CONSEIL DE L'ATLANTIQUE NORD
NORTH ATLANTIC COUNCIL

EXEMPLAIRE
COPY N° 2103

N A T O R E S T R I C T E D (1)

ORIGINAL: ENGLISH
10th March, 1975

CORRIGENDUM 2 to
VOLUME I to
C-M(55)15(FINAL)

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

CORRIGENDUM 2 to Volume I to C-M(55)15(Final)
(dated 31st July, 1972)

Following approval by Council on 11th November, 1974 of amendments to Enclosures "B" and "C" to C-M(55)15(Final) contained in C-M(74)51, holders of Volume I of C-M(55)15(Final) should substitute the attached pages 5, 8, 9, 16-19, 26, 29-32, 34 and 45-72 for the existing ones (N.B. there is no existing page 18(A)).

2. For ease of reference, holders may wish to note that substantive changes to Enclosure "C" consist of the addition of the following new paragraphs: 3, 4.1, 5(footnote), 32, 34, 37, 37.1, 37.2, 44.1, 89(a), 109, 110, 116, 162-207 inclusive, and of new Annexes 1, 2 and 6.

3. The amendment sheet in the front of Volume I should be annotated accordingly.

NATO,
1110 Brussels.

(1) NATO UNCLASSIFIED when detached from enclosure

PERSONNEL SECURITY

Clearance of Personnel

9. All persons, civilian and military, whose duties require access to information classified CONFIDENTIAL or above should be cleared before such access is authorized. This clearance should be designed to determine whether such individuals are of:

(a) unquestioned loyalty; and

(b) such character, habits, associates and discretion as to cast no doubt upon their trustworthiness in the handling of classified information.

Particularly close scrutiny in the clearance procedures should be given to:

(c) persons to be granted access to TOP SECRET information;

(d) all persons occupying positions involving constant access to a considerable volume of information classified SECRET;

(e) persons originating from or having connections of any nature, directly or indirectly with nationals of Communist countries(1); and

(f) any other persons who may be vulnerable to pressure from foreign or other sources.

In the circumstances outlined in sub-paragraphs (c), (d), (e) and (f) above, the fullest practicable use should be made of the technique of background investigation.

10. When persons such as messengers, night custodians, etc., are employed in circumstances in which they will have special opportunities to obtain improper access to classified information, consideration should be given to their first being security cleared as if they were, in fact, authorized to have access to information of the same classification.

Removal of Personnel

11. Persons who are considered to be security risks such as those who are members of subversive organizations, or those concerning whose loyalty or trustworthiness there is reasonable doubt, should be excluded or removed from positions where they might endanger the security of the nation.

(1) A list of Communist countries is at Annex 6 to enclosure "C"

ENCLOSURE "C"

SECURITY PROCEDURES FOR THE PROTECTION OF NATO CLASSIFIED INFORMATION

INTRODUCTION

1. The detailed procedures in this document are designed to protect NATO classified informatic (1).

2. The term "NATO classified information" used throughout this document embraces all classified information, military, political and economic, circulated within NATO, whether such information originates in the Organization itself or is received from member nations or from other international organizations.

3. Classified information contributed by member nations, NATO commands or agencies or by other international organizations may be circulated, in accordance with the need-to-know principle and without reference to the originator, within the North Atlantic Treaty Organization. It should be emphasised that the information itself remains the property of the originator and may not be given to any non-NATO nations or to any other international organization except by the originator or as set out in Annexes 1 and 2.

4. If a NATO Committee believes that one of its economic, scientific or technical reports, the classification of which is not higher than NATO SECRET, is of a general interest warranting a wider distribution within NATO member governments and that it cannot

---

(1) Throughout these instructions:

(a) the words "classified information" mean any classified item, be it an oral communication of classified contents or the electrical or electronic transmission of a classified message, or be it "material" as defined in (b) below;

(b) the word "material" includes "document" as defined in (c) below and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

(c) the word "document" means any letter, note, minute, report, memorandum, signal/message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, etc. or other form of recorded information (e.g. tape recording, magnetic recording, punched card, tape, etc.)

with advantage be so distributed by declassifying it, then with the consent of the contributing governments, and the approval of the appropriate NATO authority, the following statement may be inserted by the committee at the beginning of the text of the particular document and the member governments may distribute the report:

> "Member governments are authorized, after removal of all NATO markings and the separation of this statement from the basic report, and after inclusion in the basic report of the statement 'no further dissemination is authorized without the permission of the National Security Authority', to effect its further dissemination under corresponding national classification and protection."

4.1 Although NATO UNCLASSIFIED information does not require security protection, it may only be released to non-NATO nations, organizations and individuals when such release would not be against the interests of the North Atlantic Treaty Organization. Any procedures considered necessary for such release will be decided independently by member nations and NATO commands and agencies.

5. The procedures have been set out in convenient sections so that all persons who are required to handle NATO classified information may be readily aware of their responsibility in fulfilling their particular function. It is not possible, however, in this document to allow for national and local conditions, and member nations and NATO commands and agencies(1) may require to supplement these procedures with more detailed regulations of their own.

(1) Except where specifically noted otherwise, the term "NATO command and agency" and "NATO command or agency" used throughout C-M(55)15(Final) include the following: the Military Committee, International Military Staff, Major NATO commands, NATO Military agencies, NATO International Secretariat, NATO civil agencies.

27. NATO This word is a marking which, when applied to a document, signifies:

(a) that the document is the property of NATO and if bearing a security classification may not be passed outside the Organization except under the conditions laid down in paragraph 3,

(b) that the document, if bearing a security classification, is subject to the security protection outlined in these procedures.

28. The marking NATO will be applied to all copies prepared for circulation within the North Atlantic Treaty Organization of SECRET, CONFIDENTIAL and RESTRICTED documents. The marking NATO may also be applied to UNCLASSIFIED documents.

SECTION III

ACCESS TO NATO CLASSIFIED INFORMATION

NEED-TO-KNOW

29. Access to NATO classified information will be confined to those whose duties make such access essential. No person is entitled solely by virtue of rank or appointment or security clearance to have access to NATO classified information. In each and every case the need-to-know will be established.

PERSONNEL SECURITY

30. Each member nation will be responsible for security clearing all its nationals before they are authorized access to NATO information classified TOP SECRET, SECRET or CONFIDENTIAL either in member nations or NATO commands or agencies.

31. Each member nation will, at the request of the NATO command or agency, at which a person is to take up duty, provide a completed copy of the NATO security clearance certificate (copy at Annex 3) certifying that the person has been security cleared. If any information about one of its nationals serving with a NATO command or agency is received by a member nation, which in its opinion would affect the security of NATO, that nation will either communicate such information to the security authority of the NATO command or agency concerned, in so far as national security permits, or withdraw that person's security clearance. If the latter course of action is taken, the security authority of the NATO command or agency will similarly be informed. Where such information has been obtained by a member nation in respect of a national of another member nation or by a NATO command or agency in respect of a member of its staff, the nation concerned should be advised.

32. The security clearance certificate provided under the terms of paragraph 31 for an individual on initial appointment to NATO will be based on an investigative action which was completed:

(a) in the case of personnel seconded from the armed forces or civil services, not more than three years before the date of the appointment;

(b) in the case of personnel not seconded from the armed forces or civil services, not more than nine months before the date of the appointment.

In either case, the date of expiry appearing on the certificate will in no case be more than five years from the date of the last investigative action. After the issue of the initial security clearance certificate and provided the staff member has unbroken service with NATO, the certificate will be renewed at intervals not exceeding five years with effect from the date of the last investigative action on which it was based.

BRIEFING

33. Before having access to COSMIC TOP SECRET information, all persons will be briefed on NATO security procedures and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorized hands either by intent or through negligence. Persons with access to NATO SECRET, NATO CONFIDENTIAL and NATO RESTRICTED information will be made aware of the appropriate NATO security regulations and of the consequences of negligence.

34. It is important that persons who are required to handle NATO classified information are made aware of the dangers to security arising from indiscreet conversation; on their relationship with the press; and on the threat presented by activities of hostile intelligence. Such persons will be thoroughly briefed on these dangers with particular emphasis on the serious threat to security inherent in professional or social contacts with nationals of Communist countries(1).

35. Such personnel must be urged to report immediately to the appropriate security authorities any contacts they may have with nationals of Communist countries occurring outside their normal duties and any approach or manoeuvre with suspicions of an intelligence background.

36. All personnel normally exposed to frequent contact with representatives of Communist countries must be given a briefing on the techniques known to be employed by various intelligence services.

37. Persons who have access to NATO classified information and who intend to travel to or through (including schedules stop-overs by air travel) Communist countries or to any destination by any form of transport that belongs to, is registered in, or managed from a Communist country, shall, before commencing their journey:

(a) be given a thorough briefing about the security hazards which may be involved. During the briefing, they will be requested to report as soon as they return on any occurrence, no matter how unimportant it may seem, which could have security implications;

(b) if serving in NATO commands or agencies, obtain prior approval for the journey from the head (or the officer designated by him) of their NATO command or agency who, in turn, must seek prior authority through established channels from the appropriate parent National Security Authority. Additionally, the NATO Office of Security will be consulted in cases involving NATO civil agencies and the appropriate military security authority will be consulted in cases involving NATO military commands or military agencies;

(c) if holding permanent or temporary NATO passes or NATO Civil Wartime Agencies' identification cards, deposit these documents in a secure place.

(1) Throughout C-M(55)15(FINAL) the term 'Communist countr(y)(ies)' includes any of the countries listed at Annex 6

37.1 Staff of NATO commands and agencies whose dependents wish to make similar journeys shall notify the security authority in their NATO command or agency prior to the journey. The dependents will be suitably briefed and debriefed, preferably by the security authorities concerned, or, if this is impracticable, by the person whose dependents are making the journey.

37.2 The procedures in paragraphs 37 and 37.1 above are without prejudice to any more stringent regulations of the traveller's parent nation which exist on this subject.

ACCESS TO NATO CLASSIFIED INFORMATION

38. Each individual in possession of NATO classified information is responsible for ensuring that persons to whom it is passed are authorized to have access to information of at least that specific classification.

39. The responsibility for authorizing access to NATO classified information, and for the briefing of personnel on the NATO security procedures, rests with the responsible officials of the government department or NATO command or agency in which the person is to be employed.

40. Member nations and the heads of NATO commands and agencies sponsoring delegates to conferences and meetings away from their parent organizations will transmit certification to the appropriate authorities that such delegates are authorized to have access to NATO classified information of the appropriate level. Exceptionally, such certification may be hand-carried by the delegates concerned. A copy of the certificate of security clearance to be used for all visits, except repeated visits or visits to facilities in more than one member country to be made under the terms of Section VI of Enclosure 'D', is at Annex 4.

41. Persons outside regular government or NATO employment on NATO or national business requiring access to NATO classified information do so under the sponsorship of their own government and will be security cleared and briefed as to their responsibility for security.

ACCESS TO COSMIC TOP SECRET INFORMATION

42. Access to COSMIC TOP SECRET information must be specially controlled. Those who are required to have such access will be specifically designated by the government department or NATO command or agency concerned, and their names will be recorded in the appropriate COSMIC registry or control point.

43. All persons to be authorized access to COSMIC TOP SECRET information will sign a certificate to the effect that they have been briefed on NATO security procedures and that they fully understand their special and continuing responsibility for safeguarding COSMIC TOP SECRET information, and the consequences of unauthorized disclosure of classified information either by intent or through negligence.

44. The names of all persons ceasing to be employed in duties requiring access to COSMIC TOP SECRET information will be removed from the COSMIC list. All persons will be reminded of their special and continuing responsibility for the safeguarding of COSMIC TOP SECRET information and will sign a certificate to the effect that they understand this. Should any such person be re-employed on duties requiring access to COSMIC TOP SECRET information, the procedures in paragraphs 33 to 37.2, 42 and 43 above will be completed by the new department in which the person is to be employed.

ACCESS TO NATO CRYPTO INFORMATION

44.1 Security clearance procedures for establishing a person's eligibility to have access to NATO classified information are equally applicable for eligibility to have access to NATO crypto information. In addition, individuals who in the normal course of their duties are required to have continuous access to NATO high grade key material or crypto information of a sensitive nature must be specifically authorized in accordance with the procedures set forth in NATO crypto security instructions which have been promulgated by the Military Committee.

INTERIM ACCESS TO NATO CLASSIFIED INFORMATION IN AN EMERGENCY

45. In wartime or in periods of mounting international tension when emergency measures require it, member nations and heads of NATO commands and agencies may in exceptional circumstances grant by a written authorization access to NATO classified information to persons who do not possess the requisite security clearance provided that such authorization is absolutely necessary and there are no reasonable doubts as to the trustworthiness of the person concerned.

46. In the particular case of COSMIC TOP SECRET information, this emergency access will be confined wherever possible to those personnel whose clearances already afford them access to NATO SECRET or NATO CONFIDENTIAL information.

47. Whenever such emergency access is granted a record of the authorization will be made by the authority concerned who will, as soon as possible, institute the procedures necessary to fulfil the normal clearance requirements.

DISTRIBUTION

86. Distribution of NATO classified documents will be on a need-to-know basis. Documents classified NATO CONFIDENTIAL and above will be restricted to persons currently authorized to have access to such information.

87. The initial distribution of documents classified NATO CONFIDENTIAL and above should be specified by the originator. The addressee may authorize such wider distribution as may be required in accordance with the principle laid down in paragraph 86 above.

88. Distribution of COSMIC TOP SECRET documents will be through registry channels except as provided for in paragraph 119. COSMIC TOP SECRET documents on loan outside a registry or control point will be returned when no longer required.

EXTRA COPIES, TRANSLATIONS AND EXTRACTS

89. If an addressee requires extra copies of a COSMIC TOP SECRET document these should normally be obtained, except in the case of a signal/message, from the originating member nation or NATO command or agency. It is recognized, however, that it may be necessary in exceptional cases for an addressee to make copies or translations of COSMIC TOP SECRET documents. In such cases reproductions or translations of COSMIC TOP SECRET documents and signals/messages must:

(a) be authorized by the Control Officer(1) of a COSMIC central registry. This authorization may be delegated to a Control Officer of a COSMIC sub-registry but in such cases a report of such reproduction or translation will be reported to the COSMIC central registry who will monitor such reproductions and translations and record the copies made. In the case of a signal/message the officer in charge of the signal office primarily concerned may authorize the production of those copies and translations necessary to make initial distribution. Thereafter the authority for reproduction and translation of signals/messages will be the same as for other COSMIC TOP SECRET documents;

(b) bear the reference and copy number of the original document together with the name of the originating authority and that of the reproducing element;

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

(d) display the COSMIC TOP SECRET marking and classification and all other markings accorded to the original document;

(1) The terms Control Officer of a COSMIC central registry; Control Officer of a COSMIC sub-registry; and COSMIC Control Officer throughout this Section and Section VII include their alternates - see paragraph 116

(ii) copies when produced are brought under registry and inventory control applicable to COSMIC TOP SECRET documents and reported in the annual muster along with other COSMIC TOP SECRET documents held;

(iii) the Control Officer of a sub-registry authorizing reproduction from microfilm reports the number of copies made to the Control Officer of the COSMIC central registry.

TRANSMISSION

Packaging

97. Documents classified NATO CONFIDENTIAL and above will be transmitted under double opaque and strong cover. The inner cover will be secured and bear the marking COSMIC or NATO as appropriate together with the security classification. The inner cover will be enclosed in a secure outer cover. The outer cover will bear an address and a package number for receipting purposes and will not indicate the classification of the contents or the fact that it contains classified information. If documents are transmitted under double cover by courier, the outer cover should be clearly marked, e.g., "by courier only". A locked pouch or box or a sealed diplomatic pouch may be considered as the outer cover.

98. When NATO classified documents are carried between offices of the same building or enclosed group of buildings by officials (other than messengers), they will be covered in such a way as to prevent observation of their contents. If they are carried by messengers they will be enclosed so that the messenger does not have access.

Document Control

99. A receipt will be enclosed in the inner cover of COSMIC TOP SECRET and NATO SECRET documents. NATO CONFIDENTIAL documents will be receipted for only if required by the transmitter. The receipt will be immediately returned to the sender after having been dated and signed. COSMIC TOP SECRET documents transmitted between registries and control points will be opened and receipted for only by a COSMIC Control Officer. In exceptional circumstances the inner cover of a COSMIC TOP SECRET document may be addressed to an individual through a COSMIC Control Officer, in which case only that individual will open and receipt for the documents. The receipt and disposal of such documents will be recorded in the usual manner.

100. A continuous receipt system is required for COSMIC TOP SECRET documents. For transmission of NATO SECRET documents within member nations and NATO command and agencies, each member nation or NATO command or agency concerned will establish internal controls, to include periodic inspections, and such other appropriate measures as will ensure that NATO SECRET documents are controlled and their movements recorded.

101. A receipt, which requires no security classification, will quote only the reference number, date, copy number and language of the document and not its title.

102. For NATO CONFIDENTIAL and above couriers and messengers will obtain receipts against package numbers. Receipts for packages containing NATO CONFIDENTIAL documents are only required if carried outside the confines of a building or enclosed group of buildings.

Personal Carriage

103. Each member nation and NATO command and agency will prepare instructions covering the personal carriage of documents classified NATO CONFIDENTIAL and above based on these regulations. The bearer will be required to read and sign these instructions. In particular, the instructions should make it quite clear that in no circumstances:

(a) may the documents leave the possession of the bearer unless they are housed in accordance with the provisions for safe custody contained in Section IV above;

(b) may documents be left unattended (e.g. in hotels, and vehicles) or stored in hotel safes or luggage lockers;

(c) may documents be read in public places (e.g. in aircraft, trains, etc.).

INTERNATIONAL TRANSMISSION

104. Documents classified NATO CONFIDENTIAL and above will be conveyed by diplomatic pouch or military courier service. In addition, NATO SECRET and NATO CONFIDENTIAL documents may be transmitted by registered mail through specific postal services approved by the NATO Office of Security.

105. Exceptionally, documents classified NATO CONFIDENTIAL and above may be carried by hand of persons other than couriers provided:

(a) they are authorized access at least to the level of classification of the documents carried;

(b) that a record is held in the appropriate registry in the case of COSMIC TOP SECRET documents, and in the appropriate offices in the case of NATO SECRET and NATO CONFIDENTIAL documents, of all documents carried. The receipt for the documents or the actual documents, if returned, should be checked against this record;

(c) the documents will be carried in a locked container which will bear a label with an identification and instructions to the finder;

(d) this container will be covered by an official seal, or likewise protected under procedures designed to prevent customs examination;

(e) the bearer carries a courier certificate (copy at Annex 5) recognized by all NATO nations authorizing him to carry the package as identified;

(f) the bearer does not travel either by surface routes through non-NATO nations or by air routes over Communist countries. When speed is of paramount importance, this restriction may be waived on the specific authority of the head of the NATO command or agency or his authorized designate or by the appropriate authority of the member nation.

NATIONAL TRANSMISSION

106. National transmission of documents classified NATO CONFIDENTIAL and above will be by authorized messenger service, courier or hand of person authorized to have access at least to the level of the classification of the documents carried. Additionally NATO SECRET and NATO CONFIDENTIAL documents may be transmitted by registered or insured mail if such transmission is permitted under national regulations.

107. Whenever a messenger service is used for the carriage of documents classified NATO CONFIDENTIAL and above outside the confines of a building or an enclosed group of buildings, the packaging and receipting provision contained in paragraphs 97 to 99 and 102 above will be complied with. Exceptionally documents classified NATO CONFIDENTIAL and above may be carried within a member nation provided the provisions of paragraphs 103 and 105(a), (b) and (c) are complied with.

TRANSMISSION OF NATO RESTRICTED DOCUMENTS

108. NATO RESTRICTED material will be transmitted nationally or internationally by such means as are authorized by the appropriate National Security Authority. In the case of NATO commands and agencies, the rules governing such transmissions will be set by the head of the command or agency after agreement with the National Security Authority of the member nation in which the material is despatched.

ELECTRICAL TRANSMISSION

109. Signals/messages will be accorded at least equivalent protection to that laid down for other documents of the same classification. When electrically transmitted, messages classified NATO CONFIDENTIAL and

above will be encyphered and if classified COSMIC TOP SECRET or NATO SECRET only the cryptographic systems specifically authorized by the Military Committee will be used. The handling of COSMIC TOP SECRET messages in signal centres will be restricted to officers or other specially designated cryptographic personnel whose number should be kept to a minimum. In addition, each message or signal centre used for the receipt of encyphered NATO classified messages will initiate a system to ensure that persons not authorized access to NATO classified information will not gain such information through reviewing incoming message files. NATO RESTRICTED messages will be encyphered when transmitted across national frontiers. They will also be encyphered when transmitted nationally except where the means of encyphering is not available or speed is of paramount importance; in such cases, they may be passed in clear text over the telex system provided national security regulations allow such transmission.

110. Telephones even with speech inversion equipment will not normally be used in the discussion of information classified NATO CONFIDENTIAL and above. As an exception such classified information may be conveyed by telephone when secure voice equipment evaluated and approved by the Military Committee is used. Information so conveyed will not exceed the classification levels for which approval has been given. The discussion of NATO RESTRICTED information over the telephone will be subject to the regulations laid down by the National Security Authority of the member nation in which the call originates.

SECURITY OF COURIER AND MESSENGER PERSONNEL

111. All couriers and messengers employed to carry documents classified NATO CONFIDENTIAL and above will be security cleared by the appropriate national authority. There is, however, no necessity for such persons to be briefed on NATO security procedures. Couriers and messengers will be instructed on their duties for protecting the documents entrusted to them.

DESTRUCTION OF NATO CLASSIFIED DOCUMENTS

Routine Destruction

112. To prevent unnecessary accumulation, superseded documents and documents no longer needed will be destroyed as soon as practicable. It is not necessary to await destruction instructions from the originator. Holders of NATO classified documents will maintain a continuing review of them to determine whether they can be destroyed.

113. Surplus or superseded classified documents including all classified waste such as spoilt copies, working drafts, shorthand notes, carbon paper, etc. will be destroyed under appropriate security regulations and supervision by burning, reducing to pulp, shredding or pulverising into an unrecognizable form and beyond reconstruction:

(a) except as provided for in sub-paragraph (c) all COSMIC TOP SECRET documents for destruction will be returned to the registry which holds them on charge. Each COSMIC TOP SECRET document will be listed on a certificate of destruction which is to be signed by the COSMIC Control Officer and by the official witnessing the destruction who must be authorized to have access to COSMIC TOP SECRET information. Destruction certificates of COSMIC TOP SECRET documents which have been microfilmed should so indicate that fact;

SECTION VII

COSMIC REGISTRIES AND CONTROL POINTS

116. The purpose of COSMIC registries and control points is to ensure the correct recording, handling and distribution of COSMIC TOP SECRET documents. The head of the COSMIC registry or control point is designated the "COSMIC Control Officer". Alternate COSMIC Control Officers should be designated as necessary. An alternate COSMIC Control Officer may perform some of the duties of the COSMIC Control Officer on a permanent basis and will assume all authority and responsibility during the latter's absence.

117. Central registries act as the main receiving and despatching authority for the member nation or NATO command or agency within which they have been established. Central registries may also act as sub-registries where appropriate.

118. Sub-registries are responsible for the internal distribution of COSMIC TOP SECRET documents and for keeping records of the location of each document held on the sub-registry's charge. When issued on temporary loan to other than a control point, such records will include the individual custody.

119. A COSMIC control point is an administrative means for assisting in the control of COSMIC TOP SECRET documents below the registry level. Its primary purpose is to provide facilities for the receipt, routing, and custody of COSMIC TOP SECRET documents received from the registry under which it operates, and when authorized from other COSMIC central registries, sub-registries or control points and to control them when on temporary loan to individual users.

120. COSMIC control points may be established in accordance with regulations issued by the appropriate National Security Authority, the Secretary General, the Military Committee or Major NATO Commanders. Infrequent and temporary access to COSMIC TOP SECRET documents does not necessarily require the establishment of a COSMIC control point provided procedures assure that the documents remain under the control of the appropriate COSMIC registry or existing control points.

121. In exceptional circumstances control points may be authorized to exchange COSMIC TOP SECRET documents directly with other registries and control points provided that the transmission and receipt is recorded in the registries responsible for holding the documents on charge.

122. Control points are responsible for keeping up-to-date records of the individual custody of all COSMIC TOP SECRET documents in their charge.

123. In order to expedite NATO business, and for administrative economy, sub-registries and control points may be authorized by the appropriate authority of the member nation or NATO command or agency to transmit COSMIC TOP SECRET documents direct to other sub-registries and control points within the same member nation or NATO command or agency.

SECTION X

PROTECTION OF NATO CLASSIFIED INFORMATION HANDLED AND STORED IN AUTOMATIC DATA PROCESSING SYSTEMS

INTRODUCTION

162. The security policy and requirements in this Section apply to all automatic data processing systems processing NATO classified information except ADP systems and installations used solely for communications purposes. The securit requirements for such communications computers are defined elsewhere. Because these are based on the same security principles, this will not inhibit interface between data processing and communications computers when necessary. Furthermore, paragraphs 165 through 167 and 177 through 181 apply only to automatic data processing systems operated by NATO commands and agencies. Some ADP systems currently used or already initiated may not permit attainment of all the objectives immediately but every effort should be made for their earliest practicable inclusion. They must be included in all systems initiated at a future date. Any computer or terminals which are connected to the NATO systems must meet the requirements of this Section.

GENERAL

163. ADP installations are capable of processing and storing large amounts of NATO classified information in a compact form designed to permit its quick retrieval and use. Within ADP installations it is not always practical to implement the "need-to-know" principle to the same extent as in a conventional office and opportunities are increased for the surreptitious acquisition of information. These installations are, therefore, attractive espionage targets. The complex electronic equipment comprising an ADP system is expensive, difficult to repair or to replace rapidly and is very vulnerable to accidental or malicious damage.

164. To achieve protection equivalent to that afforded under conventional circumstances, ADP installations processing NATO classified information require the highest appropriate standards of conventional security coupled with special security procedures and techniques designed for automatic data processing.

SECURITY RESPONSIBILITY

165. The responsibility for security of ADP systems will rest with the security authority of the NATO organization. This responsibility is distinct from that of operational responsibility vested with the

operational element of the organization as described in paragraph 169. As the security problems will include areas which are covered by the communications security and counter-intelligence services, proper co-operation and co-ordination between the different elements must be assured.

166. Similarly, co-operation and co-ordination between the ADP authority and the security authority are essential from the outset whenever an organization:

(a) plans to develop or acquire an ADP system;

(b) proposes to make changes to an existing configuration;

(c) proposes to make significant changes to the mode of operation;

(d) proposes to make significant changes to existing, or to adopt new, controlling systems software (see paragraph 195);

(e) proposes to undertake work of a higher security classification than has previously been processed by an existing ADP installation.

167. The security authority and the ADP authority will decide on security measures to be applied by the suppliers during the installation and testing stages.

168. The ADP authority will be responsible for the implementation and control of the special security features designed as part of the overall ADP system. Before an ADP system becomes operative, the responsibilities for the implementation and supervision of security during operation must be detailed.

169. The head of the office immediately responsible for an ADP system will designate from his ADP staff an ADP security officer to whom will be delegated the responsibility for the supervision of the implementation of the security provisions within the ADP system, including those outlined in the Operating Procedures (paragraph 207 below).

PERSONNEL SECURITY

170. Because of the vulnerabilities described in paragraph 163 above, particular care must be taken over the training and supervision of ADP staff.

Clearance of Staff

171. Individuals must be cleared to the highest classification and category of information to which their duties could possibly give them access.

Compartmentalization of Staff Duty Assignments

172. Wherever possible, duties and responsibilities should be so allocated to ADP staff that no one person has complete knowledge or control of the system security key and software. The aim should be that collusion between two or more individuals would be necessary for surreptitious acquisition of NATO classified information or intentional degradation of the system.

TRAINING

173. In order to ensure that security measures are sensibly devised and implemented, ADP and security staff with responsibility for ADP security must be trained to the extent necessary to understand each other's problems.

AUTOMATIC DATA PROCESSING SYSTEMS

Design of Security Safeguards

174. The aim of the design must be:

(a) to prevent unauthorized access to NATO classified information;

(b) to detect, abort and report attempts to obtain unauthorized access; and

(c) to detect and report unauthorized access after the event.

An evaluation of the security features of the hardware and software must be made and consideration given to the design of additional measures and procedures necessary to give an acceptable degree of protection to NATO classified information. Monitoring and auditing facilities should be provided to allow a continuous check on security to be carried out.

175. Any means for the electrical transmission of NATO classified information outside the ADP centre must satisfy pertinent communications security standards.

176. A central computer facility must have the capability of positively denying access to NATO classified information to any or all of its remote terminals, when required, either by physical disconnection or by special software features approved by the security authority.

Procurement

177. Procurement of ADP systems will be limited, in so far as possible, to systems designed and manufactured in NATO member nations. Specifications for procurement should include the requirement that appropriate security safeguards are incorporated in the system. A complete description of these safeguards and how they function should be made available by the supplier. The specifications should also include a requirement for the supplier to provide, on request, documentation on all hardware and software as originally supplied, to identify any subsequent modifications and to state how they affect the operation of the security features.

178. In deciding whether equipment to be used for classified work should be purchased or leased, it must be borne in mind that such equipment, if classified, cannot be released outside an appropriately secure environment without first being declassified to the approval of the security authority and that such approval may not always be possible.

Installation

179. Installation of ADP systems should be so specified that installation is carried out by security qualified installers under constant supervision of technically qualified personnel who are cleared for access to NATO classified information to the level equivalent to the highest classification which the ADP system is expected to handle. All equipment must be installed in accordance with NATO directives pertinent to the installation of electrical/electronic equipment for the processing of classified information.

Acceptance Testing and System Approval

180. The suppliers of an ADP system should give an assurance that it incorporates the security features required by the procurement specification. Before the system is used for processing NATO classified information, it should be subjected to security testing and approval by an independent team of technically qualified and appropriately security cleared personnel acting for the user organization.

Maintenance

181. Contracts for scheduled and on-call maintenance of ADP systems processing NATO classified information must specify requirements and/or arrangements for maintenance personnel who must enter the classified ADP area or who may acquire access to NATO classified information in the course of their maintenance duties (see paragraphs 171 and 184).

Routine Checking of Security Features for Continued Approval

182. After acceptance, the correct operation of security features should be checked as often as possible, and in the case of NATO commands and agencies at least once annually. It must also be checked after any modification, repair or failure any of which could have affected the security safeguards of the system. Continued approval of the system depends on the satisfactory completion of the checks. Changes will be effected in conjunction with the relevant security authority.

PHYSICAL SECURITY

Classified ADP Areas

183. Areas in which classified information is transcribed or processed or stored by ADP means, must be designated as classified ADP areas and established as NATO Class I or Class II security areas or national equivalent, as appropriate.

Control of Entry

184. Entry to and departure from the classified ADP areas of both people and material will be controlled by positive means. Individuals requiring temporary or intermittent access to these areas will be authorized entry as visitors by the responsible security authority. Visitors must be supervised at all times to ensure they are denied unauthorized access to NATO classified information and that they do not gain access to the ADP equipment for illicit purposes.

Application of Physical Security Measures

185. Physical security measures appropriate to the highest category of information normally processed or stored must be applied at all times to the classified ADP areas. A central computer facility should never be occupied by only one authorized individual.

SECURITY OF INFORMATION

Classification

186. It is the responsibility of the requester of the information to be processed, in consultation, where necessary, with the system analyst/programmer to identify and classify all input, programmes, data files and output and any intermediate form in which his data will be recorded during processing. The agreed classification must be included in the system and/or programme documentation. Output will have the same classification as the data used for its production, unless the competent authority has agreed, after review, to a different one - see also paragraph 71. The fact that the data may be in a brevity code, transmission code or in any form of binary representation does not provide any security protection and should not, therefore, influence the classification of the data.

187. Re-usable storage media used for recording classified information shall retain the highest classification for which they have ever been used until destroyed or properly declassified.

Identification

188. User data input and output in documentary form shall be identified by control number, user identity, security classification and date. Where possible, the system shall identify each terminal with its authorized users and each combination of terminal and authorized user with the access allowed. The beginning and end of all classified output deriving from user data bases shall be indicated and each page of printout shall be numbered and marked with the classification. Multiple copies of material classified COSMIC TOP SECRET and NATO SECRET and special categories of information (e.g. ATOMAL and SIOP) will be identified individually and assigned copy numbers prior to release. Classified outputs produced for reproduction purposes will be identified as reproduction masters and controlled appropriately.

Marking

189. Information must be clearly marked with its classification in plain language before being removed from the classified ADP area. Within the classified ADP area plain language classification markings will be used whenever practicable. When not practicable, a locally devised classification code must be used.

Control

190. Manual and, where possible, automatic logs will be kept to control NATO classified information through all its stages of processing and storage. These logs should be retained for a period to be agreed with the security authority.

191. Except as stated in paragraph 192 below, classified ADP output and material containing accountable information shall be transferred from the classified ADP area to a recipient only by prescribed classified document control procedures. Classified information recorded in machine readable form, i.e. magnetic tape, punched tape and punched cards, etc., will be identified and described on the receipt form as to classification, subject and content.

192. Information connected with a particular classified job held within the classified ADP area or in the custody and under the control of the individual for whom the material was originally produced, may be handled as one classified item and need not be registered with the central (or other) document registry, provided the material is identified, marked with its classification and controlled within the classified ADP area until reduced to record copy and placed on permanent file, or entered into transmission channels or destroyed. This material may be handled as classified working papers and held in approved storage facilities for the minimum required period after which time it shall either be brought under formal document accountability or destroyed. Appropriate records and control of bulk classified material shall be maintained by the custodian and the ADP centre until the material is brought under formal document accountability control or destroyed.

Destruction of NATO Classified Information Stored on Removable ADP Media

193. Electromagnetically recorded NATO classified information should be destroyed by approved methods as soon as it is no longer required. When a storage medium comes to the end of its useful life, it should be physically destroyed unless it can be released under the terms of paragraph 178. NATO classified information in hard copy (i.e. printout, punched cards, punched tape, etc.) should be destroyed by procedures approved for the destruction of NATO classified material as laid down in Section VI.

Access Codes or Security Keys

194. All information controlling access to data must be clearly identified and protected under such arrangements as prescribed for the highest classified information to which it may give access.

Controlling Systems Software

195. Master copies of all controlling systems software(1) in use should be stored under the most secure conditions available. The versions in use should be verified at regular intervals to ensure their integrity and correct functioning in order to preclude security violations. New versions of any controlling systems software should not be used for the processing of NATO classified information until the software security features have been thoroughly checked.

Handling and Control of Removable Magnetic Stores

196. All removable magnetic stores held within a classified ADP area must be properly identified and controlled. The control must include:

(a) means of identification for each separate medium;

(b) records, manual or by computer, of the general content and classification of the information; and

(c) fixed procedures for entry into and release from the area and for final disposition of the stores by destruction or other methods.

To avoid confusion in manual systems of having, for example, NATO SECRE information recorded on a magnetic tape marked COSMIC TOP SECRET (see paragraph 187), it is recommended that the locally devised classification code referred to in paragraph 189 should be amplified to show the disposition category of the store as well as the classification of the information recorded on it.

(1) All systems software which may be present to control the execution of applications software or the interaction of computer system components

Electrically Transmitted Information

197. The information passed between a central computer facility and its remote terminals or between two or more ADP systems, shall include, as a preamble, the highest NATO security classification of the information being transmitted as well as any other information needed to control its proper handling, processing and distribution.

Protection against Compromising Radiations and Clandestine Devices

198. Where required by the security authority a technical inspection and radiation survey of the ADP system shall be carried out by a technically qualified security inspection team and appropriate corrective measures taken before the system is allowed to begin processing classified information. To ensure continued conformity with the criteria in NATO directives pertinent to the installation of electrical equipment for the processing of classified information, such technical inspections and radiation surveys shall be repeated after any major change in the configuration or after any new conductor has been introduced into or through the inspected zone or at intervals as required by the security authority. Additionally, such technical inspections and radiation surveys will be carried out at least once a year in NATO commands and agencies.

199. Where the possibility of technical security or counter-intelligence monitoring of signals exists, the monitoring sweeps should include examination of those frequencies which might carry signals originating from the ADP system and should be performed at such intervals as to intercept signals originating from the ADP system during periods of classified operations.

200. Before an ADP system first processes classified work, its rooms, furnishings and ancillary devices shall be comprehensively examined for the detection and neutralization of clandestine intelligence devices. Such examinations shall be conducted by qualified counter-intelligence teams and repeated at intervals as required by the security authority. These examinations will be carried out once a year, in NATO commands and agencies.

SECURITY DURING PROCESSING

201. Until and unless it shall have been proved to the contrary, it must be assumed that no software or hardware features can be relied upon, either individually or in combination

to prevent or detect unauthorized acquisition of information by a person who has good knowledge of the system and who has authority to enter the computer room, submit a job over the counter, or use a terminal or who has access to any other entry port(1). These features must, therefore, be augmented by additional security measures including, where necessary, restrictions on certain modes of processing.

202. When special category information, i.e. ATOMAL and SIOP, or information classified COSMIC TOP SECRET is being processed, the equipment used should be dedicated to this category and/or classification. When such de lication is impracticable, information concurrently processed ithin the ADP system must be held at the COSMIC TOP SECRET and/or special category level until reviewed (see paragraph 186) and all terminals not authorized access to this level and category of information must be denied access (see paragraph 176).

203. Each ADP system qualified for NATO classified work will ensure that security measures are in effect to permit access by only specified and authorized personnel to classified information processed or produced. This may be accomplished through such ADP access control techniques as a user identity code, a terminal identity code, and an information identity code or a combination thereof. An information identity code or some other equivalent technique shall be used to control access to all data or information on all classified ADP systems.

204. The access control measures shall allow NATO classified data or information to be transmitted to or received from only authorized local or remote terminals which are manned by authorized personnel. Release of NATO classified information to unmanned facilities will be prohibited unless special arrangements are in force.

205. The security measures should also be capable of aborting any unauthorized attempt to gain access to NATO classified data or information and to record and display or print at the ADP centre pertinent information concerning the attempt so that the officer in charge of operations can take immediate action and report the incident to the responsible security authority.

(1) Any facility or point of access whereby data or information may be passed to or from an ADP system

206. System security features will allocate to each local and remote terminal used for automatic data processing of NATO classified information an entry port which the system shall recognize and verify prior to passing NATO classified data to the terminal. The system shall also be capable of positively checking that the requesting user, the terminal and the communications link(s) via which the terminal is accessed, are authorized for such data.

OPERATING PROCEDURES

207. Organizations having ADP systems will issue instructions covering operating procedures for processing of NATO classified information. Such instructions will be prepared by the ADP authority in consultation, where appropriate, with the security authority, who will co-ordinate with other security elements concerned. The instructions must cover where applicable, the aspects listed hereunder:

(a) the allocation of security responsibilities to particular members of the staff;

(b) arrangements for liaison with the organization's security authority;

(c) the personnel authorized routine access to the classified ADP areas, their duties and responsibilities;

(d) arrangements for the establishment and maintenance of a list of authorized users and their access control codes and for the safeguarding of the latter;

(e) visitor control and the measures to be taken for preventing unauthorized personnal having access to classified information;

(f) receipt of input;

(g) the control of the collection, distribution and transmission of output;

(h) control of all storage media;

(i) destruction of classified information;

(j) methods of marking identification and classification on all information-carrying media;

(k) handling of work within the classified ADP area and the records to be kept in this respect;

(l) periodic accountability control, inventory and audit of all classified holdings within an ADP centre;

(m) measures to ensure the integrity of software;

(n) computer configuration to be used for processing under various conditions, including any terminals to be denied access and any peripheral equipments which are to be disabled;

(o) security classification and category and description of data which may not be processed under normal operating conditions and actions to be taken before such information may be processed

(p) details of the precautions to be taken before and after processing or preparing different types of classified work, including routines for clearing main memory and clearing all stores, including those associated with peripheral devices and data processing apparatus;

(q) running of monitor or audit programmes and scrutiny of the records created by such programmes for detection of unauthorized attempted access;

(r) examination of manual records and the computer logs in order to ensure that instructions are being followed;

(s) detailed procedures to be followed in the event of failure of systems components, power outage or other fault conditions which could affect the reliability and/or operational characteristics of the ADP systems security features;

(t) guidance to ADP users, for example, about preparation of input including security requirements, responsibility for classification, safeguarding of user identification, and file access passwords, and reporting unusual incidents which might be relevant to security such as receipt of wrong output;

(u) the responsible authority who shall approve procedures under which the remote terminals shall resume processing classified data or producing classified information after

such processing or producing has been suspended because of suspicious actions, e.g., unauthorized attempts to gain access;

(v) an emergency destruction plan for all classified ADP information.

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO INTERNATIONAL ORGANIZATIONS OUTSIDE THE NORTH ATLANTIC TREATY ORGANIZATION COMPOSED ONLY OF SOME OR ALL NATO NATIONS

1. Any member nation or NATO command or agency considering it would be advantageous to NATO to release to an international organization, outside the North Atlantic Treaty Organization, composed only of some or all NATO member nations NATO classified information up to and including COSMIC TOP SECRET but excluding that originated by one or more of the nations participating in a NATO Production and Logistics Organization or other organization granted a charter under the terms of C-M(62)18 or generated within such an organization and pertaining to it - see paragraph 3 below - will submit an application for its release to the Military Committee or NATO civil committee most concerned with the information(1).

2. The authority to release such NATO classified information will rest exclusively with either the Council or the relevant committee. In the case of information referred to a NATO civil committee that committee will authorize its release, provided it is unanimous that the information may be released and provided the information is not classified higher than NATO CONFIDENTIAL. If the information is classified COSMIC TOP SECRET or NATO SECRET, the NATO civil committee, having agreed that the information should be released, will seek the approval of Council, for its dissemination. Normally, such approval will be sought case by case but where there is a need to release a certain type of information on a continuing basis, Council may authorize the NATO civil committee to act on its behalf. (If the originator of the information, for which release is desired, is not a member of the relevant committee, that committee must first seek the originator's consent to the release, if the originator or originators cannot be established the relevant committee will assume the responsibility of the originator.)

3. In the case of NATO classified information originated by one or more of the nations participating in a NATO Production and Logistics Organization or other organization granted a charter under the terms of C-M(62)18 or generated within that organization and pertaining to it, the application for release - see paragraph 1 above - will be submitted to the Board of Directors (or to any other body designated by higher authority) of the NATO organization concerned.

(1) For ease of reference, hereafter in this Annex the term "relevant committee" will be used in lieu of the expression "as appropriate, either to the Military Committee or to the NATO civil committee most concerned with the information"

Provided it unanimously agrees that the information should be released, the Board of Directors (or any other body designated by higher authority) will seek the approval of the National Security Authorities of the nations participating in the NATO organization programme for its dissemination. If approval is given, the information will be passed in accordance with the procedures referred to in paragraph 4 below. The NATO organization concerned will maintain records of all NATO classified information passed under these procedures together with the written confirmation mentioned in paragraph 4 below. These records will be subject to examination by the NATO Office of Security during their annual inspections.

4. When approval for release has been given and before any NATO classified information is passed to such an international organization, that organization will confirm, in writing, to the security authority of the member nation or NATO command or agency or NPLO (or other) Management Agency making the release, with a copy to the NATO Office of Security, that the relevant paragraphs of the Security Regulations set out in the attached Appendix will be implemented at all times. Normally, this written confirmation will be required only before NATO classified information is passed to the international organization for the first time. Subsequent confirmation may be required as a result of an inspection by the NATO Office of Security.

SECURITY REGULATIONS TO ENSURE THE PROTECTION OF NATO CLASSIFIED INFORMATION PASSED BY THE NORTH ATLANTIC TREATY ORGANIZATION TO AN INTERNATIONAL ORGANIZATION COMPOSED ONLY OF SOME OR ALL NATO NATIONS

PERSONNEL

1. The number of officials of the international organizations who will have access to NATO classified information must be strictly confined to those whose duties make such access essential according to the principle of the need-to-know. It will be the responsibility of the Military Committee or the NATO civil committee most concerned with the information to be passed, or of the Board of Directors (or of any other body designated by higher authority) in respect of information pertaining to NATO Production and Logistics Organizations (NPLO) and other organizations governed by the terms of C-M(62)18, to obtain assurances from the recipient organization that the individuals of that organization who will be given access to the NATO information hold NATO security clearances, at the appropriate level, issued by their parent governments and that the number of such individuals is kept as low as possible consistent with the efficient use of the information.

2. Security clearance certificates for the individuals concerned must be provided to the NATO Headquarters Security Service, or to the security authority of the NPLO or other organization concerned before such individuals can have access to NATO classified information.

DOCUMENTS

3. The selection of NATO documents to be transmitted to the international organization rests exclusively with the Military Committee or the NATO civil committee or the Board of Directors (or any other body designated by higher authority), as appropriate, referred to in paragraph 1 above.

Despatching

4. NATO documents selected in accordance with paragraph 3 above will be forwarded to the international organization through approved channels as laid down in Section VI of Enclosure "C".

Packaging

5. The double cover system will be used. The inner cover will be marked "NATO", together with the security classification. A receipt form will be enclosed for each NATO classified document. The receipt

form, which requires no security classification, should quote only the reference number, date, copy number and language of the document and not its title.

6. The inner cover will be enclosed in an outer cover which will bear a package number for receipting purposes. Under no circumstances will any security classification appear on the outer envelope.

7. Messengers will always obtain receipts against package numbers.

Registration on Arrival

8. As soon as a NATO classified document is received, it will be listed in a special register, held by the organization, the pages of which will bear columns indicating the date received, the date of the document, its serial number, its copy number, its security classification, its title, the date when the receipt is returned and the date the document, when no longer required, is sent back to NATO.

Custody and Security Protection

9. When not in use, documents will be stored in a security container which is approved for the storage of national documents of the same classification as the NATO document. Such containers will bear no indication of their contents, which will be accessible only to those authorized to have access to NATO classified information. In the case of combination locks, the combination will be known only to the officials of the international organization authorized access to NATO classified information and will be changed every six months, or sooner in case of transfer of an authorized official, or when compromise is suspected.

10. NATO classified documents may only be removed from the security container in which they are housed, by members of the international organization who are authorised to have access to the documents. The person removing a document from the security container will be responsible for ensuring its safe custody at all times until he replaces it in the container. In particular, he must ensure that no one, who is not authorised to see the document, has access to it.

11. No copies or extracts of NATO classified documents will be made.

12. Plans for the destruction in an emergency of NATO classified documents should be prepared.

Breaches of Security

13. When a breach of security involving a NATO classified document occurs or is suspected, the following action should be taken immediately:

(a) discover the circumstances of the breach of security;

(b) notify the NATO Office of Security;

(c) minimize the damage done;

(d) devise measures to prevent recurrence;

(e) implement any recommendations made by the NATO Office of Security to prevent a recurrence.

PHYSICAL

14. When not in use, any security container used for the storage of NATO classified documents will at all times be kept securely locked.

15. When maintenance personnel or cleaners are required to enter or remain in the room in which the security container is located, they must at all times be escorted by a member of the international organization's security section.

16. Outside office hours (at night, week-ends and holidays) protection of the security container will be provided either by a watchman or by an automatic alarm system.

INSPECTIONS

17. The NATO Office of Security will be permitted to carry out inspections of the security measures in force to protect NATO classified information within the international organization.

REPORTS

18. So long as the international organization holds NATO classified information it will submit an annual report, to reach the NATO Office of Security by 31st January each year, to confirm the above security regulations are being implemented.

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND TO INTERNATIONAL ORGANIZATIONS COMPOSED EITHER WHOLLY OR PARTLY OF NON-NATO NATIONS

1. Any member nation or NATO command or agency considering it would be advantageous to NATO to release to a non-NATO nation or to an international organization composed either wholly or partly of non-NATO nations, information classified up to and including NATO SECRET, excluding that originated by one or more of the nations participating in a NATO Production and Logistics Organization or other organization granted a charter under the terms of C-M(62)18 or generated within such an organization and pertaining to it - see paragraph 3 below - will, as a sponsor, submit an application for its release as appropriate, either to the Military Committee or to the NATO civil committee most concerned with the information(1). The application should:

(a) establish the need-to-know of the intended recipient;

(b) define the advantage which would accrue to NATO if the release were made.

2. The authority to release the NATO classified information in question will rest exclusively with either the Council or the Military Committee. In the case of information for which release must be approved by Council, the NATO civil committee most concerned will first consider the request, and only if it supports the application will the approval of Council be sought for its dissemination. This will be done by the silence procedure. (If the originator of the information, for which release is desired, is not a member of the relevant committee, that committee must first seek the originator's consent to the release. If the originator or originators cannot be established the relevant committee will assume the responsibility of the originator.)

3. In the case of NATO classified information originated by one or more nations participating in a NATO Production and Logistics Organisation or other organisation granted a charter under the terms of C-M(62)18 or generated within that organisation and pertaining to it, the application for release - see paragraph 1 above - will be submitted to the Board of Directors (or to any other body designated by higher authority) of the NATO organisation concerned. Provided it unanimously agrees that the information should be released, the Board of Directors (or any other body designated by higher authority) will seek the approval of the National Security Authorities of the nations participating in the NATO organisation's programme for its dissemination.

(1) For ease of reference, hereafter in this Annex the term "relevant committee" will be used in lieu of the expression "as appropriate, either to the Military Committee or to the NATO civil committee most concerned with the information"

If approval is given, the information will be passed in accordance with the procedures referred to in paragraphs 4 and 5 below. Records of all classified information passed under these procedures together with the written confirmation referred to in paragraph 5 below will be maintained by the NATO organization concerned. These records will be subject to examination by the NATO Office of Security during their annual inspections.

4. If approval is given, the relevant committee or Board of Directors (or any other body designated by higher authority), as appropriate, will ask the sponsor to obtain from the intended recipient, confirmation that the information to be released will be accorded at least that measure of security protection already afforded to it within the North Atlantic Treaty Organization. In certain circumstances the sponsor may consider it useful to send to the intended recipient a copy of the relevant instructions as set out in the attached Appendix.

5. When release has been approved by Council or the Military Committee or the National Security Authorities concerned, as appropriate, and the sponsor confirms that the written undertaking required by paragraph 4 above has been obtained, the release will be made:

(a) in respect of military information excluding that noted in (c) below by the sponsor or other body designated by the sponsor;

(b) in respect of non-military information excluding that noted in (c) below by the Division of Political Affairs;

(c) in respect of information pertaining to NATO Production and Logistics Organizations or other organizations granted charters under the terms of C-M(62)18 by the Board of Directors (or by any other body designated by higher authority) of the NATO Organization concerned.

In all the above cases, the marking NATO and all other reference markings should be removed, if this is considered practicable or desirable, before the documents are transmitted.

SECURITY REGULATIONS TO ENSURE THE PROTECTION OF NATO CLASSIFIED INFORMATION PASSED BY THE NORTH ATLANTIC TREATY ORGANIZATION TO NON-NATO NATIONS AND TO INTERNATIONAL ORGANIZATIONS COMPOSED EITHER WHOLLY OR PARTLY OF NON-NATO NATIONS

PERSONNEL

1. The number of officials in the non-NATO nation or the international organization who will hav access to NATO classified information must be strictly confined to those whose duties make such access essential according to the principle of need-to-know. These officials must be authorized to have access to national information of the same classification as the NATO document.

DOCUMENTS

Registration on Arrival

2. As soon as a NATO classified document is received, it will be listed in a special register, held by the nation or national organization, the pages of which will bear columns indicating the date received, the date of the document, its serial number, its copy number, its security classification, its title, the date when the receipt is returned and the date the document, when no longer required, is sent back to NATO or destroyed.

Return of Documents

3. If a NATO classified document is returned to the sender the double cover system must be used. The inner cover will be marked NATO together with the security classification. A receipt form will be enclosed for each NATO classified document. The receipt form, which requires no security classification, should quote only the reference number, date, copy number and language of the document and not its title. The inner cover will be enclosed in an outer cover which will bear a package number for receipting purposes. Under no circumstances will any security classification appear on the outer envelope. Messengers will always obtain receipts against package numbers.

Custody and Security Protection

4. When not in use, documents will be stored in a security container which is approved for the storage of national documents of a similar classification as the NATO documents. Such containers will bear no indication of their contents, which will be accessible only to those authorized to have access to NATO classified information. In the case of combination locks, the combination will be known only to the officials of the nation or

international organization authorized access to NATO classified information and will be charged every six months, or sooner in case of transfer of an authorized official, or when compromise is suspected.

5. NATO classified documents may only be removed from the security container in which they are housed by members of the nation or international organization who are authorized to have access to the documents. The person removing a document from the security container will be responsible for ensuring its safe custody at all times until he replaces it in the container. In particular, he must ensure that no one who is not authorized to see the document has access to it.

6. No copies or extracts of NATO classified documents will be made. Original requests for the document should denote the number of copies required - which must be kept to a minimum.

7. Plans for the rapid and total destruction in an emergency of NATO classified documents should be prepared and confirmed as workable.

PHYSICAL

8. When not in use, any security container used for the storage of NATO classified documents will at all times be kept securely locked.

9. When maintenance personnel or cleaners are required to enter or remain in the room in which the security container is located, they must at all times be escorted by a member of the national or international organization responsible for that particular room or by a member of the security staff of that organization.

10. Outside office hours (nights, week-ends and holidays), protection of the security container will be provided either by a watchman or by an automatic alarm system.

BREACHES OF SECURITY

11. Whenever a breach of security affecting NATO classified information is discovered:

(a) a report giving details of the breach will be sent immediately to the security authority of the sponsor or NATO body which sent the document;

(b) an investigation into the circumstances of the breach will be made. When completed, a full report will be submitted to either security authority mentioned in (a) above. At the conclusion of this investigation, remedial or corrective action, where appropriate, will be taken.

REPORTS

12. So long as the nation or international organization holds NATO classified information it will submit an annual report, to reach the NATO Office of Security by 31st January each year, to confirm the above security regulations are being implemented.

NATO SECURITY CLEARANCE CERTIFICATE

Certification is hereby given that:

Full Name:

Date and Place of Birth:

has been granted a security clearance by the Government of

.... in

accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including: (1) .....

.....

.....

.....

.....

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

.....

Signed:

Title: Offical government stamp

Date:

---

(1) Insert, as appropriate, one or more of the following:

(a) COSMIC TOP SECRET
(b) NATO SECRET
(c) NATO CONFIDENTIAL
(d) COSMIC TOP SECRET ATOMAL
(e) NATO SECRET ATOMAL
(f) NATO CONFIDENTIAL ATOMAL

(2) Date of expiry of this certificate must conform to the provisions of paragraph 3 of the Supplement to C-M(55)15(Final)

CERTIFICATE OF SECURITY CLEARANCE

Issued by .....
(member nation or NATO command or agency)

Date and Place of Issue .....

..... Valid until .....

This is to certify that:

Full Name .....

Date of Birth .....

Place of Birth .....

Nationality .....

Where employed .....

Purpose and Duration of Visit .....

.....

.....

.....

Holder of Passport/Identity Card No. .....

Issued at ..... Dated .....

Military Rank and Number (where applicable) .....

.....

has been cleared for access to NATO information classified up to and including ..... in accordance with current NATO security regulations and has been briefed accordingly by

.....

Signed:

Title: Offical seal or stamp

Date:

NOTE: This certifcate must be handled in accordance with the provisions of paragraph 40 of Enclosure "C" to C-M(55)15(Final)

COURIER CERTIFICATE

Valid until .....

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

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 authorized to carry ..... of packages of official NATO documents, the
(number)
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 Authorizing Official:

Designation:
(Name and rank in capitals)

Official stamp of NATO member nation or NATO command or agency Date:

ORDRE DE MISSION D'UN COURRIER

Valable jusqu'au .....

1. Il est certifié par la présente que le porteur .....,
(nom et grade, le cas échéant)
détenteur du Passeport/Carte d'identité no. .....est membre de .....
.....
(organisme d'appartenance)

2. Au cours des voyages mentionnés au verso, le porteur voyage en exécution de ses fonctions officielles et est accrédité comme un courrier officiel de l'OTAN. Il est autorisé a transporter ..... paquets contenant des documents officiels
(nombre)
de l'OTAN, dont les sceaux correspondent au modèle du sceau apposé en regard du voyage indiqué.

3. Tous les fonctionnaires des services de douanes et de l'immigration sont, en conséquence, priés d'appliquer à la correspondance et aux documents officiels transportés sous sceau officiel par le porteur l'immunité prévue en matière de visite et de contrôle douanier par la Convention sur le Statut de l'Organisation du Traité de l'Atlantique Nord, des Répresentants nationaux et du Personnel international et la Convention entre les Etats parties au Traité de l'Atlantique Nord sur le Statut de leurs Forces.

Signature du fonctionnaire responsable:

Désignation:
(nom et grade en majuscules)

Sceau officiel du pays membre de l'OTAN ou du commandement ou organisme de l'OTAN Date:

DETAILS OF ITINERARY
DETAILS DE L'ITINERAIRE

SPECIMEN OF SEAL USED
MODELE DU SCEAU UTILISE

From / De	to / à	
		See note below / Voir note ci-dessous
From / De	to / à	See note below / Voir note ci-dessous
From / De	to / à	See note below / Voir note ci-dessous
From / De	to / à	See note below / Voir note ci-dessous

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.

En complément à l'impression du sceau, le fonctionnaire apposant le sceau doit mentionner en majuscules, son nom et grade ainsi que le nom et l'adresse de son service, commandement, organisme ou établissement.

COMMUNIST COUNTRIES

Albania
Bulgaria
Chinese People's Republic
Cuba
Czechoslovakia
German Democratic Republic
Berlin (East)
Hungary
North Korea
North Vietnam
Outer Mongolia
Poland
Rumania
Soviet Union
Yugoslavia

INDEX

to

ENCLOSURES "A", "B", "C", "D" AND SUPPLEMENT

Note: In this Index, the references given are to paragraphs, preceded by the letters A, B and C representing the appropriate Enclosures, with cross-references to the Indexes to Enclosure "D" (D) and The Supplement (S)

Example: COMMUNIST CONTACTS — B. 9(e), C. 34-37 See also Index to D, Index to S

indicates that the required information will be found in paragraph 9(e) of Enclosure "B", in paragraphs 34 to 37 of Enclosure "C" and under "COMMUNIST CONTACTS" in the Indexes to Enclosure "D" and to The Supplement.