CONSEIL DE L'ATLANTIQUE NORD
NORTH ATLANTIC COUNCIL

EXEMPLAIRE N° 212
COPY

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

ORIGINAL: ENGLISH
17 September, 1980

CORRIGENDUM 7 to
VOLUME I to
C-M(55)15(Final)

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

CORRIGENDUM 7 to Volume I to C-M(55)15(Final)
(dated 31st July, 1972)

Following approval by the North Atlantic Council of C-M(80)43, holders of Volume I of C-M(55)15(Final) should substitute the attached pages (ii), 5, 18, 18A, 20, 20A, 21, 21A, 22, 31 and 72 for the existing pages (ii), 5, 18, 18A, 20, 21, 22, 31 and 72 which should be destroyed. Changes have been underlined or sidelined.

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

3. Amendments to the Index will issue later.

NATO,
1110 Brussels.

(1) NATO UNCLASSIFIED when detached from enclosures.

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 countries with special security risks(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 countries with special security risks is at Annex 6 to Enclosure "C"

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 initially made aware, and periodically reminded, of the dangers to security arising from indiscreet conversation with persons having no need-to-know, on their relationship with the press, and on the threat presented by the activities of hostile intelligence. Such persons will be thoroughly briefed on these dangers.

35. Such personnel must be urged to report immediately to the appropriate security authorities any contacts they may have with nationals of countries with special security risks(1) 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 countries with special security risks 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 scheduled stop-overs by air travel) countries with special security risks or to any destination by any form of transport that belongs to, is registered in, or managed from such a 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;

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

(1) A list of countries with special security risks is at Annex 6.

37.1 Heads of NATO commands and agencies must seek prior authority from the prospective traveller's National Security Authority before granting permission for the visit to take place. The Head of a NATO command or agency has absolute discretion to grant or refuse a request, except that he may not grant permission when the National Security Authority has recommended refusal. Additionally, the NOS 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.

37.2 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.

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

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.

SECTION IV

PHYSICAL SECURITY

GENERAL

48. This Section lays down the policy and minimum standards for the physical security measures for the protection of NATO classified information. The object of physical security measures is to prevent an unauthorized person from gaining access to NATO classified information.

SECURITY REQUIREMENTS

49. The premises in which NATO classified material is housed will vary greatly, ranging from the large government department in a capital city to a tent pitched in a field, and the security measures necessary will vary also. In some buildings there is much NATO classified information which requires safeguarding and in these, comprehensive physical security measures will be necessary. In other buildings there may be little NATO classified information and it may be possible to arrange that all highly classified material is kept in one safe or strong room, or under permanent guard.

50. In deciding what degree of physical security protection is necessary, account must be taken of all relevant factors such as:

- the level of classification and category of information;
- the amount and form of the information held;
- the security clearance and need-to-know of the staff; and
- the locally assessed threat from hostile intelligence services, and terrorist and criminal activities.

51. The physical security measures achieved must be designed to:

(a) deny surreptitious or forced entry by an intruder;

(b) deter, impede and detect actions by disloyal personnel (the spy within); and

(c) allow for segregation of staff in their access to NATO classified information in accordance with the principle of need-to-know.

PHYSICAL SECURITY MEASURES

Security Areas

52. Areas where information classified NATO CONFIDENTIAL or higher is handled and stored must be organized and structured so as to correspond to one of the following:

(a) Class 1 Security Area: an area where NATO CONFIDENTIAL information or higher and of any category is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information, e.g. document registries and operations centres. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) a control of entry system which admits only those appropriately cleared and specially authorized to enter the area;

(iii) specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;

(b) Class 2 Security Area: an area where NATO CONFIDENTIAL information or higher and of any category is handled and stored in such a way that it can be protected by controls established internally from access by unauthorized persons, e.g. premises containing offices in which information classified NATO CONFIDENTIAL and higher is regularly handled and stored. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) a control of entry system which admits unescorted only those cleared and specially authorized to enter the area. For all others, provision is made for escorts or equivalent controls to prevent unauthorized access to NATO classified information and uncontrolled entry to areas subject to technical security inspections.

Those areas which are not occupied by duty personnel on a 24 hour basis will be inspected immediately after normal working hours to ensure that NATO classified information is properly secured.

Administrative Zone

53. Around or leading up to Class I or Class II Security Area an Administrative Zone of lesser security may be established. Such a zone requires a visibly defined perimeter within which possibility exists for control of personnel and vehicles. NATO RESTRICTED information only will be permitted to be handled and stored in Administrative Zones.

Control of Entry

54. Entry into Class I and Class II Security Areas will be controlled by a pass or personal recognition system governing the regular staff. A system of control of visitors designed to deny unauthorized access to NATO classified information must also be established. Whenever possible, a pass should not show in clear text or symbols the identity of the issuing organization and/or the place to which its holder is allowed entry. Pass systems may be supported by automated identification, which should be regarded as a supplement to, but not a total replacement for, guards.

Guards

55. When guards are used to ensure the integrity of security areas and NATO classified information they must be appropriately cleared, qualified by training and supervised.

55.1 Patrols of Class I and Class II security areas should take place outside normal working hours and on non-working days at intervals to be determined by the security authority in the light of the local threat. The patrols shall ensure that NATO classified information is properly protected and that there is no sign of any untoward incident.

55.2 In order to improve general guard coverage and, for security areas where in the interests of security it has been determined that members of the guard force may not have direct entry, intruder detection by means of devices such as closed circuit television, alarm system or visual inspection ports should be provided. The former devices may also be employed as substitutes for patrols.

55.3 The response force required is to provide a minimum of two guards to any point of a security disorder on the site without weakening site protection elsewhere. Guard response to alarms or emergency signals shall be tested and must be within a time limit evaluated as capable of preventing an intruder's access to the NATO classified information being protected.

Security Containers and Strong Rooms

56. Containers used for storage of NATO classified information are divided into three classes:

- Class A: containers nationally approved for storage of COSMIC TOP SECRET information within a Class I or a Class II Security Area;
- Class B: containers nationally approved for storage of NATO SECRET and NATO CONFIDENTIAL information within a Class I or a Class II Security Area;
- Class C: office furniture suitable for storage of NATO RESTRICTED information only.

57. For strong rooms constructed within a Class I or a Class II Security Area and for all Class I Security Areas where information classified NATO CONFIDENTIAL and higher is stored on open shelves or displayed on charts, maps, etc, the walls, floors and ceilings, door(s) with lock(s) must be certified by a national security authority to offer equivalent protection to the class of security container approved for the storage of the NATO classified information involved.

Locks

58. Locks used with security containers and rooms in which NATO classified information is stored shall meet the following standards:

- Group A: nationally approved for Class A containers;
- Group B: nationally approved for Class B containers;
- Group C: suitable for Class C office furniture only.

Control of keys and combinations

59. Keys of security containers should not be taken out of the office building. Combination settings of security containers will be committed to memory by persons needing to know them. Spare keys and a written record of each

combination setting for use in an emergency should be held in sealed opaque envelopes by the government department or NATO command or agency concerned. Working and spare security keys should be kept in separate containers. The record of each combination should be kept in a separate envelope. The keys and the envelopes should be given security protection no less stringent than the material to which they give access.

60. Knowledge of combination settings of security containers will be restricted to the smallest possible number of persons. Settings will be changed:

(a) at intervals of not more than six months;

(b) whenever a change of personnel occurs;

(c) whenever a compromise has occurred or is suspected.

Intruder Detection Devices

61. When alarm systems, closed circuit television and other electric devices are used in the protection of NATO classified information, electricity must be provided through permanently connected external mains supply with a rechargeable standby battery. Another basic requirement is that a malfunction in or tampering with such systems shall result in an alarm or other definitive warning to the monitoring personnel.

Approved Equipment

62. National security authorities will maintain, from their own or from bilateral resources, lists of equipment which they have approved for the direct or indirect protection of NATO classified information under various specified circumstances and conditions. NATO commands and agencies will consult with their host nation before purchasing such equipment.

Physical Protection of Copying Machines

63. Copying machines must be physically protected to the extent necessary to ensure that only authorized persons can use them and that all classified products are properly controlled.

PROTECTION AGAINST OVERLOOKING AND EAVESDROPPING

Overlooking

64. When NATO classified information is at risk from overlooking, appropriate measures must be taken to counter this risk under daylight as well as artificial light conditions.

Eavesdropping

65. Offices or areas in which highly classified information is regularly discussed must be protected against passive and active eavesdropping.

65.1. Protection against passive eavesdropping - the leakage of classified information via insecure communications or by overhearing directly - will

involve technical security inspections as described in paragraph 65.3 below and may involve soundproofing walls, doors, floors and ceilings.

65.2 Protection against active eavesdropping - the leakage of classified information by wired microphones, radio microphones or other implanted devices - requires a technical security inspection of the fabric of the room, its furnishings and fittings and its office equipment, including office machines and communications.

Technically Secure Areas

65.3 Areas to be protected against eavesdropping should be technically inspected at least once a year and after any entry by uncleared and unsupervised people for maintenance work, redecoration and the like. These areas are to be designated as technically secure areas and entry to them must be specially controlled. They should be kept locked when not occupied and the keys treated as security keys. No new furnishings or equipment should be allowed in until inspected and approved by the technical security authority. Whenever possible, telephones should not be installed in areas which are technically inspected. Where their installation is unavoidable, and where the nature of the telephone system makes this desirable, telephones should be provided with a positive disconnect device.

Examination of electric/electronic office equipment

65.4 Before being used in those areas where meetings or work is being performed which involves highly classified NATO information or the threat is considered to be high, communications equipment and electric or electronic office equipment of any kind should be examined by technical or communications security experts to ensure that no intelligible information is inadvertently/illicitly transmitted by such equipment beyond the perimeter of the appropriate security area.

Security of Courier and Messenger Personnel

107. 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.

Personal Carriage

108. Each member nation and NATO command and agency will prepare instructions covering the personal carriage of documents classified NATO CONFIDENTIAL and above by hand of persons other than couriers and messengers based on these regulations. These instructions will make it clear that:

(a) in no circumstances may COSMIC TOP SECRET documents be carried internationally;

(b) the bearer must be cleared for access to at least the level of classification of the documents carried;

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

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

(e) the documents must not leave the possession of the bearer unless they are housed in accordance with the provisions for safe custody contained in Section IV, i.e. the documents must not be left unattended (e.g. in hotels, and vehicles) or stored in hotel safes or luggage lockers;

(f) the documents must not be read in public places (e.g. in aircraft, trains, etc.);

and, when international carriage is involved, that:

(g) the container or document package will be covered by an official seal, or likewise protected under procedures designed to prevent customs examination;

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

(i) the bearer must not travel either by surface routes through non-NATO nations or by air routes over countries with special security risks (see Annex 6). 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.

The bearer will be required to read and sign these instructions.

COUNTRIES WITH SPECIAL SECURITY RISKS

Popular Republic of Albania

Berlin (East)

People's Republic of Bulgaria

People's Republic of China

Republic of Cuba

Czechoslovak Socialist Republic

German Democratic Republic

People's Republic of Hungary

Democratic State of Kampuchea

Korean Democratic People's Republic

People's Democratic Republic of Laos

Mongolian People's Republic

Polish People's Republic

Socialist Republic of Romania

Union of Soviet Socialist Republics

Socialist Republic of Vietnam

Socialist Federal Republic of Yugoslavia