphs 39 and 40 and the receipt requirements of paragraphs 47 to 50 shall be complied with. The physical transmission of classified information within a NATO nation shall be by the following means:

(a) **Military or government courier service**;

(b) **National postal services/**
NATO information classified up to and including NS may be transmitted by a national postal service under conditions fixed by national regulations;

(c) **Authorised commercial courier service/**
Where appropriate, such services may be used for NATO information classified up to and including NS if permitted by national regulations, provided their use is approved by the relevant NSA/DSA;

(d) **Personal Carriage**
The personal carriage of NATO classified information may be permitted within a NATO nation under conditions no less stringent than the national regulations for the personal carriage of national information of equivalent classification, provided that:

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

(ii) classified information shall be packaged in accordance with the requirements of paragraphs 39 to 40, and the locked briefcase or similar approved container shall be of such size and weight that it can be retained in the personal possession of the courier;

(iii) classified information shall not leave the possession of the bearer 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) classified information shall not be read in public places; and

(v) the individual shall be briefed on his security responsibilities and be provided with either a formal written authorisation, in accordance with national rules and regulations; and, when carrying information classified NC and above, be provided with a NATO courier certificate (Appendix 1 contains an example of a courier certificate).

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

(a) it shall be enclosed in two opaque and strong covers. 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 classification, as well as other prescribed markings and warning terms, and bear the full designation and address of the addressee;

(c) the outer cover shall bear the designation and address of the addressee and a package number for receipting purposes;

(d) the outer cover shall not indicate the classification of the contents or reveal that it contains classified information; and

(e) if the classified information is transmitted by courier, the outer cover shall be clearly marked with the notice, “By Courier Only”.

40. 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.

International Transmission

41. The international transmission of information classified CTS shall be by diplomatic pouch or military courier. Personal carriage internationally of information classified CTS is prohibited.

42. The international transmission of NATO classified information up to and including NS shall be by diplomatic pouch, military courier, registered mail or personal carriage as set out below. Information classified NR may also be transmitted by other postal or commercial services.

43. Information classified up to and including NS that cannot be transmitted by one of the foregoing methods and that is relevant to the industrial domain may be transmitted by other means in accordance with the relevant provisions in Enclosure “G” of the NATO security policy and its supporting industrial security directive.

44. The following requirements shall be met for the international transmission of packages containing information classified NC and above :

(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 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 (see example at Appendix 1) identifying the package and authorising him to carry the package; and

(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 :

(a) has given evidence by word or deed of an attitude hostile to NATO and/or NATO nations;

(b) 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

(c) 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.

45. In exceptional cases, the restrictions at paragraph 44(c) above may be waived by the NSAs or the Heads of NATO civil or military bodies, or their designated representatives, if urgent operational requirements cannot be otherwise met.

DISSEMINATION AND TRANSMISSION BY ELECTROMAGNETIC MEANS

46. Information classified NR and above shall be disseminated and transmitted in accordance with the requirements of Enclosure “F” of NATO security policy and its supporting directives.

RECEIPTS AND RECORDS

47. Receipts are required for packages containing accountable information that are transmitted 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 security rules and regulations. Receipts shall be unclassified, shall quote the reference number, copy number, and language of the documents, and a short title, if it is unclassified.

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

49. The receipt, listing the documents, shall be immediately returned to the sender after having been dated and signed. Documents that contain accountable information shall be signed for only by the CCO or other registry system individual. The inner cover of a package containing a CTS document 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 other authorised registry system individual, and a copy of the external receipt or other identifying information shall be provided so that the document may be entered into the registry system.

50. A continuous receipt system is required for the distribution of information classified CTS. For the distribution of information classified NS within member nations and NATO civil and military bodies, each member 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.

51. Users of a CTS document 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.

DISPOSAL AND DESTRUCTION

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

53. Any such actions need to meet not only security requirements, but also need to meet NATO information management and archival requirements.

Destruction

54. Classified information 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 not necessary to await destruction instructions. Registries and other offices that hold NATO classified information shall maintain a continuous review of the information to determine whether it can be destroyed.

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

(a) all information classified CTS shall be returned to the registry holding them 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 NSA 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. Copies 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 NS information; and

(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 or military bodies, but for not less than 5 years.

56. The control records to be retained should be sufficient to undertake a damage assessment or conduct a security investigation into the compromise or loss of accountable information.

57. The recording of the destruction and the retention of control records of information classified NC and NR is not required; unless required by the originator or specifically required by national security rules and regulations.

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

Action on Breaches of Security

58. All breaches of security shall be reported immediately to the appropriate security authority. Each reported breach of security 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 breach, to determine :

(a) whether NATO classified information has been compromised[1];

(b) if so, whether all the unauthorised individuals who have or could have had access to the information have at least either a national or a NATO personnel security clearance and are known from existing records to be of such reliability and trustworthiness that no harm to NATO will result from the compromise; and

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

59. Where the investigation yields positive answers to both 58(a) and (b), the administrative authority shall take steps to brief and/or indoctrinate the individuals concerned, as appropriate, to the classification and category of the information to which they have had inadvertent access. The administrative authority can close such cases without reporting to the NOS. Where the investigation yields a positive answer to 58(a) and a negative answer to either part of 58(b) the compromise is reportable to the NOS as described below.

[1] Classified information lost, even temporarily, outside a security area is to be presumed compromised. Classified information lost, even temporarily, inside a security area, including that in documents which cannot be located at periodic inventories, is to be presumed compromised until investigation proves otherwise.

Records of Breaches of Security

60. Heads of NATO civil and military bodies shall arrange for records of breaches of security regulations, including reports of investigation and remedial and corrective actions, to be kept for three years and to be available during security inspections.

Reporting of Compromises

61. When a compromise of NATO classified information has to be reported under the terms of paragraph 59, the report shall be forwarded through the NSA or the Head of the NATO civil or military bodies concerned to the NOS. Where possible, the reporting authority should inform the originating NATO component 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) CTS or NS information is involved; or

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

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

62. Initial reports shall contain the following information:

(a) a description of the information involved, including its classification and 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.

63. 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 62(a), (b) and (c). There is no requirement to report compromises involving information classified NR unless they meet the criteria set out paragraph 61(b) or (c) or specifically required under national security rules 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.

Relief From Accountability for Lost Accountable Documents

64. When the final report of investigation shows that an accountable document has been irretrievably lost rather than mislaid, the NSAs or the Head of the NATO civil or military body may grant relief from accountability.

Action by the Originating NATO Component

65. The main purpose of reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimise the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS.

Action by the NATO Office of Security (NOS)

66. The NOS shall :

(a) coordinate enquiries where security authorities from more than one NATO nations 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

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

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND INTERNATIONAL ORGANISATIONS

68. Enclosure "E" to NATO security policy sets out the principles for authorising the release of NATO classified information to non-NATO nations and international organisations, and the release authority conditions. The following Appendices to this directive address the specific procedures and arrangements :

(a) APPENDIX 2
Procedures for the Release of NATO classified information to non-NATO Recipients;

(b) APPENDIX 3
NATO Production and Logistic Organisations (NPLOs) - Procedures to be Followed for the Release of NATO Classified Information Belonging to an NPLO or other Organisation Granted a Charter under the Terms of C-M(62)18;

(c) APPENDIX 4
Security Provisions for the Exchange of Classified Information Between NATO and the European Union (EU);

(d) APPENDIX 5 - *Cancelled*;

(e) APPENDIX 6
Security Arrangements for the Release and Protection of NATO Classified Information to a NATO-led Combined Joint Task Force (CJTF) or Similar Formation and the Exchange and Protection of Classified Information with non-NATO Nations / Organisations Participating in a NATO-led CJTF or Similar Formation;

(f) APPENDIX 7
Minimum Standards for the Handling and Protection of NATO Classified Information (NATO SECRET and Below) to be Met by Non-NATO Recipients;

(g) APPENDIX 8
Security Assurance;

(h) APPENDIX 9
Personnel Security Clearance Certificate (for non-NATO national); and

(i) APPENDIX 10
Attestation of Personnel Security Clearance (for non-NATO national).

APPENDIX 1
ANNEX 1
AC/35-D/2002-REV4

COURIER CERTIFICATE
(Example)

Valid until ……..

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

2. On the journeys detailed overleaf, the bearer is travelling in the execution of his official functions and is designated as an official NATO courier. He 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.

Signature of Authorising Official:

Designation:
(Name and rank in capitals)

Official stamp of NATO member
Nation or NATO civil or military body

Date:

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 his name, rank and the name and address of his department, command, agency or facility.

PROCEDURES FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO RECIPIENTS

REQUESTS FOR RELEASE OF NATO INFORMATION

1. Release authorisation shall be based on the principles stated in Enclosure “E” of NATO security policy.

2. Requests for release shall be sent to the relevant addressee as follows:

   (a) the Council Secretariat, NATO International Staff, for NATO classified information issued by the NAC;

   (b) to the Secretary of the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it;

   (c) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and/or bodies subordinate to it;

   (d) to SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET);

   (e) to the Mission Commander for a NAC-approved operation involving non-NATO Troop Contributing Nations, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR); and

   (f) the Head of an NPLO, for NATO classified information originated by and belonging to one or more of the nations participating in the NPLO.

3. Requests for release shall include the following information:

   (a) for NAC-approved cooperative activities, where potential non-NATO participants to that activity have also been endorsed by the NAC on a case-by-case basis:

      (i) reference to the relevant subject in the overall work plan or the OPLAN for the cooperative activity;

      (ii) purpose and justification for the release (initiating cooperation, progress in cooperation, exercise, etc);

      (iii) identification of document(s) containing the NATO classified information (reference number, date and NATO classification);

      (iv) description of the NATO classified information which should be released (the whole document(s), part of the document or excerpt from the document);

(v) if appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents, etc., stating maximum classification and any other limitations regarding the possible future release).

(b) for release outside cooperative activities approved by the NAC, the document containing the NATO classified information must be identified and the information requested in (a) (ii), (iii) and (iv) above must be given. Generic release is not authorised.

Actions upon the Receipt of a Release Request

4. Addressees receiving a request for release of NATO classified information shall ensure that :

(a) the justification given in the release request is adequate; and

(b) the NATO classified information concerned is properly identified and described; and

(c) in accordance with the requirements of Enclosure "E" to NATO Security Policy, a Security Agreement has been concluded between NATO and the non-NATO recipient and that the required security survey has been carried out by the NOS with a positive result;

or

in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient has been provided;

or

the non-NATO recipient has provided, through its NATO Sponsor, a written Security Assurance to NATO that it will protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information of an equivalent classification;

or

the NATO sponsor has provided the necessary assurance that the appropriate security system is in place in the non-NATO recipient for the protection of released information;

and

(d) the request is sent to the appropriate committee or delegated authority for a decision; and

(e) any international organisation which requests release has a Security Agreement in force with NATO and the release of information to its non-NATO members is in accordance with relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities.

5. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g. a military document prepared by NAMILCOM and approved by the Defence Planning Committee (DPC) and issued under the latter's reference), it is the responsibility of the initial addressee to coordinate the response to the request.

Actions by the Release Authority

6. Based on the information contained in the request, the Release Authority will approve or refuse the release.

7. National members of the Release Authority are responsible for obtaining any approval which may be required from national authorities.

8. The Release Authority is responsible for ensuring that any information released to a non-NATO recipient has been reviewed / sanitised so that the non-NATO recipient is only given information for which he has a requirement / need-to-know.

9. Approval, whether obtained in committee or under the silence procedure, will be recorded in writing.

10. In the context of NAC-approved cooperative activities, the Release Authority may approve generic release of NATO classified information issued under its authority. Such approval must state the specific subject areas or series of documents of the NATO classified information and the level of classification authorised for release and may stipulate any other limitations regarding possible future release.

11. Should a request for release of NATO classified information not be approved by a delegated Release Authority, the request, together with the latter's reason for not approving it, may be presented to the next level and ultimately to the NAC for final decision. This action will only be taken in cases when sought by the requesting NATO member nation(s) or NATO body or when the delegated Release Authority decides that such action is appropriate.

Marking Information to be Released

12. The following procedures shall be used for marking NATO classified information:

(a) **for existing NATO information**: classified information originating from NATO which is released to non-NATO recipients shall retain its NATO classification. In addition, the cover or first page of the copy of any document released, and the archive copy, shall be marked with the name of the Release Authority, the date the release decision was taken and any related terms or conditions;

(b) **for NATO information created within NAC-approved activities**:

(i) NATO classified information originated in the context of a NAC co-operative activity shall bear the marking "NATO" followed by the designation of the activity or by the name(s) of the international organisation(s) or participating nation(s) and the classification level;

Example:

NATO/EAPC RESTRICTED

NATO/RUSSIA CONFIDENTIAL

NATO/ISAF CONFIDENTIAL

NATO/OAE CONFIDENTIAL

(ii) the dissemination of information generated within a NATO co-operative activity may be restricted by the originator to some of the non-NATO recipients. In this case, a caveat showing the non-NATO recipients permitted access shall be added below the classification line:

Example:

NATO/PfP RESTRICTED
SWEDEN AND SWITZERLAND ONLY

(iii) information created by a NATO civil or military body that is intended to be further disseminated outside the environment within which it was created shall bear the caveat "Releasable to":

Example:

NATO CONFIDENTIAL
RELEASABLE TO CHILE

NATO/EAPC RESTRICTED
RELEASABLE TO AUSTRALIA

NATO CONFIDENTIAL
RELEASABLE to KFOR

NATO CONFIDENTIAL
RELEASABLE to OAE

Transmission of Information to be Released

13. All NATO classified information released to non-NATO recipients shall be forwarded via physical or electromagnetic means, in accordance with the requirements of NATO Security Policy and supporting directives.

Records of Information to be Released

14. NATO civil and military bodies shall keep control records of all information classified CONFIDENTIAL and above which they have released to non-NATO recipients and shall, at least every six months (or as directed by the appropriate Security Authority), report details of the reference number, title and release date to the NATO Central Registry, Brussels. The report sent to the NATO Central Registry identifies the details of the information released since the previous report. On request, national authorities can obtain details through the NATO Central Registry, Brussels.

NATO PRODUCTION AND LOGISTICS ORGANISATIONS (NPLOs)

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION BELONGING TO AN NPLO OR OTHER ORGANISATION GRANTED A CHARTER UNDER THE TERMS OF C-M(62)18

1. NATO classified information originated by one or more of the nations participating in an NPLO or other organisation granted a charter under the terms of C-M(62)18, or generated within such an organisation and pertaining to it, may be the subject of an application for release to a non-NATO recipient by any member nation, or NATO body considering that it would be advantageous to NATO.

2. The provisions of Appendix 2 shall apply, except that the application shall be submitted to the Head of the NATO organisation concerned, who will pass it on to the Board of Directors (or its delegated representative) for a decision. It must specify the document(s) or the class of information to be released, the proposed recipient's need for access to the information, and the purpose for which it will be used. The Board shall take into account already concluded Security Agreements and other arrangements with international organisations that govern the participation of their non-NATO members in NATO-related activities.

3. Provided that the Board (or its delegated representative) agrees that the NATO classified information should be released, it shall ask the NSA of the nations participating in the NATO organisation's programme to satisfy themselves that adequate security arrangements for the protection of the NATO classified information intended to be released exist or are created.

4. For NR information, a Project / Programme Security Group involving the NSAs of the participating nations may delegate authority for release to the Security Officer of the NPLO, in consultation with the appropriate management within the NPLO.

5. The security arrangements shall include a Security Agreement / Arrangement accepted by the nations participating in the NPLO and, on behalf of the intended recipient(s), by an authority competent to commit them to undertake to provide the NATO classified information released a level of security protection no less stringent than that afforded to it within NATO as set out in Appendices 7 and 8. A copy of these Appendices shall be provided to the intended recipient(s). Where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities.

6. NSAs shall also take whatever steps they consider appropriate to ensure that the intended recipient(s) are competent to comply with the provisions of the Security Agreement.

7. Release shall be administered on behalf of the Board of Directors of the NATO organisation concerned, by its Security Office. Records shall be kept of all information classified NC or NS passed under these procedures. These records shall be subject to examination by the NOS during its periodic inspections of the organisation.

SECURITY PROVISIONS FOR THE EXCHANGE OF CLASSIFIED INFORMATION BETWEEN NATO AND THE EUROPEAN UNION (EU)

GENERAL

1. The release and exchange of information classified RESTRICTED and above between NATO and the EU is regulated by the Agreement between the North Atlantic Treaty Organisation and the European Union on the Security of Information. This Appendix sets out the policy, procedures and minimum requirements for the handling of NATO classified information to be released to the EU. Attachment 1 contains the "NATO Procedures for Requesting Classified Information from the EU". Attachment 2 contains the "Security Standards Between the NATO Office of Security (NOS), the EU Council General Secretariat Security Office (GSCSO) and the European Commission Security Office (ECSO) for the Protection of Classified Information Exchanged Between NATO and the EU".

RELEASE AUTHORITY

2. The North Atlantic Council (NAC) is the ultimate authority for the release of NATO classified information to the EU except for information classified up to and including COSMIC TOP SECRET which has been originated by the NATO Military Committee (NAMILCOM) (see paragraph 3(b) below). The release of other information classified COSMIC TOP SECRET will always require approval by the NAC. NAC approval is also required for the release to the EU of NATO SECRET information originated by Committees subordinated to the NAC.

3. The NAC has delegated release authority to :

(a) the relevant committee for information classified up to and including NATO CONFIDENTIAL;

(b) the NAMILCOM for information classified up to and including COSMIC TOP SECRET which has been originated by the NAMILCOM and bodies subordinate to it; and

(c) the Board of Directors of a NATO Production and Logistics (NPLO), or other organisations granted a charter under the terms of C-M(62)18, for information classified up to and including NATO SECRET, which has been originated by one or more nations participating in the NPLO or other organisations.

4. Authority for release will only be delegated to a committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the relevant committee will assume the responsibility of the originator(s).

REQUESTS FOR RELEASE

5. Requests from the EU for the release of NATO classified information (which must explain their requirement and provide details of intended recipients) will be sent to the relevant addressee, as follows :

(a) the Executive Secretary, NATO International Staff, for NATO classified information issued by the NAC and committees subordinate to it;

(b) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and bodies subordinate to it; and

(c) the Head of an NPLO, or other organisation granted a charter under the terms of C-M(62)18, for classified information originated by one or more nations participating in the NPLO or other organisation.

ACTIONS UPON RECEIPT OF A RELEASE REQUEST

6. The addressee will task relevant NATO staffs to prepare the required documents for the appropriate committee (or, in the case of an NATO Production and Logistics Organisation (NPLO), for the Board of Directors) for a decision on release. These documents will contain the following information :

(a) identification of document(s) containing the NATO classified information (reference number, date and NATO security classification);

(b) description of the NATO classified information which could be released (the whole document(s), part of the document(s) or excerpts from the document(s));

(c) in the case of requests for release to non NATO EU Member State(s), confirmation that the EU Member State(s) have subscribed to the "Partnership for Peace" framework document and**,** in that context**,** have a valid security agreement with NATO; and

(d) in the case of requests for release to non-EU Member States, a written confirmation that the EU has completed security formalities and a Security Agreement is in place to ensure implementation of security procedures in the non-EU Member states. This confirmation will be provided to the NATO Office of Security (NOS).

REQUESTS FOR GENERIC RELEASE

7. Requests for generic release (e.g. NATO SECRET planning information pertaining to NATO/EU joint CMX exercises) will also include, following the agreement of the appropriate committee, details of specific subject areas, defined series of documents, anticipated future documents or series of documents and anticipated requirements for internal release, etc., stating maximum classification. Upon approval, the appropriate committee (or Board of Directors) will state any other limitations regarding future release**.**

PROCESSING RELEASE REQUESTS

8. The request will be sent to the appropriate committee (or Board of Directors) for a decision, which will entail obtaining the approval of the originator(s). National members of the relevant committee are responsible for obtaining any approval which may be required from their national authorities. The Board of Directors of an NPLO, having agreed on the release of classified information originated by and belonging to one or more of the states participating in the NATO Production and Logistics Organisation (NPLO)**,** will seek prior to dissemination, the approval of the national security authorities**.**

9. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g., a military document prepared by NAMILCOM and approved by Defence Planning Committee (DPC), it is the responsibility of the originating authority to coordinate the response to the request.

CLASSIFICATION MARKINGS

10. Classified information originating from NATO which is released to the EU will retain its NATO ownership label and security classification. A caveat will be added below the line to denote releasability :

E.g.: NATO (Security Classification)
RELEASABLE TO EU

Or: NATO (Security Classification)
RELEASABLE TO EU COUNCIL AND/OR (NAMED DIVISION) ONLY

Or: NATO (Security Classification)
RELEASABLE TO EU COUNCIL AND/OR EU COMMISSION

Or: NATO (Security Classification)
RELEASABLE TO EU **AND** NAME(S) OF THIRD COUNTRY(IES) ONLY

11. In addition, the cover or first page of any document released will be marked with the name of the committee (or Board of Directors) which has authorised the release, the date the release decision was taken and any limitation caveats.

RECORDS

12. NATO bodies will keep complete, separate records of all NATO accountable information which they have released to the EU and will send details of the reference number, title, classification, and release date to the NATO Central Registry, Brussels.

13. NATO Central Registry shall maintain a master record of accountable information released to the EU. This record shall be accessible by NATO Member States.

MINIMUM REQUIREMENTS FOR THE HANDLING OF NATO CLASSIFIED INFORMATION RELEASED TO THE EU

14. Within the EU, in accordance with Articles 6, 11 and 12 of the Agreement between the North Atlantic Treaty Organisation and the European Union on the Security of Information, NATO classified information will be handled in accordance with EU security regulations. All NATO classified information which is released to the EU is for official use only. It will, therefore, only be disseminated to individuals in the EU with a need-to-know, an appropriate security clearance for NATO CONFIDENTIAL information and above only, and in accordance with stipulated release caveats.

CLASSIFICATION SYSTEM

15. Classification markings will be used to indicate the sensitivity of the NATO classified information and thus the security procedures and regulations which will apply for its protection. The classifications are as follows: RESTRICTED, CONFIDENTIAL, SECRET and COSMIC TOP SECRET. These correspond to :

NATO	UE COUNCIL / COMMISSION
NATO RESTRICTED	RESTREINT UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO SECRET	SECRET UE
COSMIC TOP SECRET	TRÈS SECRET UE

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

16. All NATO classified information released to the EU (or to the EU recipients) shall be transferred through a NATO registry to a separate registry established for NATO information in the EU.

ELECTROMAGNETIC TRANSMISSION

17. The electromagnetic transmission of classified information between NATO and the EU shall be conducted in accordance with agreed NATO/EU mechanisms / procedures to be agreed, which assure its protection.

NOS RESPONSIBILITIES

18. The NOS shall:

(a) ensure that the Security Arrangements for the protection of released classified information meet the minimum requirements as laid down in this Appendix;

(b) coordinate inspections with the EU counterpart; and

(c) keep records on all CTS documents held by EU, based on a calendar year report received annually by the 31st March.

ATTACHMENT 1
APPENDIX 4
ANNEX 1
AC/35-D/2002-REV4

NATO PROCEDURES FOR REQUESTING CLASSIFIED INFORMATION FROM THE EUROPEAN UNION

GENERAL

1. NATO, NATO Commands and Agencies shall use the attached form for requesting classified information from the EU.

PROCEDURES FOR REQUESTING

2. A request for EU classified information shall contain the following :

(a) identification and description of the EU classified information that is requested;

(b) if appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents etc.);

(c) intended recipients in NATO; and indication of possible further release outside NATO; and

(d) rationale and justification of the request**;** if appropriate, reference to the relevant NATO activity/mission and/or NATO/EU joint activity or co-operation.

	NATO RESTRICTED
	NATO CONFIDENTIAL
	NATO SECRET
	COSMIC TOP SECRET

NORTH ATLANTIC TREATY ORGANIZATION

FROM: (DIVISION/OFFICE)

REQUEST FOR RELEASE OF EU CLASSIFIED INFORMATION

TO : EU (COUNCIL OR COMMISSION, AS APPROPRIATE) INFO. : REFS. :	FILE : NO :
1. IDENTIFICATION OF DOCUMENT(S) (WHERE KNOWN)	

2. RATIONALE FOR THE REQUEST
3. INTENDED RECIPIENTS IN NATO AND, IF APPROPRIATE, OUTSIDE NATO
4. (Describe here if the whole document is needed or which part or extract is requested)

Date: Signature:

ATTACHMENT 2
APPENDIX 4
ANNEX 1
AC/35-D/2002-REV4

SECURITY STANDARDS BETWEEN THE NATO OFFICE OF SECURITY (NOS), THE EU COUNCIL GENERAL SECRETARIAT SECURITY OFFICE (GSCSO) AND THE EUROPEAN COMMISSION SECURITY OFFICE (ECSO) FOR THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN NATO AND THE EU

INTRODUCTION

1. Pursuant to Article 12 of the NATO-EU Security Agreement, reciprocal standards for the protection of classified information exchanged between NATO and the EU are hereby agreed. NOS, the GSCSO and the ECSO are responsible for the implementation and oversight of these standards.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

2. Subject to Article 5(a) of the NATO/EU Security Agreement, positions which require access to NATO or EU classified information (respectively NCI and EUCI) must be identified. Access to EUCI and NCI will be authorised only for individuals who have a "need-to-know". Furthermore, individuals occupying such positions which require access to information classified at or above NATO CONFIDENTIAL or CONFIDENTIAL UE level must have a 'need-to-know' as well as a valid Personal Security Clearance (PSC) issued in accordance with the relevant provisions contained in the respective security rules of NATO, the General Secretariat of the Council and/or the European Commission.

3. The parent National Security Authority (NSA) of the individual concerned is the competent authority responsible for seeing that the necessary security investigations on their nationals/citizens have been carried out in accordance with the respective NATO/EU minimum security standards.

4. Before being given access to classified information, all individuals who require access to classified information must be briefed on the protective security regulations relevant to the classification of the information they are to access. Those individuals accessing classified information must be made aware that any breach of the security regulations will result in disciplinary action and/or possible further legal action in accordance with their respective security regulations or provisions.

CLASSIFICATION SYSTEM

5. Classification markings will be used to indicate the sensitivity of the classified information and thus the security procedures and regulations which will apply for its protection. The classifications and their equivalence are as follows :

NATO	EU
NATO RESTRICTED	RESTREINT UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO SECRET	SECRET UE
COSMIC TOP SECRET	EU TOP SECRET/TRES SECRET UE

The NATO or EU marking in the classification line indicates ownership of the information and defines, inter alia, originator rights.

All information originated by one of the Parties and provided to the other(s) shall include an express releasability marking, such as:

NATO SECRET
RELEASABLE TO THE EU

SECRET UE
RELEASABLE TO NATO

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

6. A registry system is established at NATO, the General Secretariat of the Council and the European Commission for the receipt, dispatch, control and storage of classified information. The EU Council General Secretariat will be the Central Registry for NATO classified information provided to the EU. At each organisation a designated registry will act as the main point of entry and /exit for information classified NATO CONFIDENTIAL above or CONFIDENTIEL UE and above, as defined per the respective rules of NATO and the EU. Such registries are established as follows :

(a) for NATO: at NATO HQ and SHAPE (for information to be distributed within Allied Command Europe); and

(b) for the EU: at the EU Council General Secretariat.

7. Central and sub-Registries will be responsible for :

(a) distribution and control of classified information within their respective organisation(s);

(b) storage of classified information; and

(c) final disposal and/or downgrading and/or declassification of classified information, including the maintenance of destruction certificates for NATO accountable or EU classified information.

8. The NOS, the GSCSO and the ECSO will be responsible for the oversight and control of registries within their respective organisation(s) and will inform their counterparts of the establishment/disestablishment of registries containing each other's classified information.

9. When exchanging classified information, appropriately cleared couriers will be used by both sides and will be granted, upon presentation of the appropriate security clearance certificate, access badges to the building(s) they need to visit to deliver and collect the documents.

ELECTROMAGNETIC TRANSMISSION

10. The electromagnetic transmission of classified information between NATO and the EU and between the EU and NATO shall be encrypted in accordance with the sender's requirements as outlined in its Security Policies or Regulations.

11. Crypto equipment employed for communications between NATO and the EU must have been certified by the appropriate authority of one of the States designated under Article 5a of the Security Agreement if the level of the information is CONFIDENTIAL or below. When the equipment is intended for the transmission of information classified SECRET and above, it must have been evaluated and approved in accordance with NATO or EU policies or regulations.

BREACHES OR COMPROMISES OF SECURITY

12. Whenever a breach/compromise of security affecting information classified NATO CONFIDENTIAL**/**CONFIDENTIEL UE or above is discovered or suspected:

(a) a report giving details of the breach/compromise must be sent :

(i) by the GSCSO or ECSO to the NOS, for NCI;

(ii) by the NOS to the GSCSO or ECSO, as appropriate, for EUCI;

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the office to which the initial report was addressed. At the conclusion of the investigation, remedial or corrective action, where appropriate, must be taken.

13. For information classified NATO RESTRICTED or RESTREINT UE breach/compromises of security need to be reported only when they present unusual features and/or when it is assessed that actual damage resulted from the breach/compromise is in accordance with the respective NATO and UE security regulations.

INSPECTIONS / LIAISON

14. The three Security Offices will facilitate reciprocal inspections to ensure that information originated by their parent organisation is properly protected. In this respect, a joint GSCSO-ECSO team will inspect NATO Headquarters and SHAPE**,** while the NOS will conduct separate inspections to the General Secretariat of the Council and the European Commission.

REVIEW

15. The three Security Offices will facilitate, as appropriate, the presence of observers on their respective inspections. NOS may observe with respect to inspections of EU Member States relative to the protection of NATO classified information releasable to the EU, and GSCSO ECSO may observe with respect to inspections of NATO Member States relative to the protection of EU classified information releasable to NATO.

LIAISON

16. The NOS, the GSCSO and the ECSO will maintain constant liaison to oversee the release and exchange of classified information under the terms of the NATO-EU Security Agreement. These Offices will meet to discuss and review matters of common interest and assess the implementation of these standards. Any modifications to this Security Standards document shall be subject to agreement between the NOS, the GSCSO and the ECSO and the approval by the NATO Security Committee and the EU Council Security Committee respectively.

This Page Intentionally Left Blank

SECURITY ARRANGEMENTS FOR THE RELEASE AND PROTECTION OF NATO CLASSIFIED INFORMATION TO A NATO-LED COMBINED JOINT TASK FORCE (CJTF) OR SIMILAR FORMATION AND THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION WITH NON-NATO NATIONS/ORGANISATIONS PARTICIPATING IN A NATO-LED CJTF OR SIMILAR FORMATION

1. The CJTF concept of deployable multinational, multi-service formations involving NATO and non-NATO nations/organisations generated and tailored for specific contingency operations was endorsed at the NATO Summit of January 1994 and is being implemented through PO(96)63 and the latest version of MC 389. It reflects NATO's determination to give full and practical effect to its new roles, to strengthen the European defence capability of the Alliance and to enhance the development of the Partnership for Peace (PfP) programme. Similar formations may include specific operations that have been approved by the NAC.

2. Participation in a NATO-led CJTF presumes that NATO and non-NATO nations will release/exchange and protect classified information required for the conduct of the CJTF, principally to maintain force protection and the effectiveness of the mission.

3. This Appendix sets out the security requirements for the release and protection of NATO classified information to a NATO-led CJTF and the exchange and protection of classified information with non-NATO nations/organisations participating in a NATO-led CJTF; it draws on existing NATO Security Policy and procedures for the release and protection of NATO classified information outside NATO.

4. The following principles shall apply:

   (a) political and military endorsement of the CJTF mission shall have been obtained and any legal requirements satisfied before classified information can be released to/exchanged within a CJTF;

   (b) the non-NATO nation shall have signed a Security Agreement with, or provided a Security Assurance to, NATO. The international organisation shall have concluded a Security Agreement with NATO to enable the former to receive NATO classified information.

   (c) the release of information to a non-NATO nation on the basis of a Security Assurance shall be limited to NC. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), NS information may be released to non-NATO troop contributing nations (NNTCN);

   (d) NATO security policy and procedures for the handling and protection of NATO classified information shall apply to all nations/organisations participating in the CJTF;

(e) the originator is responsible for determining the security classification and initial dissemination of information; the release of NATO classified information to non-NATO recipients shall be in accordance with the requirements of Enclosure "E" to NATO Security policy;

(f) non-NATO members participating in the CJTF shall be eligible to receive information classified up to and including NS released to the CJTF in accordance with NATO procedures, and in accordance with the understanding in sub-paragraph (c) above;

(g) all classified information released/exchanged will be disseminated under strict observance of the need-to-know principle and shall only be used for the accomplishment of the CJTF mission;

(h) the CJTF Mission Commander shall balance the requirement to protect classified information with the need to maintain force protection and the effectiveness of the CJTF mission. Any classified information of an operational nature that has the potential to affect the lives of CJTF personnel, shall be withheld only in the most exceptional circumstances;

(i) following the decision on which non-NATO nations shall join the CJTF, and in order to ensure force protection and the effectiveness of the mission, authority for the release/exchange of all classified information of an urgent operational nature, such as support of combined combat operations, may be delegated by the NATO Military Committee (NAMILCOM) to the level best suited to evaluate the importance of that information and the need for its immediate release. This shall be specified in the promulgating NATO Operations Order (OPORD). The guiding principle shall be that classified information of an operational nature that has the potential to affect the lives of CJTF personnel shall be withheld only in the most exceptional circumstances. Such release of information not marked by the originator as releasable to the CJTF shall be reported promptly to the NAMILCOM which will decide what limitations should be imposed on the continuing release of such information and inform the appropriate commander(s).

5. As stated at paragraph 4, a political and military mandate for the mission shall be required, any legal requirements satisfied, and security formalities completed before any classified information can be released to or exchanged within a CJTF.

6. A security organisation shall be established in the promulgating NATO Operations Order at the inception of the CJTF. The security organisation shall be directed by a Security Authority who, as a rule, will be the ACOS Intelligence (or equivalent) of the CJTF HQ. Security responsibilities shall also be clearly identified and defined in that OPORD. These shall include :

(a) regulating and coordinating all physical, personnel, information and INFOSEC issues;

(b) clearly identifying release authorities for classified information which shall be established in accordance with agreed NATO security policy;

(c) overseeing and monitoring the security regime, to include the provision of advice and guidance to non-NATO participants on the protection of NATO classified information; and

(d) contingency planning for emergency access and destruction of classified information.

SECURITY REGULATIONS - GENERAL

7. NATO civil and military bodies participating in the CJTF shall comply with NATO security regulations and procedures for the handling and protection of NATO classified information. National/other organisation classified information released to the CJTF shall be handled and protected to the same standard as NATO classified information unless other procedures are required by the originator.

8. Non-NATO personnel shall be denied access to any NATO or national classified information that has not been authorised for release by the appropriate authority. Physical controls and security procedures shall be established in order to maintain separation between NATO classified information which is not releasable to the CJTF and NATO classified information released to the CJTF.

9. This regime shall be achieved by:

(a) establishing separate NATO facilities for the collation and screening of NATO classified information prior to release. These facilities shall be at the lowest level consistent with the security and effectiveness of the CJTF;

(b) permitting access to NATO secure areas by non-NATO personnel only when escorted;

(c) prohibiting access by non-NATO personnel to primary sources of NATO classified information or to IT systems and networks processing NATO classified information;

(d) permitting access by non-NATO personnel to meetings/briefings only after NATO classified information to be used in them has been approved for release;

(e) providing non-NATO nations with copies of this Annex and its Appendices and any other relevant NATO security documents to enable them to handle and protect classified information to NATO standards.

SECURITY REGULATIONS - DETAIL

10. The following addresses the requirements for physical security, personnel security, security of information and INFOSEC :

(a) **Physical Security**

(i) areas containing NATO and other classified information must be selected to provide both effective security and for operational efficiency;

(ii) NATO classified information shall be stored and controlled separately from other classified information;

(iii) NATO-only and CJTF areas must be separated and clearly identified;

(iv) access to these areas shall be permitted to authorised personnel only, who have a valid and appropriate security clearance and possess a pass issued by the authorities controlling these areas;

(b) **Personnel Security**

(i) access to classified information shall only be permitted to individuals who have a valid and appropriate personnel security clearance issued by their national security authority or other competent national body;

(ii) it is the CJTF commander's responsibility to ensure :

- that all individuals participating in the CJTF are informed of the security regime and of current security regulations and procedures;
- that these individuals are aware of their personal responsibility for the protection of classified information to which they have access; and
- that these individuals receive appropriate security education and training, particularly with regard to the protection of NATO classified information.

(c) **Security of Information**

(i) **COSMIC TOP SECRET (CTS)** - CTS shall not be released to non-NATO members of the CJTF. CTS information is only to be handled by appropriately security cleared NATO and NATO member nation personnel with authorised access to the subject matter. Regulations and procedures for handling and protecting information classified CTS are to be found in the relevant Enclosures of NATO Security Policy. In case of actual release, the CJTF commander shall develop an annex summarising the appropriate provisions.

(ii) **SECRET information** is to be handled by appropriately security cleared personnel with authorised access to the subject matter. When not in use, SECRET information is to be stored in security containers. The area in which the container is located is to be under guard at all times and a control of entry system is to be established which only permits authorised individuals to enter the area. Displays of SECRET information shall only take place within appropriately controlled areas. SECRET information is to be transmitted by diplomatic courier, secure messenger services or approved secure telecommunications. Copies may only be made after receipt of written approval from the originator. All copies are to be registered and controlled in the same manner as the original. All transactions involving SECRET information are to be covered by a continuous chain of receipts;

(iii) **CONFIDENTIAL information** is to be handled by appropriately security cleared personnel with authorised access to the subject matter. When not in use, CONFIDENTIAL information is to be stored in security containers located in controlled areas. Displays of CONFIDENTIAL information shall only take place within appropriately controlled areas. Transmission is to be via diplomatic couriers or military messenger services or approved secure telecommunications. Copies may be reproduced by recipients provided that dissemination is made under the need-to-know principle;

(iv) **RESTRICTED information** is to be handled, displayed and stored in areas to which unauthorised individuals are denied access. Transmission is to be achieved through secure means. Transmission by public telecommunications is to be avoided unless speed of delivery is essential to CJTF force security and mission success. Copies may be reproduced by recipients;

(v) **Recipients** are to maintain records of all information classified NATO CONFIDENTIAL and above or that is classified CONFIDENTIAL and above by a member nation, non-NATO nation or another organisation released to the CJTF. Information no longer required is to be destroyed by secure means and, for information classified NATO SECRET and above, a destruction certificate completed containing the signatures of two appropriately security cleared individuals having witnessed the destruction.

(vi) **Should** a compromise of information classified CONFIDENTIAL or above take place, an investigation of the circumstances shall be carried out by the appropriate security authority and the originator informed. CJTF participants, whether NATO or non-NATO, shall cooperate in the investigation as required. Remedial or corrective action shall be taken to correct any deficiency in procedures that caused the compromise. A report on the compromise and on action taken will be forwarded to the NATO Office of Security (NOS) by the investigating security authority.

(d) **INFOSEC**

(i) **identification and authentication/access control** - only authorised users, who have been uniquely and reliably identified and authenticated, shall have access to relevant classified information, whether this is national, other organisation, NATO or CJTF;

(ii) **accounting/audit** - authorised users shall be individually **accountable** for their access (read, write, modify and delete) and actions (transmit/receive) with regard to classified information within the CJTF. Measures will be implemented by the CJTF security authority/ies (as specified in the OPORD) to detect and prevent users or bodies (inside or outside the CJTF) from breaching or attempting to breach the security environment;

(iii) **confidentiality** - measures shall be taken to prevent the interception or redirection of data communications that carry classified information within the CJTF;

(iv) **integrity** - the integrity of all classified information stored, processed or transmitted within the CJTF shall be maintained; and

(v) **availability** - classified information within the CJTF shall be available to authorised users when required.

MARKING AND CLASSIFICATION

11. The following are the marking and classification requirements :

(a) there will be a requirement to release/disseminate classified information from the planning/preparatory stages of the CJTF onwards. Originators should designate as much classified information as possible as releasable to the CJTF. CJTF commanders and others involved in the CJTF should seek to anticipate classified information requirements at the earliest possible stage and seek approval for its release/dissemination as outlined in paragraph 12 below. Separate compartments for **NATO only** and for **NATO classified information released to the CJTF** must be created in order to provide a mechanism to control the circulation of classified information within the CJTF.

(b) information shall be marked and classified as follows :

(i) with an identifying marking - NATO, NATO nation, non-NATO nation or another organisation;

(ii) classified according to NATO Security Policy - RESTRICTED, CONFIDENTIAL, SECRET;

(iii) carry a release designator where appropriate:

Either: NATO SECRET
Releasable to (name of CJTF)

or:

(cite NATO nation, non-NATO nation or other organisation)SECRET
Releasable to (cite NATO only or name of the CJTF);

and

(iv) contain any caveats regarding further dissemination :

NATO SECRET
Releasable (cite the name of the CJTF and/or
the name or names of nations) Only

(c) information originated in the theatre of operations by a CJTF component and intended for dissemination throughout the CJTF shall be marked as NATO/CJTF. As a rule, all information of an operational nature originated in theatre shall bear this marking;

(d) component parts of documents classified CONFIDENTIAL and above shall be marked and classified (including by paragraph) by the originator to allow further dissemination of appropriate sections. Original security classifications markings / caveats shall be retained when information is used to prepare composite documents or briefings.

RELEASE AUTHORITY

12. The release authorities are as follows, based on the source/originator of the classified information :

(a) **NATO Nation, Non-NATO Nation or Other Organisation**: Classified information originated by a NATO nation, a non-NATO nation or another organisation may be provided to NATO and/or to the CJTF. Classified information provided exclusively to NATO can only be further released on the authority of the providing nation/organisation.

(b) **NATO**: The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated in accordance with the requirements of NATO Security Policy (Enclosure "E"). This shall also apply to all NATO classified information previously contributed by NATO nations where the national originator cannot be determined. Classified information originated within elements of the CJTF as NATO-only may subsequently be authorised for release to the CJTF by the originator;

(c) **CJTF**: classified information generated within the CJTF shall generally be marked as NATO/CJTF and may therefore be disseminated, when necessary, throughout the CJTF based on the security clearance and on the need-to-know of the recipient(s). Classified information generated within the CJTF which cannot be disseminated, for whatever reason, to the CJTF as such, shall be handled as either national or NATO classified, and is subject to release as described above. CJTF commanders of OF-6 rank or above may authorise the release of information originated by the CJTF or already released to it to individuals or organisations beyond the CJTF on a need-to-know basis for CJTF force protection and the effectiveness of the CJTF mission.

MINIMUM STANDARDS FOR THE HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION (NATO SECRET and Below) TO BE MET BY NON-NATO RECIPIENTS

INTRODUCTION

1. All NATO classified information which is released to a non-NATO recipient is for official use only. It shall, therefore, only be disseminated to individuals with a need-to-know. The recipient shall agree that the minimum standards provided in this document will be met. These security measures only address information classified NS and below. Should it be determined that it is necessary to release information classified CTS to a non-NATO recipient, additional security measures will be required; these additional measures shall be extracted from the pertinent Enclosures of NATO Security Policy and its supporting directives.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

2. Before an individual is granted access to information classified CONFIDENTIAL or SECRET, he shall be subject to a personnel security clearance procedure which meets the minimum standards below to determine whether he is trustworthy and reliable. When the result of such a procedure is positive, a Personnel Security Clearance shall be granted to the individual by his Security Authority in accordance with the format at Appendix 9.

3. Before an individual is authorised access to classified information, he shall be briefed on the security regulations relevant to the level of classification of the information released and the legal and disciplinary consequences of infractions/breaches of these regulations.

4. When an individual who has been personnel security cleared is designated as a representative of his organisation to a meeting in which classified information is involved or the venue for the meeting is within a secure area, his Security Authority, when requested, will send an Attestation of Security Clearance, in accordance with the format at Appendix 10 to the organisation convening the meeting. The requirements for escorting individuals who do not hold a NATO Personnel Security Clearance remain valid if the meeting takes place in a NATO secure area.

Criteria for Assessing Eligibility for a Personnel Security Clearance

5. The following paragraphs contain the principal criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC. These paragraphs consider aspects of character and circumstances which may give rise to potential security concerns.

6. Although the criteria apply to the individual being cleared, where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member’s character, conduct and circumstances may also be relevant and should be taken into account when considering an individual's eligibility for clearance.

7. The criteria shall be applied to determine if an individual or his spouse, co-habitant, and where appropriate and in accordance with national legislation, close family member :

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such, unless these associations were authorised in the course of official duty;

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks the overthrow of the government of a nation(s), or a change in the form of government of a nation(s);

(d) is, or has recently been, a supporter of any organisation described in sub-paragraph (c) above, or who is, or who has recently been closely associated with members of such organisations.

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing the personnel security form or during the course of a security interview;

(f) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; or has serious financial difficulties or unexplained affluence; or has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(g) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;

(h) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;

(i) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);

(j) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in his judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or

(k) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals.

Investigative Requirements for NATO CONFIDENTIAL and NATO SECRET Clearances

8. The initial security clearance for access to information classified NC and NS shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following :

(a) the completion of a **Personnel Security Questionnaire** (which can be either NATO or national);

(b) **identity check / citizenship / nationality status** – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources; for example, due to former residence or past associations; and

(c) **national and local records check** – a check shall be made of national security and central criminal records, where these latter exist, and/or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

9. A registry system shall be established by the recipient for the receipt, dispatch, control and storage of classified information. This shall include a Central Registry and other registries as necessary. Registries shall be responsible for :

(a) the recording of the receipt and dispatch of all classified information;

(b) the distribution and control of all classified information within the nation/organisation served;

(c) the storage of the classified information; and

(d) the final disposal of the classified information, including the maintenance of:

(i) destruction certificates for all information classified SECRET;

(ii) log books or document registers for information classified RESTRICTED or CONFIDENTIAL.

REQUIREMENTS FOR THE HANDLING, STORAGE, AND TRANSMISSION OF NATO CLASSIFIED INFORMATION

10. These are as follows :

(a) **NATO SECRET** information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated appropriately cleared individuals with an established need-to-know for official purposes. NATO SECRET information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held only by designated security cleared personnel needing access to the stored information to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag.

Only cryptographic systems specifically authorised by the NAMILCOM shall be used for the encryption of information, however transmitted (e.g. electromagnetic), which is classified NATO SECRET. Reproductions and translations of documents classified NATO SECRET may be produced by the addressee under strict observation of the need-to-know principle. Copies of documents classified NATO SECRET must be marked with identifying reproduction copy numbers. The number of reproductions and/or translations of NATO SECRET documents and their copy numbers must be recorded by the registry (or sub-registry);

(b) **NATO CONFIDENTIAL** information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO CONFIDENTIAL information transmitted by electromagnetic means. Reproductions and translations of documents classified NATO CONFIDENTIAL may be produced by the addressee under strict observation of the need-to-know principle;

(c) **NATO RESTRICTED information** shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. Documents may be sent through postal channels by such means as are authorised by the appropriate NSA. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO RESTRICTED information transmitted by electromagnetic means. In exceptional circumstances, when speed is of paramount importance and means of encryption are not available, information classified NATO RESTRICTED may be transmitted electromagnetically in clear text over public systems. Reproductions and translations of documents classified NATO RESTRICTED may be produced by the addressee under strict observation of the need-to-know principle.

COMMUNICATION AND INFORMATION SYSTEMS

11. Non-NATO communication and information systems used for the processing/storage/transmission of NATO classified information shall meet the standards required by NATO Security Policy and supporting directives.

BREACHES OR COMPROMISES OF SECURITY

12. Whenever a breach/compromise of security affecting classified information is discovered:

(a) a report giving details of the breach/compromise shall be sent immediately to the NOS; and

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases the originator shall be informed.

13. Reports shall contain the following information:

(a) a description of the information involved, including its classification and 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.

INSPECTIONS

14. A non-NATO recipient participating in a NAC approved activity shall facilitate periodic inspections by the NOS to ensure that the security arrangements for the protection of released information meet the minimum standards dictated in this Annex.

ADMINISTRATIVE ARRANGEMENTS TO BE IMPLEMENTED BY NON-NATO RECIPIENTS

15. Non-NATO recipients shall appoint a Security Authority responsible for the implementation of security arrangements and procedures under the Security Agreement and shall identify this authority to NOS which is the equivalent security authority for NATO. The NOS shall establish liaison with the Security Authority of the non-NATO recipient to facilitate implementation of these security arrangements and procedures.

16. In accordance with the provisions contained in the Security Agreement, the NOS and the Security Authority of a non-NATO recipient must establish to their satisfaction that the recipient party will protect the classified information it receives as required by the originator.

17. The administrative arrangements shall cover, as required, the establishment of:

(a) a Security Authority which shall implement and oversee the security measures for the protection of classified information released and classified information exchanged in the cooperative activity;

(b) a registry system, including a Central Registry and other registries as required by the non-NATO recipient;

(c) procedures for the recording, control and destruction of classified information;

(d) standards of security containers used for the storage of classified information;

(e) channels of transmission;

(f) personnel security clearance procedures; and

(g) a system and procedures for the investigation of compromises/breaches of security.

18. After signature of the Security Agreement and the completion of the administrative arrangements, and before the exchange of classified information begins, the NOS shall, and non NATO recipients may, carry out a survey of the preparations made by an intended non-NATO recipient or NATO respectively for the handling and storage of the classified information to be exchanged. A copy of the NOS survey report shall be provided to the intended non-NATO recipient.

SECURITY ASSURANCE

A Security Assurance provided by a non-NATO recipient of NATO classified information shall contain the following certification:

The government of the

……
(cite the applicable nation or organisation)

represented by

……
(cite the signatory's name and position) [1]

in furtherance of participation in

……..
(cite the name of the NAC approved activity, e.g., CJTF or other programme or operation)

hereby agrees:

(a) to protect classified information provided to it by (name of the CJTF or other programme or operation) in accordance with the Annex to this Assurance;

(b) to provide such classified information only to appropriately cleared individuals under its jurisdiction with a need-to-know;

(c) to use such information only for the purposes for which it was provided;

(d) not to transfer such information to a third party without the prior written approval of the originator of the information; and

(e) to continue to abide by these security requirements of the Annex to this Assurance even after completion of (name of the CJTF or other programme or operation).

[1] The signatory is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

MINIMUM STANDARDS FOR THE PROTECTION OF NATO/ (1) CLASSIFIED INFORMATION

(applicable Nation or Organisation)

Security Clearance and Authorisation for Access

1. Before an individual is granted access to NATO/ (1) classified information, he will be subject to a security clearance procedure designed to determine whether the individual is loyal and trustworthy. When the result of such a procedure is positive, the recipient nation/organisation is to produce an Attestation of Personnel Security Clearance in accordance with the format at Attachment 2 to this Annex, which is to be forwarded to the (2) Security Office.

2. Upon receipt of the Attestation of Personnel Security Clearance, the (2) Security office will authorize access to information and areas, in accordance with the individual's need-to-know.

3. The individual shall be briefed by the (2) Security Office on the security regulations relevant to the classification of the information he is going to have access to.

Definitions of Classification Markings

4. The following principles apply to the classification of NATO/ (1) information:

(a) NATO/(1) SECRET
The unauthorised disclosure of which would result in grave damage to the NATO and (2) mission.

(b) NATO/(1) CONFIDENTIAL
The unauthorised disclosure of which would be damaging to the NATO and (2) mission.

(c) NATO/(1) RESTRICTED
The unauthorised disclosure of which would be detrimental to the interests or effectiveness of the NATO and (2) mission.

Requirements for Receipt, Handling, Storage and passing on of NATO/ (1) Classified Information

5. **Receipt/Registration**. A Registry system shall be established by the recipient for the receipt, dispatch, control and storage of classified information. Sub-registries may be established as necessary. Registries shall be responsible for:

(a) The recording of the receipt and dispatch of all NATO/(1) classified information;

(b) The distribution and control of all NATO/(1) classified information within the nation/organisation served;

(c) The storage and final disposal of all NATO/(1) classified information which must include:

(1) Destruction certificates for all information classified NATO/ (1) SECRET;

(2) Logbooks and registers for all information classified NATO/ (1) RESTRICTED or CONFIDENTIAL.

6. **Handling, Storage and passing on**. The following rules and regulations apply for the handling, storage and passing on of NATO/ (1) classified information:

(a) **NATO/(1) SECRET**
NATO/ (1) SECRET information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated, appropriately cleared individuals with an established need-to-know for official purposes. NATO/ (1) SECRET information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held only by designated, security cleared personnel, who require access to the stored information in order to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag.

(b) Copies of classified information are not to be made without prior authorisation from (2) HQ J2 Chief/Head of Security Office. If authorised, copies of NATO/ (1) SECRET may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle. Copies of documents classified NATO/ (1) SECRET must be marked with identifying reproduction copy numbers and must be recorded by the registry (or sub-registry).

(c) **NATO/(1) CONFIDENTIAL**
NATO/ (1) CONFIDENTIAL information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally approved locks, the keys or combinations to which shall be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Copies of classified information are not to be made without prior authorisation from (2) HQ J2-Chief/Head of Security Office. If authorised, copies of NATO/ (1) CONFIDENTIAL may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle.

(d) **NATO/(1) RESTRICTED**
NATO/ (1) RESTRICTED information shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. Copies of classified information are not to be made without prior authorisation from (2) HQ J2 Chief/Head of Security office, If authorised, copies of NATO/ (1) RESTRICTED may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle.

7. Destruction and Disposal. Classified information, 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.

8. The destruction of information classified NATO/ (1) SECRET is to be recorded. The record is to be signed by the destruction official and an independent witness, both of whom shall be appropriately cleared and authorised to have access to NATO/ (1)SECRET information. Destruction certificates and control records for information classified NATO/ (1) SECRET are to be retained in the registry or office performing the destruction for a period of not less than 5 years.

Breaches or Compromises of Security

9. Whenever a breach or compromise of security affecting classified documents is discovered, an initial report giving details of the breach/compromise must be sent immediately to (2) HQ Security Officer (SO). An investigation into the circumstances of the breach/compromise must be carried out immediately in conjunction with (2) HQ SO and a full report is to be sent to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases, the originator shall be informed by the NATO Office of Security.

10. The initial breach/compromise report is to contain the following information:

(a) A description of the information involved, including its classification, marking reference, copy number, date, originator, subject and scope.

(b) A brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise.

(c) If known, the number and/or category of unauthorised individuals who have or could have had access to the document.

(d) Whether the originator has been informed.

Security Surveys

11. The Government/Organisation ..... will facilitate periodic Surveys by NOS (or Delegated Authorities) to ensure that the security arrangements for the protection of released information meet the minimum established standards.

NOTE:

(1) Name of the NAC-approved Activity

(2) Applicable Nation, Organisation or Command

ATTACHMENT 2
APPENDIX 8
ANNEX 1
AC/35-D/2002-REV4

ATTESTATION OF PERSONNEL SECURITY CLEARANCE

1. Certification is hereby given that.

Full Name (LAST NAME, Middle Name(s), First Name):

……

Title/Rank:

……

Date and Place of Birth (DD/MM/YYYY, City, Country):

……

has been authorised to have security clearance by:

……
(the Government of/name of Organisation)

in accordance with national laws and regulations in compliance with the provisions of the Security Assurance (2) signed by
……

(the Government of/name of Organisation)

is deemed suitable to be entrusted with information classified up to and including (see Note below):
……
……
……

Note. Insert, as appropriate, one of the following:

(a) NATO/(1) SECRET

(b) NATO/(1) CONFIDENTIAL

2. The validity of this certificate will not expire later than:
……

Signed: …… (Official stamp)

Title: ……

Date: ……

APPENDIX 9
ANNEX 1
AC/35-D/2002-REV4

PERSONNEL SECURITY CLEARANCE CERTIFICATE
(for non-NATO national)

1. Certification is hereby given that:

Full Name (Last Name, First Name):
.....

Date and Place of Birth:
.....

has been granted a Personnel Security Clearance by the Government of:
.....

in accordance with the provisions of the Security Agreement between NATO and **[nation]**, in accordance with security requirements no less stringent than those of NATO, has been briefed on the security regulations for the protection of NATO information and the legal and disciplinary consequences of infraction / breaches of those regulations, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO SECRET(*) NATO CONFIDENTIAL(*)

2. The validity of this certificate will expire not later than:
.....

3. Issued by:

Name and address of the issuing authority:
……
……

Contact details of the issuing authority (Phone, e-mail, fax):
……

Full name (Last Name, First Name):

Title:

Signature: Official government stamp

Date:

(*) Delete as appropriate
(**) The marking is not part of the template.

APPENDIX 10
ANNEX 1
AC/35-D/2002-REV4

ATTESTATION OF PERSONNEL SECURITY CLEARANCE
(for non-NATO national)

1. Attestation is hereby given that:

Full Name (Last Name, First Name):
……

Date and Place of Birth:
……

Where employed:
……

Purpose and Duration:
……
……
Holder of Passport/Identity Card No: ……...
Issued at: ……
Dated: .....……

has been granted a Personnel Security Clearance for NATO classified information in accordance with security requirements no less stringent than those of NATO, has been briefed on the security regulations for the protection of NATO information and the legal and disciplinary consequences of infraction / breaches of those regulations, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO SECRET(*) NATO CONFIDENTIAL(*)

2. The validity of the attestation will expire no later than:
……

3. Issued by:

Name and address of the issuing authority:
……...
……
Contact details of the issuing authority (Phone, e-mail, fax):
……..

Full name (Last Name, First Name):

Title:

Signature: Official stamp

Date:

(*) Delete as appropriate
(**) The marking is not part of the template.